The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Cybersecurity and Law

2026 Nr 1 (15)

DOI: 10.35467/cal/243742

AI w służbie bezpieczeństwa i obronności – zarządzanie kryzysowe, interoperacyjność i etyka w nowej europejskiej architekturze zarządzania bezpieczeństwem

AI in the service of security and defence – crisis management, interoperability and ethics in the new European security governance architecture

Kamila ZARYCHTA-ROMANOWSKA
Uniwersytet Warszawski
ORCID: 0000-0002-8403-0156
E-mail: Zarychta@gmail.com

Streszczenie

Cele: Artykuł analizuje rolę sztucznej inteligencji w nowej architekturze bezpieczeństwa Unii Europejskiej, ze szczególnym uwzględnieniem zarządzania kryzysowego, interoperacyjności, zagrożeń hybrydowych oraz gwarancji prawnych i etycznych. Celem jest wyjaśnienie, w jaki sposób AI może wspierać prewencję i współpracę instytucjonalną bez naruszania zasad państwa prawa.

Metody: Zastosowano analizę instytucjonalno-prawną oraz krytyczną analizę literatury i dokumentów strategicznych UE, w tym raportu Safer Together, regulacji AI Act i ram współpracy agencji odpowiedzialnych za bezpieczeństwo.

Wyniki: Interoperacyjność należy rozumieć jako zdolność zarządczą łączącą detekcję, analizę, decyzję i egzekwowanie prawa, a nie wyłącznie integrację systemów informatycznych. AMLA i FIU.net mogą wzmacniać wykrywanie ryzyka finansowego, Europol wspierać interpretację operacyjną, EPPO zapewniać reakcję prawną, a ENISA rozwijać odporność cyfrową. EMPACT stanowi platformę koordynacji działań bez konieczności centralizacji kompetencji wywiadowczych.

Wnioski: Wdrażanie AI powinno opierać się na prewencji, nadzorze człowieka, audytowalności, proporcjonalności i rozliczalności. O skuteczności unijnej architektury bezpieczeństwa decyduje nie tylko dostępność danych, lecz przede wszystkim ich zgodna z prawem wymiana i terminowe wykorzystanie.

Słowa kluczowe

sztuczna inteligencja, bezpieczeństwo Unii Europejskiej, interoperacyjność, zagrożenia hybrydowe, cyberbezpieczeństwo

Abstract

Objectives: This article examines artificial intelligence in the emerging European Union security architecture, focusing on crisis management, interoperability, hybrid threats and legal and ethical safeguards. It asks how AI can strengthen prevention and institutional cooperation while preserving the rule of law.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Methods: The study employs legal-institutional analysis and a critical review of academic literature, EU strategic documents and regulatory frameworks, including the Safer Together report and the AI Act.

Results: Interoperability is conceptualised as a governance capacity linking detection, analysis, decision-making and legal enforcement, rather than merely the technical integration of databases. AMLA and FIU.net can support financial-risk detection; Europol can facilitate operational interpretation; EPPO can provide a prosecutorial response; and ENISA can strengthen digital resilience. EMPACT offers a framework for operational coordination without premature centralisation of intelligence powers. The principal constraint is not necessarily a lack of data, but fragmented institutional, technical and legal arrangements for using them.

Conclusions: Responsible AI deployment requires preventive objectives, meaningful human oversight, auditability, proportionality and institutional accountability. The effectiveness and legitimacy of the EU security architecture depend on lawful information-sharing, timely decisions and sustained public trust.

Keywords

artificial intelligence, European Union security, interoperability, hybrid threats, cybersecurity

Wstęp

Jesteśmy świadkami kolejnej rewolucji technologicznej związanej z upowszechnieniem się sztucznej inteligencji (SI) jako powszechnie dostępnego narzędzia analitycznego (GenAI). Jednocześnie żyjemy w warunkach polikryzysu- wojna na wschodniej flance Unii Europejskiej, intensyfikacja zagrożeń hybrydowych i kinetycznych- co zasadniczo zmieniło postrzeganie bezpieczeństwa. Odwrót od wąskiego, materialnego rozumienia tego dobra zainicjował badania nad wymiarem ontologicznym bezpieczeństwa, rozumianego jako zdolność wspólnot i instytucji do podtrzymywania porządku, przewidywalności oraz zaufania do porządku normatywnego[1].

Bezpieczeństwo Unii Europejskiej ewoluuje przybierając funkcję komponentów dotychczas zarezerwowanych dla bezpieczeństwa narodowego-europejskiego homeland - rozumianego jednak w sposób holistyczny -nie jako militaryzacja przestrzeni wewnętrznej, a potrzeba wspólnej ochrony integralności politycznej, porządku normatywnego i wartości konstytutywnych[2]. Wojna, presja hybrydowa, destabilizacja informacyjna w warunkach polikryzysów przesuwają akcent z rozproszonej odpowiedzialności państw na współdzieloną gotowość i solidarność w obronie europejskiej wspólnoty bezpieczeństwa.

Sztuczna inteligencja – budząca tak fascynację, jak i społeczne obawy – oferuje wyjątkowe możliwości wielowymiarowej analizy ryzyka i koordynacji działań. Niesie także ryzyka reprodukcji uprzedzeń (bias), błędów systemowych, halucynacji algorytmicznych oraz przesunięcia odpowiedzialności z poziomu instytucjonalnego na techniczny.

W artykule wskazano, iż odpowiedzią Unii na ten proces nie jest jedynie centralizacja czy reaktywne zarządzanie kryzysowe, lecz stopniowe i konsekwentne budowanie sieciowej architektury gotowości i prewencji. Fundamentalnymi elementami stają się w niej specjalistyczne instytucje i mechanizmy - od wywiadu finansowego i egzekucji prawnej (AMLA, EPPO), przez cyberbezpieczeństwo i regulację technologii (ENISA), po koordynację analityczno-operacyjną (Europol i Frontex) – wzmacniane

[1] J. Mitzen, Ontological security in world politics, „European Journal of International Relations" 2006, t. 12, nr 3, s. 341–370.

[2] K. Zarychta-Romanowska, Creating an EU homeland security: Examining the potential of EBCGA and EPPO cooperation in countering terrorist and criminal financing, [w:] Countering terrorist and criminal financing, S. Romaniuk, C. Kaunert, A.P.H. Fabe (red.), Routledge 2022.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

nowymi paradygmatami bezpieczeństwa, sformułowanymi w raporcie Niinistö, w tym najważniejszym, wskazującym że przygotowanie na kryzys winno być rozwijaną postawą „preparedness is an attitude".

Podstawowym problemem jest więc nie tylko dostępność danych, ale i zdolność do ich zgodnej z prawem syntezy, właściwej interpretacji i translacji na działanie prewnecyjne kryzysu. Interoperacyjność oznacza tu, tym samym, zdolność zarządzania – governance, wychodząc ponad techniczną kompatybilność systemów.

Budowa nowej architektury bezpieczeństwa

Współczesne bezpieczeństwo Unii Europejskiej często przybiera postać stanu zaufania, i jest rozpatrywana w kategorii zdolnością instytucji do utrzymania przewidywalności, spójnej interpretacji status quo i szybkiej reakcji w granicach prawa. To często kryzys braku poczucia bezpieczeństwa implikuje kryzys wewnętrzny UE - społeczny, polityczny i tożsamościowy - oraz podatność strategiczną, którą wrogie siły wykorzystują jako narzędzie wytwarzania chaosu i celowej erozji zaufania. Odpowiedź UE musi więc dotyczyć nie tylko ochrony systemów, ale też ochrony porządku, przy jednoczesnym zachowaniu praworządności, jako warunku legitymizacji działań[3].

Unia Europejska rozwija ramy regulacyjne dotyczące sztucznej inteligencji, cyberbezpieczeństwa i rynku cyfrowego. Wyzwaniem pozostaje pogodzenie innowacji i operacyjnych zastosowań technologii z ochroną danych, odpowiedzialnością instytucji i prawami podstawowymi.

Wykorzystanie baz danych w działaniach organów ścigania ujawnia systemowy problem fragmentaryzacji europejskich systemów informacyjnych, wykraczający poza politykę migracyjną. Przypadek Cambridge Analytica pokazuje zarazem, jak profilowanie i mikrotargetowanie mogą służyć operacjom wpływu, których konsekwencje dotyczą nie tylko zachowań konsumenckich, lecz także bezpieczeństwa i zaufania do instytucji.[4]

Wojna Rosji przeciwko Ukrainie unaocznia kruchość europejskiego poczucia bezpieczeństwa, także wśród ludności mieszkającej poza obszarem bezpośrednich działań kinetycznych. Dezinformacja i presja hybrydowa pogłębiają niepewność, w której kryzysy przestają mieć charakter incydentalny.[5]

Kształtowane przez algorytmy zagrożenia hybrydowe działają najskuteczniej nie przez niszczenie infrastruktury, lecz poprzez podważanie zdolności wspólnoty politycznej do rozpoznawania zagrożeń, intencji przeciwnika oraz utrzymania zaufania do procedur państwa. Ontologiczny aspekt bezpieczeństwa staje się przez to kluczową kategorią analityczną tak w interpretacji agresji, jak i w rekonstrukcji unijnych strategii bezpieczeństwa po 2022 r.

W tym ujęciu presja ekonomiczna, regulacyjna i technologiczna nie stanowi wyłącznie narzędzia polityki, lecz staje się elementem podkreślenia normatywnej tożsamości Unii w warunkach ontologicznej niepewności. Bezpieczeństwo cyfrowe, regulacja sztucznej inteligencji oraz przeciwdziałanie zagrożeniom hybrydowym stają

[3] O. Elkhova, Ontological-societal security node as a phenomenon of the digital environment, „RUDN Journal of Philosophy" 2025, t. 29, nr 2, s. 317–334; M. Perfetto, Weaponisation of interdependence: Unpacking European ontological anxieties, „Central European Journal of International and Security Studies" 2025.
[4] C.O. Schneble, B.S. Elger, D. Shaw, The Cambridge Analytica affair and Internet-mediated research, „EMBO Reports" 2018, t. 19, nr 8, e46579.
[5] M. Słowikowski, What does ontological security theory tell us about Russia's decision to start the war against Ukraine?, „Studia Polityczne" 2025, t. 53, s. 5–36.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

warunkiem *sine qua non* utrzymania zaufania społecznego, zdolności decyzyjnej oraz demokratycznej sprawczości UE[6].

Nowe technologie i wielorakie zagrożenia hybrydowe muszą być odczytywane przez pryzmat oczekiwań obywateli UE i skutków politycznych, zwłaszcza w obszarze ochrony demokracji. Złośliwe operacje informacyjne – takie jak neurolingwistycznie „dostrojone" kampanie wpływu używane do produkcji masowej perswazji - uderzają w istotę węzła ontologiczno-społecznego: rozstrajają zaufanie, rozrywają więzi, relatywizują normy i destabilizują. W efekcie rola organów ścigania i instytucji odpowiedzialnych za bezpieczeństwo nabiera nowego znaczenia w kontekście obecności i gotowości w domenie cyfrowej.

Program polityki „Droga ku cyfrowej dekadzie" do 2030 r. wiąże rozwój infrastruktury danych, zaufanych technologii i kompetencji cyfrowych z cyberbezpieczeństwem oraz interoperacyjnością. W tym sensie cyfryzacja staje się także elementem gotowości instytucjonalnej i odporności UE.[7]

Raport „Safer Together" Saulia Niinistö (2024) ujmuje gotowość cywilną i wojskową jako fundament nowoczesnych polityk UE, wskazując na konieczność implementacji triady potrzeb- szybkiej identyfikacji ryzyka, koordynacji i przełamywania sektorowego rozproszenia działań.[8]

Niinistö wychodzi z założenia, że współczesne kryzysy mają charakter strukturalny, są trudne do przewidzenia i nie respektują podziałów sektorowych. Implikują przez to konieczność detekcji i reakcji w czasie zbliżonym do rzeczywistego, przy jednoczesnym zachowaniu, rozbudowanej w UE, kontroli prawnej, demokratycznej i politycznej. Postulaty identyfikacji ryzyka, analizy antycypacyjnej i wczesnego ostrzegania, a także przezwyciężenie podejścia silosowego poprzez integrację cywilno-wojskowej gotowości oraz lepszą koordynację struktur na poziomie unijnym i krajowym stały się tym samym kamieniem węgielnym nowej struktury wzmacniania bezpieczeństwa UE. Gotowość *preparedness* nie jest hasłem normatywnym a precyzyjną diagnozą operacyjną: oznacza postawę opartą na współodpowiedzialności, koordynacji i odporności społecznej, której warunkiem jest systematyczna wymiana informacji oraz zdolność do ich terminowej integracji. Dekada Kryzysów wskazuje, że bezpieczeństwo w XXI wieku zależy od skracania pętli decyzyjnych i konwergencji danych pochodzących z domen wojskowej, policyjnej, granicznej, cybernetycznej i finansowej. W tym ujęciu intelligence-led policing oraz border policing przestają być funkcjami sektorowymi, a stają się elementami wspólnej architektury zarządzania ryzykiem w warunkach presji hybrydowej.[9].

Wojna Rosja – Ukraina jako wyścig wywiadowczy: implikacje dla UE i rozwoju JHA Network

Doświadczenia wojny przyspieszyły w UE przesunięcie w stronę *intelligence-led policing* jako dominującego paradygmatu bezpieczeństwa wewnętrznego. Obejmuje on dziś nie tylko klasyczne działania policyjne, lecz również *security policing,* policyjne zarządzanie granicami *(border policing)*- oraz zarządzanie kryzysowe *(crisis management)*, integrując analizę zagrożeń, wczesne ostrzeganie i transgraniczną

[6] Komisja Europejska, Strategia UE w zakresie unii bezpieczeństwa 2020–2025, COM(2020) 605 final.
[7] Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r.
[8] S. Niinistö, Safer together: Strengthening Europe's civilian and military preparedness and readiness, Komisja Europejska 2024.
[9] Ośrodek Studiów Wschodnich, Resilience of the European Union and NATO in the era of multiple crises, [dostęp:28.02.2025].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

koordynację. Granice zewnętrzne UE nabierają fundamentalnego znaczenia jako jako węzły wywiadowcze, w których krzyżują się dane migracyjne, kryminalne, finansowe, cybernetyczne i infrastrukturalne.

Niewątpliwie rola Frontexu ulega jakościowej transformacji. Agencja przestaje być wyłącznie operatorem wsparcia granicznego, a staje się kluczowym elementem europejskiej architektury *border intelligence*, osadzonej w interoperacyjności systemów informacyjnych, analizie ryzyka i współdzielonej świadomości sytuacyjnej. Integracja Frontexu z siecią JHA (Europol, Eurojust, EPPO, AMLA, ENISA) tworzy zalążek sieciowej architektury bezpieczeństwa, w której informacja krąży pomiędzy domenami zarządzania bezpieczeństwem, a nie pozostaje zamknięta w sektorowych silosach infrastruktury.

Pytania badawcze i strategiczne sformułowane w raporcie Niinistö - dotyczące identyfikacji ryzyka, analizy antycypatywnej, wczesnego ostrzegania, przygotowania cywilno-wojskowego oraz koordynacji na poziomie krajowym i unijnym - wyznaczają kierunek rozwoju nowej architektury bezpieczeństwa UE, połączonej z rozwojem JHA Network, pogłębioną interoperacyjnością systemów IT oraz ściślejszą współpracą Frontexu z agencjami bezpieczeństwa. Działania te to europejska odpowiedź na egzystencjalne wyzwanie: jak zachować otwartość, wolność i rządy prawa w warunkach permanentnej presji hybrydowej [10].

Od kryzysu ontologicznego do architektury prewencji: AI, zagrożenia hybrydowe i sieciowa logika bezpieczeństwa UE

Wojna w cyberprzestrzeni czy złośliwe użycie generatywnej AI przez wrogie podmioty stają się integralnym komponentem presji hybrydowej. Jej celem jest destabilizacja nie przez frontalny atak, lecz przez zaburzenie wiarygodności, rozmycie odpowiedzialności i przeciążenie systemów decyzyjnych. Problemem nie jest już brak danych, lecz brak zdolności do ich terminowej syntezy i przełożenia na decyzję w czasie umożliwiającym zapobieżenie atakowi. To właśnie tu materializuje się potrzeba architektury konwergencji: nie jako „superinstytucji", lecz jako ulepszonego, sprawnego, odpornego i kontrolowalnego systemu wiązania informacji, analizy i odpowiedzialności.

Odpowiedzią Unii Europejskiej na deficyty w komponencie konwergencji informacyjnej i decyzyjnej stała się stopniowo wyłaniająca się sieciowa architektura bezpieczeństwa, której rdzeniem pozostaje Sieć Agencji Wymiaru Sprawiedliwości i Spraw Wewnętrznych (JHA Network). Dzięki budowanej zdolności instytucjonalnego wiązania sygnałów słabych, danych rozproszonych oraz kompetencji sektorowych instytucje uzyskują narzędzia, aby bezpieczeństwo było rezultatem trwałej kooperacji, a nie jedynie sumą równoległych, słabo skoordynowanych polityk[11]. Sieciowość nie znosi jednak ograniczeń wynikających z mandatów poszczególnych agencji. Dostęp do danych, ich dalsze wykorzystanie oraz wymiana informacji między organami muszą każdorazowo znajdować podstawę w odpowiednich przepisach, tym samym przeciwdziałając sytuacji gdy integracja technologiczna mogłaby wyprzedzić integrację prawną, wytwarzając pozór sprawczości bez rzeczywistej zdolności do wspólnego działania.

Europol pełni w tym kontekście kluczową rolę węzła analityczno-operacyjnego, stanowiąc instytucjonalną materializację logiki *intelligence-led policing* oraz skracania dystansu „sygnał–analiza–decyzja" w obszarze przestępczości zorganizowanej,

[10] Komisja Europejska i Wysoki Przedstawiciel UE, Załącznik do strategii na rzecz unii gotowości, JOIN(2025) 130 final.

[11] Eurojust, JHA Agencies Network; Frontex, Justice and Home Affairs Agencies Network, oficjalne strony agencji.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

terroryzmu, cyberzagrożeń i operacji hybrydowych. Funkcja ta wykracza poza akumulację danych; obejmuje wytwarzanie wspólnych ram interpretacyjnych i analitycznych, które umożliwiają państwom członkowskim ujmowanie zagrożeń jako zjawisk sieciowych, transgranicznych i wielodomenowych, a następnie podejmowanie działań w sposób skoordynowany i terminowy, pełniąc rolę centralnej komórki kooperacji policyjnej i bezpieczeństwa w Europie.

Istotnym komponentem tego systemu jest EMPACT (European Multidisciplinary Platform Against Criminal Threats), który stanowi praktyczną, operacyjną artykulację „sieciowości" na poziomie unijnego bezpieczeństwa wewnętrznego, zaprojektowaną jako mechanizm trwałej konwergencji analitycznej i operacyjnej najpilniejszych zagrożeń transgranicznych. Nie funkcjonuje on jako „czysto sektorowy" program działań, lecz jako zinstytucjonalizowana platforma integrująca analizę wywiadowczą, planowanie operacyjne oraz koordynację wielodomenową w perspektywie cyklicznej i długoterminowej. Wartość tego systemu buduje się nie na centralizacji kompetencji, lecz na wytwarzaniu wspólnej świadomości sytuacyjnej i priorytetyzacji zagrożeń w skali UE, co czyni EMPACT jednym z nielicznych mechanizmów zdolnych do systemowego reagowania na zagrożenia hybrydowe i sieciowe. W nowym cyklu programowym EMPACT ma uzyskać walory infrastruktury prewencyjnej, potencjalnie wspierana przez zaawansowaną analitykę danych i narzędzia oparte na sztucznej inteligencji, przy zachowaniu ram proporcjonalności, legalności i odpowiedzialności instytucjonalnej. W rezultacie prowadzic to będzie do integracji EMPACT z innymi politykami i jego umocowaniu jako wyznacznika kluczowych ram współpracy multidyscyplinarnej i multiagencyjnej[12].

Szczególne znaczenie w nowym cyklu bezpieczeństwa przypisuje się identyfikacji i zakłócania działalności najbardziej niebezpiecznych sieci przestępczych i jednostek, w tym tych, które posługują się korupcją, równoległymi systemami finansowymi, praniem pieniędzy, instrumentalnie wykorzystując legalne struktury gospodarcze oraz przemoc[13].

W tej architekturze wzrasta rola Frontex'u jako mundurowej formacji europejskiej, której obecność operacyjna na granicy zewnętrznej ma znaczenie nie tylko administracyjne, lecz strategiczne. Granica jest bowiem współcześnie przestrzenią, w które krzyżują się sygnały rzutujące na bezpieczeństwo UE: od nadużyć tożsamościowych i logistyki sieci przestępczych, przez próby infiltracji i działania pośrednie, po komponenty destabilizacji hybrydowej. Frontex – jako europejska formacja mundurowa – staje się elementem architektury prewencji: wzmacnia zdolność UE do „odczuwalnej" sprawczości tam, gdzie bezpieczeństwo zewnętrzne i wewnętrzne stykają się w sposób najbardziej namacalny[14].

W istniejącej architekturze IT i bezpieczeństwa brakowało węzła: systemowej warstwy finansowej, zdolnej do pełnienia funkcji wczesnego ostrzegania i realnego zakłócania „infrastruktury zagrożeń". W warunkach współczesnych konfliktów pieniądz jest zarówno wektorem działania, jak i nośnikiem informacji: finansuje logistykę, narzędzia, rekrutację, zakupy technologii, ale też pozostawia ślad – wzorzec, sieć, anomalię. Bez powiązania analizy finansowej z bezpieczeństwem wewnętrznym Unia pozostaje podatna na działania, które nie muszą generować natychmiastowych

[12] Rada UE, Council conclusions on the enhancement of EMPACT and on EU crime priorities for the next EMPACT cycle 2026–2029, 13.06.2025.
[13] Ibidem.
[14] K. Zarychta-Romanowska, Foreign fighters as a threat to Polish security and sovereignty, „Revista Facultății de Drept Oradea" 2019, nr 1, s. 95–122; K. Zarychta-Romanowska, M. Szostak, Frontex 3.0 - rewolucyjny czy rewelacyjny?, „Nowa Kodyfikacja Prawa Karnego" 2018, t. 50, s. 112–131.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

incydentów, aby systematycznie erodować zdolność instytucji do reagowania, w tym zdolność do egzekwowania sankcji i ochrony interesu publicznego.

Ustanowienie Europejskiego Urzędu ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (AMLA) należy interpretować nie tylko jako techniczną korektę reżimu compliance, ale fundamentalną przebudowę architektury bezpieczeństwa Unii Europejskiej. AMLA wprowadza bowiem do tego systemu wymiar wywiadu finansowego o charakterze systemowym, transgranicznym i analitycznym, zakotwiczony na poziomie unijnym, a nie rozproszony wyłącznie pomiędzy jurysdykcje krajowe. Jej zasadniczą funkcją nie jest zastępowanie kompetencji państw członkowskich ani ingerencja w relacje państwo–obywatel, lecz standaryzacja i integracja zdolności analitycznych całego systemu AML/CFT, rozumianego jako narzędzie prewencji bezpieczeństwa, a nie jedynie nadzoru regulacyjnego[15].

Szczególnego istotna jest rola węzła koordynującego działalność jednostek analityki finansowej (FIU). System FIU.net pełni funkcję bezpiecznego kanału wymiany informacji, zyskuje potencjał infrastruktury wspólnych analiz i wczesnego ostrzegania. Umożliwia to identyfikację anomalii, trajektorii ryzyka oraz transgranicznych sieci powiązań na etapie poprzedzającym materializację zagrożeń. Prowadzenie skoordynowanych analiz spraw o znaczeniu ponadnarodowym, przy wsparciu narzędzi informatycznych i rozwiązań opartych na sztucznej inteligencji, lokuje AMLA w logice intelligence-led security, a nie wyłącznie w roli regulatora rynku finansowego[16].

O rzeczywistej skuteczności tej zmiany decyduje jednak sposób sprzężenia warstwy wywiadu finansowego z pozostałymi elementami unijnej architektury bezpieczeństwa. W warunkach zagrożeń hybrydowych sama detekcja pozostaje niewystarczająca, jeśli nie prowadzi do przerwania łańcucha oddziaływania. Z tego względu szczególnego znaczenia nabiera relacja pomiędzy AMLA, Europolem oraz Prokuraturą Europejską (EPPO), uzupełniana perspektywą stopniowego budowania europejskiej współpracy wywiadowczej. To właśnie w tej konfiguracji ujawnia się nowa jakość instytucjonalna: zdolność zapewnienia ciągłości między identyfikacją finansowych trajektorii ryzyka, ich interpretacją operacyjną oraz skutecznym egzekwowaniem odpowiedzialności prawnej w trybie ponadnarodowym[17]. Wymaga to jednak rozróżnienia między analitycznym modelem współpracy a istniejącymi podstawami prawnymi przekazywania informacji. Sama zbieżność celów bezpieczeństwa nie stanowi jeszcze upoważnienia do swobodnego łączenia zasobów danych ani do przekazywania ich poza zakresem ustawowych zadań danej instytucji.

W tym układzie AMLA pełni funkcję węzła detekcji i standaryzacji analizy finansowej; Europol - jako centralny podmiot intelligence-led policing - osadza dane w szerszym kontekście operacyjnym przestępczości zorganizowanej, terroryzmu, cyberzagrożeń i operacji hybrydowych; natomiast EPPO domyka cykl bezpieczeństwa poprzez warstwę egzekucyjną: ściganie, konfiskatę i odzyskiwanie mienia. Obecność EPPO sprawia, że konwergencja nie ogranicza się do wymiany informacji, lecz staje się realną zdolnością do zakłócania finansowych komponentów zagrożeń podważających bezpieczeństwo Unii i integralność jej porządku prawnego. Rola EPPO naturalnie jest ograniczona jej właściwością rzeczową, związaną z przestępstwami naruszającymi szeroko rozumiane interesy finansowe Unii. Nie oznacza ona ogólnej kompetencji do

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1620 z 31 maja 2024 r. ustanawiające Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu.

[16] Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (AMLA), https://www.amla.europa.eu/.

[17] European Parliamentary Research Service, Anti-money-laundering authority (AMLA): Countering money laundering and the financing of terrorism, 2022.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

ścigania finansowania terroryzmu czy całej przestępczości finansowej. Konwergencja wymaga więc wyznaczenia punktów styku między mandatami instytucji, a nie ich utożsamiania. „Gotowość Unii" przywraca debatę o budowaniu wspólnej zdolności wywiadowczej UE. Debaty wskazują, że Europa nie jest jeszcze gotowa do stworzenia w pełni scentralizowanego „urzędu wywiadowczego" o szerokich kompetencjach operacyjnych. Różnice w kulturach prawnych, poziomach zaufania, praktykach kontrwywiadowczych oraz wrażliwość suwerenności państw członkowskich wskazują, jak słusznie zauważa A. Gruszczak, taki model przedwczesnym i potencjalnie destabilizującym[18]. Jednocześnie Unia jest już gotowa - zarówno instytucjonalnie, jak i normatywnie – do pogłębionej współpracy wywiadowczej w formule sieciowej: opartej na wspólnej analizie, agregacji danych, foresighcie i priorytetyzacji zagrożeń, bez przejmowania narodowych kompetencji w zakresie pozyskiwania informacji. Paneuropejska zdolność współpracy wywiadowczej może więc pełnić funkcję warstwy scalającej działania AMLA, Europolu i EPPO, zwiększając ich terminowość i skuteczność, bez naruszania podstaw kompetencyjnych. Sieciowy model konwergencji wywiadowczej nie musi być przy tym wyłącznie etapem poprzedzającym przyszłą centralizację. Może stanowić samodzielną formułę integracji europejskiego bezpieczeństwa, adekwatną do transgranicznego charakteru zagrożeń oraz utrzymującej się odrębności kompetencyjnej państw członkowskich. Jego wartość nie wynika z koncentracji uprawnień operacyjnych, lecz ze zdolności do wspólnej interpretacji sygnałów, wyznaczania priorytetów i skracania dystansu między rozpoznaniem ryzyka a reakcją. Warunkiem jest jednak wzajemne zaufanie, i solidarność wobec zagrożeń, bez którego nawet najbardziej zaawansowane narzędzia analityczne nie przełożą się na rzeczywistą wymianę informacji.

W tak skonstruowanej architekturze zastosowanie sztucznej inteligencji uzyskuje szczególnie silną legitymizację prawną. Analiza przepływów finansowych, identyfikacja sieci powiązań, wykrywanie anomalii, korelacja danych wielojurysdykcyjnych czy mapowanie schematów finansowania ransomware i operacji wpływu pozwalają wykorzystać potencjał AI na poziomie wzorców systemowych, a nie bezpośredniej ingerencji w sferę praw jednostki. AI pełnić więc może funkcję narzędzia skracającego dystans między informacją, analizą i decyzją, wzmacniającego prewencję i ochronę interesu publicznego, bez przechodzenia w logikę nadzoru totalnego.

Warstwa AMLA-ENISA-Europol-EPPO, uzupełniona o rozwijaną współpracę wywiadowczą, stanowi naturalną przestrzeń dla modelu AI-with-safeguards, zgodnego z AI Act oraz zasadami proporcjonalności, audytowalności i nadrzędnej odpowiedzialności człowieka. Właśnie w tym segmencie architektury bezpieczeństwa Unia Europejska posiada największy potencjał do wdrażania zaawansowanych narzędzi analitycznych w sposób, który jednocześnie wzmacnia zdolność prewencyjną i nie narusza fundamentów państwa prawa[19]. Odwołanie do AI Act wymaga przy tym uwzględnienia zakresu zastosowania rozporządzenia oraz przewidzianych w nim wyłączeń, w szczególności dotyczących określonych zastosowań w sferze bezpieczeństwa narodowego i wojskowości. Gwarancje nadzoru i odpowiedzialności powinny być analizowane również tam, gdzie konkretne zastosowanie AI pozostaje poza zakresem tego aktu.

AI Act oraz gwarancje być wdrażane jako warunki trwałości całego systemu. Nadzór człowieka, kontrola legalności, audytowalność i rozliczalność demokratyczna wyznaczają granicę pomiędzy bezpieczeństwem jako dobrem wspólnym

[18] A. Gruszczak, Unia Europejska w krainie koszmarów: Refleksje nad bezpieczeństwem europejskim w czasach niepewności, „Studia Socjologiczno-Polityczne. Seria Nowa" 2023, t. 16, nr 1, s. 13–34.
[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (AI Act).

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

a bezpieczeństwem jako mechanizmem erozji wolności. Wymaga to wypracowania spójnego modelu odpowiedzialności za decyzje wspierane przez AI, tak aby odpowiedzialność nie ulegała rozproszeniu między podmiotami technologicznymi, administracyjnymi i decyzyjnymi.

Wnioski i rekomendacje

AI wykorzystywana w bezpieczeństwie i obronności może istotnie zwiększyć zdolności prewencyjne Unii Europejskiej, usprawnić analizę ryzyka i zarządzanie kryzysowe. Jednocześnie jej wdrażanie w obszarach szczególnie wrażliwych wymaga ostrożności, zarówno ze względu na ryzyko błędów systemowych i uprzedzeń algorytmicznych, jak i konieczność zachowania zgodności z prawem UE oraz gwarancjami ochrony praw człowieka. W tym kontekście zasadne wydaje się sformułowanie kilku rekomendacji dotyczących kierunków i warunków wykorzystania AI w europejskiej architekturze bezpieczeństwa.

Po pierwsze, priorytetem powinny pozostać prewencja i zarządzanie kryzysowe, a nie automatyzacja wykonywania władzy publicznej. AI może wspierać wczesne ostrzeganie, ocenę ryzyka i koordynację reakcji, nie powinna jednak zastępować człowieka w podejmowaniu decyzji ingerujących w prawa jednostki.

Szczególnie uzasadnionym obszarem zastosowania AI wydaje się wywiad finansowy, zwłaszcza w ramach AMLA i FIU.net. Analiza przepływów finansowych, identyfikacja powiązań i wykrywanie anomalii mogą zwiększyć skuteczność przeciwdziałania finansowaniu przestępczości i terroryzmu. Wykorzystanie tych możliwości wymaga jednak odpowiednich gwarancji proceduralnych i weryfikacji wyników analiz.

Po trzecie, AI powinna wspierać ochronę infrastruktury krytycznej oraz reagowanie na zagrożenia hybrydowe, w tym sabotaż i cyberataki. Istotne pozostaje przy tym rozróżnienie między wykorzystaniem technologii do identyfikacji zagrożeń i ograniczania ich skutków a rozszerzaniem zdolności nadzorczych wobec obywateli.

Po czwarte, skuteczność zastosowań AI zależy od interoperacyjności nie tylko technicznej, lecz także instytucjonalnej i prawnej. W szczególności warto rozważyć pogłębienie współpracy AMLA, Europolu i EPPO, z uwzględnieniem kompetencji Frontexu i eu-LISA. Nie chodzi przy tym o tworzenie nowych struktur, lecz o lepsze wykorzystanie istniejących mechanizmów wymiany informacji, analizy zagrożeń i współdziałania operacyjnego. Wymaga to określenia podstaw prawnych wymiany danych, odpowiedzialności za ich jakość i dalsze wykorzystanie oraz procedur kontroli wyników wspólnych analiz. Bez tych elementów interoperacyjność może pozostać postulatem organizacyjnym, nie zaś rzeczywistą zdolnością reagowania.

Po piąte, w odniesieniu do europejskiej współpracy wywiadowczej bardziej realistycznym kierunkiem niż przedwczesna centralizacja wydaje się rozwijanie konwergencji w modelu sieciowym. Wspólne analizy, prognozowanie zagrożeń i budowanie świadomości sytuacyjnej mogą być wspierane przez AI bez konieczności przenoszenia narodowych kompetencji wywiadowczych na poziom unijny.

Ponadto wykorzystanie AI musi pozostawać zgodne z zasadami proporcjonalności, odpowiedzialności i nadzoru człowieka. Szczególne znaczenie mają możliwość audytu, weryfikacja danych i wyników analiz oraz zapewnienie skutecznych mechanizmów kontroli. AI Act, w zakresie objętym jego regulacją, nie powinien być traktowany wyłącznie jako zbiór wymogów formalnych, lecz jako element szerszego systemu gwarancji prawnych.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Ostatecznie rozwój AI w europejskim systemie bezpieczeństwa nie powinien prowadzić ani do nieuzasadnionej centralizacji kompetencji, ani do osłabienia ochrony praw podstawowych. Największy potencjał tych technologii należy upatrywać w usprawnieniu współpracy między istniejącymi instytucjami, zwiększeniu zdolności prewencyjnych i poprawie reagowania kryzysowego. Warunkiem pozostaje jednak zachowanie odpowiedzialności człowieka za decyzje oraz zaufania publicznego do instytucji odpowiedzialnych za bezpieczeństwo. Właśnie zdolność do powiązania detekcji finansowej, analizy operacyjnej i reakcji prawnej, z poszanowaniem właściwości poszczególnych organów, może stać się praktycznym sprawdzianem europejskiej gotowości. O powodzeniu tego modelu przesądzi nie liczba wdrożonych systemów AI, lecz możliwość terminowego, zgodnego z prawem wykorzystania ich wyników.

Bibliografia

Aden H., Interoperability between EU policing and migration databases: Risks for privacy, „European Public Law" 2020, t. 26.

Bergeron A., Pamar M., Paquette S., Introduction et définitions de la cybercriminalité, [w:] Cybercrimes et enjeux technologiques, Presses internationales Polytechnique 2020.

Donner C., Marcum C., Jennings W., Higgins G., Banfield J., Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy, „Computers in Human Behavior" 2014, t. 34.

Elkhova O., Ontological-societal security node as a phenomenon of the digital environment, „RUDN Journal of Philosophy" 2025, t. 29, nr 2.

Giddens A., Modernity and self-identity, Polity Press 1991.

Gill P., Phythian M., From the intelligence cycle to the web of intelligence: Complexity and the conceptualisation of intelligence, [w:] Understanding the intelligence cycle, M. Phythian (red.), Routledge 2013.

Gruszczak A., Unia Europejska w krainie koszmarów: Refleksje nad bezpieczeństwem europejskim w czasach niepewności, „Studia Socjologiczno-Polityczne. Seria Nowa" 2023, t. 16, nr 1.

Mitzen J., Ontological security in world politics, „European Journal of International Relations" 2006, t. 12, nr 3.

Perfetto M., Weaponisation of interdependence: Unpacking European ontological anxieties, „Central European Journal of International and Security Studies" 2025, t. 33.

Sheptycki J., Liquid modernity and the police métier: Thinking about information flows in police organisations, „Global Crime" 2017, t. 18, nr 3.

Słowikowski M., What does ontological security theory tell us about Russia's decision to start the war against Ukraine?, „Studia Polityczne" 2025, t. 53.

Trauner F., New kids on the CFSP block: The JHA agencies, Institute for European Studies 2011.

Warner M., The past and future of the intelligence cycle, [w:] Understanding the intelligence cycle, M. Phythian (red.), Routledge 2013.

Whelan C., Managing dynamic security networks: Towards the strategic management of cooperation, coordination and collaboration, „Security Journal" 2017, t. 30, nr 1.

Zarychta-Romanowska K., Border intelligence cooperation in the time of COVID-19: Omnifarious dimensions of EU security strategies, „Journal of European and American Intelligence Studies" 2021.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Zarychta-Romanowska K., Creating an EU homeland security: Examining the potential of EBCGA and EPPO cooperation in countering terrorist and criminal financing, [w:] Countering terrorist and criminal financing, S. Romaniuk, C. Kaunert, A.P.H. Fabe (red.), Routledge 2022.

Zarychta-Romanowska K., Foreign fighters as a threat to Polish security and sovereignty, „Revista Facultății de Drept Oradea" 2019, nr 1.

Zarychta-Romanowska K., Strengthening urban security in Europe: EU policies, law enforcement, and emerging technologies for resilience and disaster response, [w:] AI, Blockchain and Social Network on Urban Crisis Management: Leveraging Emerging Technologies for Disaster Response and Resilience in Smart Cities, P.K. Dutta i in. (red.), „Advances in Computers" 2026, t. 142.

Zarychta-Romanowska K., Szostak M., Bocko P., Creating Captain Europe: Defining innovative skills necessary for modern border intelligence and investigation, [w:] Countering terrorist and criminal financing, S. Romaniuk, C. Kaunert, A.P.H. Fabe (red.), Routledge 2022.

Zarychta-Romanowska K., Szostak M., Frontex 3.0 - rewolucyjny czy rewelacyjny?, „Nowa Kodyfikacja Prawa Karnego" 2018, t. 50.