Doktryna aktywnego odstraszania cyfrowego i zabezpieczenia sztucznej inteligencji w ramach WPBiO

Oliwier Stefański · sierpień 2026

STRESZCZENIE I GŁÓWNA TEZA

Wojna Rosji przeciwko Ukrainie pokazała, że cyberataki, operacje informacyjne oraz celowe zakłócanie infrastruktury krytycznej stały się stałym elementem współczesnych konfliktów hybrydowych. Dla Unii Europejskiej oznacza to, że cyberbezpieczeństwo nie może być dłużej traktowane wyłącznie jako sprawa administracyjna i cywilna – wymaga pilnej integracji z wymiarem wojskowym w ramach Wspólnej Polityki Bezpieczeństwa i Obrony (WPBiO).

Niniejszy brief stawia tezę, że UE musi wypracować dwutorową doktrynę cyberobrony. Pierwszy filar to aktywne odstraszanie cyfrowe – zdolność do wykrywania, przypisywania sprawcom i odpierania cyberataków oraz podejmowania wobec nich proporcjonalnych działań. Drugi filar to odporność technologiczna (podejście pasywne) – stała synergia struktur cywilno-wojskowych, rygorystyczne zabezpieczanie systemów opartych na sztucznej inteligencji oraz bliska współpraca z NATO, które razem zmniejszają skuteczność i opłacalność ataków cyfrowych dla agresora.

Bez zdecydowanych kroków instytucjonalnych Unia Europejska pozostanie bezbronna wobec asymetrycznych zagrożeń wymierzonych w misje cywilne i operacje wojskowe prowadzone w ramach WPBiO.

GŁÓWNA REKOMENDACJA:

Utworzenie w strukturze Sztabu Wojskowego UE (EUMS) stałego centrum koordynacji cyberobrony dla misji WPBiO, doprecyzowanie pełnego spektrum unijnego mechanizmu odpowiedzi na cyberataki wymierzone w misje i operacje oraz uruchomienie unijnego programu testowania bezpiecznych modeli AI na potrzeby obronne.

KONTEKST I SFORMUŁOWANIE PROBLEMU

Architektura bezpieczeństwa europejskiego znajduje się pod bezprecedensową presją działań hybrydowych prowadzonych przez aktorów państwowych oraz powiązane z nimi grupy APT (Advanced Persistent Threat). Cyberprzestrzeń stała się pełnoprawnym teatrem działań wojennych, w którym granica między pokojem, kryzysem i otwartym konfliktem się zatarła. Wojna Federacji Rosyjskiej przeciwko

Ukrainie pokazała, że ataki na cyfrowe sieci dowodzenia, systemy logistyczne, energetykę i łączność satelitarną są równie niszczące, co klasyczne środki rażenia.

UE podjęła w ostatnich latach istotne kroki legislacyjne. Cyber Solidarity Act (Rozporządzenie UE 2025/38), który wszedł w życie w lutym 2025 r., wzmocnił zdolności państw członkowskich do wykrywania zagrożeń, przygotowania i skoordynowanego reagowania na incydenty na dużą skalę. Regulacja ta rozwija Wspólny Komunikat Komisji Europejskiej i Wysokiego Przedstawiciela z 2022 r. w sprawie unijnej polityki cyberobrony oraz Konkluzje Rady UE z maja 2023 r.

Mimo osiągnięć w unijnej architekturze bezpieczeństwa dalej utrzymuje się głęboka asymetria. Tworzone na poziomie unijnym instrumenty koncentrują się głównie na sektorze cywilnym, rynku wewnętrznym i administracji publicznej, podczas gdy misje WPBiO wciąż mają niewystarczający poziom integracji technologii cyfrowych z działaniami wojskowymi. Misje te, rozmieszczane często w niestabilnych regionach sąsiedztwa UE, stają się poligonem doświadczalnym dla cyberataków wymierzonych w poufność, integralność i dostępność krytycznych danych operacyjnych. Jednocześnie UE nie wypracowała dotąd spójnego mechanizmu reagowania na zidentyfikowanych sprawców tych ataków, co istotnie ogranicza jej zdolność do odstraszania.

Sytuację komplikuje szybki rozwój systemów opartych na sztucznej inteligencji (AI). Algorytmy uczenia maszynowego przyspieszają analizę danych rozpoznawczych i automatyzację logistyki, ale niosą też poważne ryzyka systemowe. Cyberprzestępcy wykorzystują takie narzędzia do automatyzacji skanowania podatności, generowania kampanii dezinformacyjnych oraz ataków na algorytmiczne systemy wsparcia decyzji dowódczych. Zagrożone są więc nie tylko łącza komunikacyjne, ale sam proces podejmowania decyzji przez UE.

ANALIZA

DWA UZUPEŁNIAJĄCE SIĘ TORY

Odporność (resilience) polega na zabezpieczeniu własnych systemów tak, by atak się nie powiódł lub jego skutki były minimalne. Odstraszanie (deterrence) polega na tym, że sprawca ponosi realne konsekwencje po ataku – dyplomatyczne, gospodarcze lub prawne – co z góry obniża jego opłacalność. Trzy poniższe podrozdziały pokazują, gdzie UE ma braki w obu wymiarach.

l. Rozdźwięk między cyberbezpieczeństwem cywilnym i wojskowym

Podstawową słabością dotychczasowego podejścia UE jest rozdzielenie instytucjonalne i kompetencyjne. Z jednej strony funkcjonują agencje cywilne, takie jak ENISA czy CERT-EU, które sprawnie obsługują incydenty w administracji unijnej i państwach członkowskich. Z drugiej strony komponent

wojskowy – osadzony w strukturach Europejskiej Służby Działań Zewnętrznych (ESDZ), Sztabu Wojskowego UE (EUMS) oraz Dowództwa Planowania i Prowadzenia Operacji Wojskowych (MPCC) – pozostaje odizolowany, działając w odrębnych reżimach prawnych i pod rygorem narodowej suwerenności nad zasobami obronnymi.

Ten podział opóźnia przepływ informacji o zagrożeniach. W cyberkonflikcie, gdzie cykl decyzyjny napastnika liczy się w sekundach, bariery biurokratyczne oraz brak wspólnych procedur wymiany informacji niejawnych uniemożliwiają skuteczną obronę prewencyjną, w tym odstraszanie. Cyberobrona musi zatem stać się pełnoprawnym, zintegrowanym komponentem operacyjnym, zdolnym do natychmiastowej atrybucji i reakcji w czasie rzeczywistym.

2. Sztuczna inteligencja jako katalizator zagrożeń

Wdrożenie AI do środowiska cyfrowego zmienia bilans sił na korzyść agresora. Tradycyjne metody audytu bezpieczeństwa nie nadążają za dynamiką zagrożeń napędzanych przez AI. Grupy przestępcze i sponsorowane przez państwa wykorzystują modele generatywne do tworzenia wektorów ataku, które adaptują się w czasie rzeczywistym do wykrywanych zabezpieczeń.

Dla misji WPBiO szczególnie groźne są trzy kategorie podatności. Po pierwsze, celowe zatruwanie danych treningowych (data poisoning) na etapie budowania modeli systemów rozpoznania obrazowego, prowadzi do fałszywego odczytu sytuacji taktycznej. Po drugie, ataki kontradyktoryjne (adversarial machine learning) na etapie operacyjnym – subtelne, niewidoczne dla człowieka zmiany w danych wejściowych – mogą sparaliżować lub oszukać algorytmy klasyfikacji obiektów. Po trzecie, wyciek parametrów modeli AI grozi skompromitowaniem całych systemów wsparcia logistycznego. UE musi odejść od bezkrytycznego wdrażania AI na rzecz rygorystycznego paradygmatu bezpiecznej sztucznej inteligencji (trustworthy AI in defence).

3. Podział ról i współpraca z NATO

Relacje między UE a NATO w obszarze cyberobrony nadal pozostają jednym z wyzwań. Obie organizacje mają w dużej mierze tych samych członków, co grozi duplikowaniem wysiłków, nieefektywnym wykorzystaniem zasobów i niespójnymi standardami. Deklaracje o współpracy podkreślają komplementarność, ale brak precyzyjnego podziału zadań prowadzi do tarć instytucjonalnych.

Rozwiązaniem jest wyraźne rozgraniczenie kompetencji przy jednoczesnym zwiększaniu interoperacyjności. NATO, dysponujące potencjałem odstraszania kolektywnego, powinno koncentrować się na zagrożeniach cybernetycznych o znaczeniu strategicznym. UE powinna wziąć odpowiedzialność za ochronę

własnych misji w ramach WPBiO, odporność łańcuchów dostaw sektora obronnego oraz harmonizację unijnych standardów odporności cybernetycznej oraz – co kluczowe dla odstraszania – za własny, autonomiczny mechanizm reakcji politycznej na ataki wymierzone w jej misje, którego NATO z definicji nie obejmuje. Kluczem do sukcesu może być bieżąca wymiana doświadczeń w ramach platform takich jak Europejskie Centrum Kompetencji ds. Cyberbezpieczeństwa.

REKOMENDACJE

1. Rada Europejska oraz Wysoki Przedstawiciel UE ds. Zagranicznych i Polityki Bezpieczeństwa powinni podjąć decyzję o powołaniu w strukturze EUMS stałej komórki operacyjnej Centrum Koordynacji Cyberobrony WPBiO. Jej zadaniem będzie monitorowanie zagrożeń cyfrowych wymierzonych w misje operacyjne, wstępna atrybucja incydentów oraz zapewnienie bezpiecznego kanału wymiany informacji między dowództwami operacyjnymi a narodowymi centrami reagowania.

2. Komisja Europejska, Dyrekcja Generalna ds. Przemysłu Obronnego i Przestrzeni Kosmicznej (DG DEFIS) oraz Europejska Agencja Obrony (EDA) powinny uruchomić wieloletni program badawczo-wdrożeniowy dedykowany testowaniu i certyfikacji bezpiecznych modeli AI na potrzeby obronne. Program powinien objąć audyt algorytmów stosowanych w systemach C5ISR pod kątem odporności na zatruwanie danych, ataki kontradyktoryjne oraz manipulacje zewnętrzne.

3. **Rada Unii Europejskiej** powinna doprecyzować kryteria polityczne, progi dowodowe atrybucji i ścieżki decyzyjne uruchamiania wspólnej odpowiedzi dyplomatycznej na zmasowane cyberataki hybrydowe (cyber diplomacy toolbox), włączając do nich odniesienia

do ataków na infrastrukturę krytyczną misji WPBiO oraz zakłóceń łańcuchów dostaw technologii obronnych, które otrzymają odrębną kategorię kwalifikującą do reżimu sankcji. Rada UE powinna ponadto rozważyć włączenie do tego reżimu opcji skoordynowanej reakcji ofensywnej, realizowanej przez zdolności cybernetyczne zainteresowanych państw członkowskich na zasadzie koalicji chętnych (coalition of the willing), analogicznie do mechanizmów już stosowanych w ramach PESCO.

Rząd Rzeczypospolitej Polskiej powinien zgłosić w ramach mechanizmu Stałej Współpracy Strukturalnej (PESCO) projekt utworzenia Wschodnioeuropejskiego Centrum Doskonałości Cyberodporności i Bezpieczeństwa AI dla Misji i Operacji. Ośrodek, oparty na kompetencjach Wojsk Obrony Cyberprzestrzeni oraz krajowych zespołów CSIRT, mógłby pełnić funkcję regionalnego hubu testowego, szkoleniowego i analitycznego, wzmacniając pozycję Polski jako lidera cyberbezpieczeństwa na wschodniej flance UE. 4.

KONKLUZJA

Bezpieczeństwo cyfrowe przestało być technicznym detalem polityki zagranicznej – stało się jej filarem. Żeby Unia Europejska mogła skutecznie chronić i realizować cele misji i operacji w ramach WPBiO oraz budować silną pozycję na świecie, musi odejść od dotychczasowej praktyki reagowania doraźnego, zależnej od decyzji pojedynczych stolic.

Okno na zmiany powoli się zamyka – najbliższe dwa, trzy lata zadecydują o tym, jak będą wyglądać globalne standardy cyfrowe, jak i architektura nowych zależności. Tylko spójne połączenie aktywnej cyberobrony, bezpiecznych algorytmów AI i bliskiej relacji z NATO da UE szansę na zapewnienie sobie strategicznej suwerenności w XXI wieku.

BIBLIOGRAFIA

RAMY OGÓLNE POLITYKI CYBEROBRONY UE

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2022). Joint communication to the European Parliament and the Council: EU Policy on Cyber Defence (JOIN(2022) 49 final, CELEX 52022JC0049).

Council of the European Union. (2023). Council conclusions on the EU Policy on Cyber Defence (ST 09618/23).

ODPORNOŚĆ TECHNOLOGICZNA I CYBER SOLIDARITY ACT

European Parliament and the Council of the European Union. (2024). Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act).

European Commission. (2025, February 4). EU Cyber Solidarity Act. Shaping Europe's digital future.

European Parliamentary Research Service. (2023). Cyber solidarity act: Strengthening cybersecurity capabilities across the Union (EPRS Briefing PE 754.614).

AKTYWNE ODSTRASZANIE: SANKCJE, ATRYBUCJA, ZDOLNOŚCI OPERACYJNE

Council of the European Union. (2017). Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

Miadzvetskaya, Y., & Wessel, R. A. (2022). The externalisation of the EU's cybersecurity regime: The Cyber Diplomacy Toolbox. European Papers, 7(1).

Permanent Structured Cooperation (PESCO). (2018). Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT).

LITERATURA TEORETYCZNA I ANALITYCZNA

Fiott, D. (2017). The cybridisation of EU defence. ISSues, (24). European Union Institute for Security Studies.

Pawlak, P., & Delerue, F. (Eds.). (2022). A language of power? Cyber defence in the European Union (Chaillot Paper No. 176). European Union Institute for Security Studies.