Pulaski Policy Papers

Komentarz Międzynarodowy Pułaskiego ISSN 2080-8852 Warszawa, 28.05.2026

Autorzy: Eto Buziashvili, Kamil Basaj, Wojciech Dziegiel, Agnieszka Grzegorzewska

Operacjonalizacja na pierwszej linii konfrontacji: Kraje B5 + Ukraina jako północno-wschodni korytarz odporności demokratycznej

Budowanie odporności społecznej i demokratycznej w krajach Morza Bałtyckiego

Streszczenie wykonawcze

Współczesne zagrożenia hybrydowe, w szczególności zagraniczne manipulacje i ingerencje informacyjne (*Foreign Information Manipulation and Interference*; FIMI), stały się trwałym elementem środowiska bezpieczeństwa Europy. W tym kontekście państwa B5, do których należą Litwa, Łotwa, Estonia, Finlandia i Polska, oraz Ukraina, ze względu na bezpośrednią ekspozycję na działania destabilizacyjne wykształciły praktyczne mechanizmy reagowania, które mogą stanowić fundament operacyjny dla rozwoju Europejskiej Tarczy Demokracji (*European Democracy Shield*; EUDS).

Europejska Tarcza Demokracji stanowi centralny element rozwijanej przez Unię Europejską architektury ochrony integralności demokratycznej. Jej założeniem jest stworzenie trwałego systemu koordynacji politycznej, regulacyjnej i operacyjnej w odpowiedzi na zagrożenia informacyjne, cybernetyczne i hybrydowe. Konstrukcja EUDS opiera się na czterech wzajemnie powiązanych filarach operacyjnych - utworzeniu Europejskiego Centrum Odporności Demokratycznej (ECDR), ochronie przestrzeni informacyjnej, wzmacnianiu instytucji i mediów, oraz zwiększaniu odporności społecznej.

Pomimo rozwoju ram, programów i inicjatyw skierowanych na przeciwdziałanie FIMI i budowaniu odporności demokratycznej, wskazuje się na utrzymującą się lukę operacyjną pomiędzy rosnącą zdolnością do wykrywania i analizowania zagrożeń informacyjnych a możliwością szybkiego, skoordynowanego reagowania. Problem ten wynika przede

wszystkim z rozproszenia kompetencji, niewystarczającej synchronizacji działań między państwami i sektorami oraz ograniczeń utrudniających rozwój zasobów technologicznych i eksperckich. Operacjonalizacja odporności demokratycznej nie wymaga zatem tworzenia całkowicie nowych struktur, lecz skuteczniejszego połączenia istniejących instrumentów w jeden spójny system działania. Kluczowe znaczenie ma w tym zakresie sprawny przepływ informacji, standaryzacja procedur reagowania, rozwój mierzalnych wskaźników skuteczności oraz budowanie społecznej legitymizacji podejmowanych działań.

Perspektywa regionalna państw B5+ oraz doświadczenia Polski i Ukrainy jako krajów znajdujących się na pierwszej linii oddziaływania zagrożeń hybrydowych i operacji informacyjnych są szczególnie ważne w tym kontekście. Państwa regionu Morza Bałtyckiego stopniowo wykształciły modele odporności oparte na współpracy administracji publicznej, społeczeństwa obywatelskiego, środowiska eksperckiego, mediów oraz sektora prywatnego. Szczególne znaczenie ma także doświadczenie Ukrainy, której praktyka funkcjonowania w warunkach pełnoskalowej wojny dostarczyła unikalnych kompetencji w zakresie przeciwdziałania operacjom wpływu, utrzymywania odporności społecznej oraz szybkiego reagowania na manipulacje informacyjne. Z kolei Polska, jako kluczowe państwo wschodniej flanki NATO i UE, pozostaje celem intensywnych kampanii dezinformacyjnych mających na celu osłabienie spójności społecznej i podważenie poparcia dla działań pomocowych. Skuteczna operacjonalizacja odporności demokratycznej wymaga nie tyle tworzenia nowych instytucji, ile lepszej koordynacji istniejących mechanizmów oraz skrócenia ścieżki między identyfikacją zagrożenia a reakcją instytucjonalną. Doświadczenia Polski i Ukrainy pokazują jednocześnie, że skuteczna obrona przestrzeni informacyjnej wymaga połączenia działań państwa z aktywnością społeczeństwa obywatelskiego, niezależnych mediów, środowisk eksperckich oraz sektora prywatnego. Tak zaimplementowany model "*whole-of-society*" pozwala przejść od reaktywnego zwalczania dezinformacji do budowy długofalowej odporności społecznej i demokratycznej

Kluczowe rekomendacje:

- Utworzenie stałych ram koordynacji operacyjnej B5+ w zakresie FIMI.
- Integracja doświadczeń regionu frontowego z rozwojem operacyjnym Europejskiej Tarczy Demokracji.
- Wzmocnienie współpracy operacyjnej między administracją publiczną, społeczeństwem obywatelskim, platformami i środowiskami badawczymi.
- Rozwój regionalnego modelu odporności społecznej opartego na podejściu „*whole-of-society*" i zaangażowaniu międzysektorowym, zwłaszcza przedsiębiorstw.
- Wzmocnienie przygotowania na manipulację informacyjną wspieraną przez sztuczną inteligencję.

Rekomendacje

1. **Utworzenie stałych ram koordynacji operacyjnej B5+ w zakresie FIMI.**

   Państwa B5, wraz z Ukrainą, powinny opracować ustrukturyzowane regionalne ramy koordynacji operacyjnej ukierunkowane na współpracę w zakresie przeciwdziałania FIMI oraz zagrożeniom hybrydowym. Mechanizm ten powinien wspierać wspólne oceny zagrożeń, zintegrowane procedury wczesnego ostrzegania, transgraniczną wymianę informacji, skoordynowane działania prebunkingowe oraz regionalne ćwiczenia dotyczące wrogich operacji informacyjnych wymierzonych w spójność sojuszniczą.

2. **Integracja doświadczeń region frontowego z rozwojem operacyjnym Europejskiej Tarczy Demokracji.**

   Doświadczenia operacyjne zgromadzone w regionie B5 i Ukrainie powinny zostać systematycznie włączone do dalszego rozwoju Europejskiej Tarczy Demokracji oraz powiązanych inicjatyw UE w zakresie odporności. Celem powinno być skalowanie adaptowalnych praktyk operacyjnych, które zostały już przetestowane w warunkach długotrwałej presji i mogą wzmocnić zdolność wdrożeniową unijnych ram politycznych.

3. **Wzmocnienie współpracy operacyjnej między administracją publiczną, społeczeństwem obywatelskim, platformami i środowiskami badawczymi.**

   Skuteczne przeciwdziałanie FIMI wymaga szybszych i bardziej niezawodnych ścieżek prowadzących od wykrycia zagrożenia do podjęcia działania. Podmioty unijne i regionalne powinny wzmacniać mechanizmy umożliwiające współpracę operacyjną ponad granicami instytucjonalnymi i sektorowymi. Priorytetem powinno być zapewnienie, aby ustalenia analityczne były konsekwentnie przekładane na działania komunikacyjne, regulacyjne, prawne lub egzekucyjne w różnych jurysdykcjach.

4. **Rozwój regionalnego modelu odporności społecznej opartego na podejściu "*whole-of-society*" i zaangażowaniu międzysektorowym, zwłaszcza przedsiębiorstw**

   1. Długoterminowa odporność zależy nie tylko od zdolności instytucjonalnych, lecz także od umiejętności społeczeństw do rozpoznawania, kontekstualizowania i

adaptowania się do zmieniających się form manipulacji. Region B5+ powinien zatem rozwijać współpracę w zakresie edukacji medialnej i cyfrowej, zaangażowania młodzieży, wsparcia niezależnych mediów oraz inicjatyw odpornościowych realizowanych przez społeczeństwo obywatelskie. Aby rozwijać taki model odporności społecznej, niezbędne jest zaangażowanie międzysektorowe, w tym sektora biznesowego, umożliwiające mobilizację zasobów, kompetencji i kanałów komunikacji kluczowych do implementacji podejścia "*whole-of-society*". Praktyka państw B5 potwierdza skuteczność takiego modelu, którego operacjonalizacja jest kluczowym obszarem do rozwoju odporności. Współpraca z sektorem biznesowym jest istotnym komponentem dla wszystkich interesariuszy, w tym dla aparatu państwa.

5. **Wzmocnienie przygotowania na manipulację informacyjną wspieraną przez sztuczną inteligencję**

Szybki rozwój treści generowanych przez AI oraz mechanizmów algorytmicznego wzmacniania przekazu wymaga bardziej skoordynowanej odpowiedzi regionalnej i europejskiej. Region B5+ powinien wspierać wspólne monitorowanie technik manipulacji opartych na AI, pogłębianie współpracy z platformami w zakresie wykrywania i eskalacji treści syntetycznych oraz rozwój zabezpieczeń przeciwdziałających manipulacji systemami AI i ich zbiorami danych.

Wprowadzenie

O seminarium

Niniejszy policy paper został opracowany w oparciu o dyskusje przeprowadzoną podczas seminarium zorganizowanego przez Fundację im. Kazimierza Pułaskiego we współpracy z Fundacją PZU oraz Ambasadą Rzeczypospolitej Polskiej w Helsinkach, pod patronatem polskiej Prezydencji w Radzie Państw Morza Bałtyckiego.

Punktem wyjścia seminarium była teza, że choć Europejska Tarcza Demokracji (*European Democracy Shield*; EUDS)[1] stała się jednym z kluczowych filarów polityki Unii Europejskiej, jej rzeczywista skuteczność powinna opierać się na inicjatywach i działaniach określonej grupy państw. EUDS, w formie kompleksowych ram politycznych i prawnych, ma na celu wzmocnić integralność sfery informacyjnej, w tym przeciwdziałać zagrożeniom hybrydowym, dezinformacji oraz zagranicznej manipulacji i ingerencji informacyjnej (FIMI), wspierać instytucje demokratyczne, a także wzmacniać odporność społeczną i zaangażowanie obywatelskie[2]. Jednak to państwa B5 - Estonia, Łotwa, Litwa, Finlandia i Polska - od lat pozostają najbardziej aktywnymi architektami obrony demokracji, często działając szybciej i bardziej zdecydowanie niż administracja europejska.

Seminarium „Budowanie odporności społecznej i demokratycznej w krajach Morza Bałtyckiego" zgromadziło przedstawicieli środowisk eksperckich z całego regionu B5 oraz Ukrainy. Wskazana konstrukcja podkreśla istotną zmianę w postrzeganiu „operacjonalizacji bezpieczeństwa na pierwszej linii konfrontacji", w ramach której kraje te pełnią funkcję północno-wschodniego korytarza odporności demokratycznej.

Przyjęcie formatu B5+Ukraina opiera się na konieczności przyjęcia podejścia „*whole-of-society*", którego znaczenie Europa dopiero zaczyna w pełni dostrzegać. Choć instytucje Unii Europejskiej stworzyły ramy dla wspólnego działania, to właśnie państwa "przyfrontowe" wypracowały rzeczywiste techniczne i społeczne mechanizmy odporności niezbędne do przetrwania. Włączenie bezprecedensowego doświadczenia Ukrainy w neutralizowaniu intensywnych operacji zagranicznych manipulacji informacjami i ingerencjami w informacje (FIMI) tworzy w ramach tego korytarza unikalną synergię sprawdzonego *know-how* oraz zdolności adaptacji. Doświadczenia tych

państw przyczyniają się do kształtowania standardów na poziomie UE oraz do budowy skutecznych odpowiedzi instytucjonalnych.

W tym kontekście grupa B5+Ukraina pełni funkcję motoru operacyjnego regionu. Ciągła presja wywierana na państwa przyfrontowe wymusiła na nich przejście od polityki o charakterze wyłącznie teoretycznym do stanu permanentnej gotowości, czyniąc je naturalnymi liderami w zakresie bezpieczeństwa regionu Morza Bałtyckiego. Celem seminarium była m.in. analiza tego doświadczenia w poszukiwaniu najlepszych rozwiązań operacjonalizacji rozwiązań w walce z opisywanymi zagrożeniami.

Dlaczego B5+

Koncepcja B5 stanowi zmianę w podejściu do europejskiej architektury bezpieczeństwa, przesuwając środek ciężkości z tradycyjnego centrum kontynentu ku północno-wschodniemu korytarzowi odporności demokratycznej.

Grupa obejmująca Estonię, Łotwę, Litwę, Finlandię i Polskę została poszerzona o państwo posiadające najbardziej bezpośrednie doświadczenie funkcjonowania w warunkach wojennych, Ukrainę, tworząc format B5+Ukraina. Państwa te, funkcjonujące w warunkach permanentnego zagrożenia, stały się głównym laboratorium przeciwdziałania współczesnej wojnie hybrydowej - od systemowego zakłócania sygnału GPS po zaawansowane kampanie

FIMI, których celem jest osłabianie spójności społecznej. Włączenie Ukrainy ma charakter nie tylko symboliczny, lecz przede wszystkim operacyjny. Jej bezpośrednie doświadczenia w identyfikowaniu i neutralizowaniu intensywnych kampanii dezinformacyjnych oraz zagrożeń hybrydowych stanowią bezprecedensowy punkt odniesienia dla pozostałych państw europejskich.

Bliskość zagrożenia sprawia, że korytarz B5+Ukraina mógłby pełnić **funkcję operacyjnego motoru Europejskiej Tarczy Demokracji**. Państwa te funkcjonują w logice wysokiej gotowości operacyjnej wynikającej z konieczności egzystencjalnej. Skutecznie przekuwają one doświadczenie bezpośredniego zagrożenia w praktyczne mechanizmy i procedury obronne. Integracja unikalnych doświadczeń Ukrainy w zakresie przeciwdziałania wojnie kognitywnej z mechanizmami B5+ może nadać Europejskiej Tarczy Demokracji wysoki poziom dynamiki operacyjnej, wzmacniając tym samym bezpieczeństwo całej wspólnoty.

Operacjonalizacja: w kierunku funkcjonalnego modelu reagowania

W ciągu ostatniej dekady poczyniono znaczące postępy w zakresie identyfikowania i analizowania zagranicznych manipulacji i ingerencji informacyjnej (FIMI). Postęp ten ujawnił jednak trwałą rozbieżność: zdolność do wykrywania i analizowania FIMI rozwija się szybciej niż zdolność do systemowego i skoordynowanego przeciwdziałania temu zjawisku.

Różnica między możliwościami identyfikacji a możliwościami działania definiuje obecne mechanizmy reagowania. Pomimo ustanowienia przez Unię Europejską oraz część jej państw członkowskich ram i programów przeciwdziałania FIMI, I, takich jak EUvsDisinfo, FIMI Toolbox, czy legislacji w postaci Digital Services Act (DSA), Artificial Intelligence Act (AI Act) czy Defence of Democracy Package 2023, wyzwaniem pozostaje szybkie i skoordynowane reagowanie na tego rodzaju zagrożenia. Powstała w ten sposób luka operacyjna oznacza rozbieżność między strategicznymi deklaracjami a rzeczywistą zdolnością ich realizacji, zarówno w zakresie zakłócania działań przeciwnika[3], jak i wzmacniania odporności społecznej.

W tym kontekście termin „**operacjonalizacja**" odnosi się do budowy możliwości operacyjnych i wykonawczych, oraz zdolności funkcjonowania w środowisku charakteryzującym się szybkością zmian i nieprzewidywalnością przeciwnika. W swojej istocie operacjonalizacja oznacza przekształcanie ram strategicznych i zobowiązań normatywnych w skoordynowane, powtarzalne i mierzalne działania.

Środowisko zagrożeń FIMI ma charakter transnarodowy i jest silnie uwarunkowane technologicznie, wykraczając poza granice jurysdykcji prawnych, kompetencji instytucjonalnych oraz poszczególnych obszarów życia społecznego. W takich warunkach operacjonalizacja nie może opierać się wyłącznie na tradycyjnych, liniowych mechanizmach wdrażania polityk ani na hierarchicznych strukturach działania „odgórnego". Wymaga ona rozproszonego i zintegrowanego modelu działania obejmującego całe społeczeństwo, łączącego instytucje państwowe, organizacje społeczeństwa obywatelskiego, niezależne media oraz podmioty sektora prywatnego.

Na poziomie UE i NATO istnieją już rozbudowane ramy przeciwdziałania FIMI[4]. Kluczowym problemem nie jest więc brak narzędzi czy struktur, lecz brak ich systematycznego i skoordynowanego wykorzystania. Pomimo funkcjonujących instrumentów prawnych,

mechanizmów regulacyjnych, zdolności analitycznych i strategii komunikacyjnych, nadal brakuje struktur integrujących te elementy w sposób umożliwiający systematyczne i powtarzalne przekształcanie identyfikacji zagrożeń w działania, a działań w trwałe efekty.

Operacjonalizacja powinna umożliwiać rozwój następujących zdolności:

- **Koordynację** – sprawny przepływ informacji i odpowiedzialności między instytucjami oraz sektorami, także ponad granicami państw;
- **Powtarzalność** – standaryzację reakcji, ich skalowalność oraz konsekwentne stosowanie ich w różnych sytuacjach;
- **Mierzalność** - tworzenie jasnych wskaźników skuteczności, obejmujących zarówno efektywność działań zakłócających, jak i wzrost odporności społecznej;
- **Adaptacyjność** – zdolność system do reagowania na ewoluujące taktyki przeciwnika i zmiany technologiczne;
- **Legitymizację społeczną** - zapewnienie, że podejmowane działania są postrzegane jako wiarygodne, przejrzyste i godne zaufania, co ogranicza podatność na manipulację

W ramach modelu operacjonalizacji wyodrębniają się dwa powiązane ze sobą wymiary działania: **odporność** oraz **zakłócanie**. Reprezentują one komplementarne logiki operacyjne funkcjonujące w ramach jednego systemu.

Zakłócanie koncentruje się na zdolności oddziaływania na infrastrukturę FIMI. Kampanie manipulacji informacyjnej opierają się na sieciach finansowania, kanałach dystrybucji oraz podmiotach pośredniczących. Elementy te mogą być identyfikowane i neutralizowane przy wykorzystaniu istniejących narzędzi prawnych, regulacyjnych i technicznych. Operacjonalizacja w tym wymiarze wymaga systematycznego wykorzystywania tych instrumentów w celu ograniczania zdolności przeciwnika do prowadzenia działań manipulacyjnych.

Operacjonalizacja musi jednak obejmować również czynniki warunkujące skuteczność FIMI. Odporne środowisko informacyjne ogranicza efektywność manipulacji poprzez zmniejszanie jej wpływu na percepcję i zachowania społeczne. Odporności nie można jednak traktować jako biernej cechy społeczeństwa. Jej operacjonalizacja oznacza aktywne kształtowanie środowiska informacyjnego poprzez odpowiednie polityki publiczne,

edukację, komunikację strategiczną oraz praktyki instytucjonalne. W ten sposób działania zakłócające ograniczają ekspozycję społeczeństw na manipulację, natomiast odporność zmniejsza jej skutki tam, gdzie mimo wszystko dochodzi do oddziaływania.

Skuteczność tego modelu zależy ostatecznie od wdrożenia podejścia obejmującego całe społeczeństwo („*whole-of-society*"). Wymaga to integracji zróżnicowanych aktorów w ramach systemu posiadającego jasno określone role, wspólne procedury oraz zaufane kanały współpracy.

Obejmuje to między innymi:

- Zinstytucjonalizowane mechanizmy koordynacji zapewniające przepływ informacji od momentu wykrycia zagrożenia do reakcji;
- Wspólne standardy wymiany danych i atrybucji, umożliwiające interoperacyjność między podmiotami o różnych kompetencjach;
- Struktury oparte na zaufaniu, pozwalające na trwałą współpracę między instytucjami publicznymi, społeczeństwem obywatelskim i sektorem prywatnym;
- Przejrzyste praktyki komunikacyjne, wzmacniające wiarygodność oraz zaufanie społeczne wobec podejmowanych działań.

W tym modelu skuteczność zależy od spójności systemu, elastyczności jego działania oraz dostępu do odpowiednich informacji. Organizacje społeczeństwa obywatelskiego często pełnią funkcję wczesnych detektorów nowych działań FIMI, podczas gdy instytucje państwowe dysponują kompetencjami wykonawczymi. Operacjonalizacja polega na połączeniu tych funkcji w jeden ciągły i trwały proces działania.

W kontekście FIMI operacjonalizacja oznacza przede wszystkim skuteczne wykorzystanie istniejących zasobów i mechanizmów. Nie polega ona na tworzeniu nowych ram działania, lecz na zapewnieniu, że istniejące już instrumenty funkcjonują jako zintegrowany system. Oznacza to zniwelowanie luki między wiedzą a działaniem, dostosowanie narzędzi do procesów operacyjnych oraz umożliwienie skoordynowanych reakcji w tempie odpowiadającym dynamice współczesnego środowiska zagrożeń.

Europejska Tarcza Demokracji – B5+ jako „silnik operacyjny"

Analiza inicjatyw instytucjonalnych UE i rozwoju Europejskiej Tarczy Demokracji (EDS)

Europejska Tarcza Demokracji (*European Democracy Shield*; EUDS) stanowi strategiczną kulminację wieloletnich wysiłków instytucjonalnych Unii Europejskiej na rzecz ochrony integralności demokracji przed podwójną presją: wewnętrzną niestabilnością oraz zewnętrznymi zagrożeniami hybrydowymi, w szczególności zagranicznymi manipulacjami i ingerencjami w informację (FIMI) [5]. EUDS funkcjonuje jako kompleksowa, paneuropejska „architektura legislacyjna", oparta na fundamentach Europejskiego Planu Działania na rzecz Demokracji z 2020 roku[6] oraz Pakietu Obrony Demokracji z 2023 roku[7]. Po wyborach do Parlamentu Europejskiego w 2024 roku przewodnicząca Komisji Europejskiej Ursula von der Leyen nadała tym rozwijającym się strategiom scentralizowaną strukturę[8], co zostało dodatkowo utrwalone poprzez powołanie Specjalnej Komisji ds. Europejskiej Tarczy Demokracji (EDS)[9] w Parlamencie Europejskim oraz przyjęcie wspólnego komunikatu pod koniec 2025 roku[10].

Realizacja EUDS opiera się na czterech filarach, które stanowią praktyczną wersję systemu „*whole-of-society*" w zakresie obrony demokracji. Pierwszym z nich jest Europejskie Centrum Odporności Demokratycznej, które ma pełnić rolę operacyjnego rdzenia systemu poprzez łączenie zasobów w celu wykrywania i reagowania na zagrożenia. Uzupełniają je działania na rzecz ochrony przestrzeni informacyjnej, takie jak egzekwowanie Aktu o usługach cyfrowych (DSA) oraz Aktu o sztucznej inteligencji (AI Act), a także utworzenie niezależnej Europejskiej Sieci Fact-checkerów, której celem jest utrzymanie integralności debaty publicznej. Ponadto EUDS koncentruje się na wzmacnianiu instytucji demokratycznych poprzez ochronę aktorów politycznych oraz niezależności mediów w ramach programu *Media Resilience Programme*, jednocześnie zwiększając odporność społeczną poprzez inwestycje w edukację cyfrową oraz zaangażowanie obywatelskie. Komisja Europejska wskazuje również na dodatkowe działania angażujące całe społeczeństwo (typu *whole-of-society*), które będą obejmowały wydarzenie wysokiego szczebla na rzecz demokracji, coroczną nagrodę za innowacje demokratyczne oraz wspieranie dobrowolnych zobowiązań sektora prywatnego w celu budowania koalicji biznesu na rzecz demokracji.

Działania Komisji Europejskiej, których wdrażanie zaplanowano do 2027 roku, obejmują cztery główne obszary:

- Utworzenie Europejskiego Centrum Odporności Demokratycznej;
- Ochronę integralności przestrzeni informacyjnej;
- Wzmacnianie instytucji i wolnych wyborów oraz niezależnych mediów;
- Zwiększanie odporności społecznej i zaangażowania obywateli.

Europejskie Centrum Odporności Demokratycznej (ECDR)

Podczas posiedzenia Rady do Spraw Ogólnych 24 lutego 2026 roku ministrowie UE, na zaproszenie Komisji oraz prezydencji Rady, oficjalnie zainaugurowali Europejskie Centrum Odporności Demokratycznej (ECDR). Strukturalnie, centrum funkcjonować ma jako platforma współpracy pomiędzy Parlamentem Europejskim, Komisją Europejską oraz Europejską Służbą Działań Zewnętrznych (EEAS), przy aktywnym udziale wszystkich 27 państw członkowskich.

ECDR zostało zaprojektowane jako rozwijający się, dobrowolny hub, w ramach którego państwa członkowskie współpracują zgodnie ze swoimi potrzebami i kompetencjami krajowymi. Działając w powiązaniu z systemem szybkiego reagowania EEAS (Rapid Alert System), centrum integruje istniejące sieci i planuje utworzenie dedykowanej platformy interesariuszy, mającej ułatwiać dialog pomiędzy instytucjami UE, środowiskiem akademickim i społeczeństwem obywatelskim. Europejska Sieć Fact-checkerów stanowi również element tego ekosystemu. Ostatecznym celem centrum jest przekształcenie działań reaktywnych w proaktywny system wczesnego ostrzegania, zwiększający świadomość sytuacyjną oraz zapewniający wsparcie operacyjne dla szybkich i skoordynowanych reakcji na dezinformację i zagrożenia hybrydowe.

Jednym z kluczowych elementów struktury ECDR ma być Platforma Interesariuszy stanowiąca istotne ogniwo łączące architekturę instytucjonalną UE z praktycznym doświadczeniem niezbędnym do przeciwdziałania zagrożeniom hybrydowym. Ponieważ ECDR opiera się na współpracy dobrowolnej, rozproszona sieć społeczeństwa obywatelskiego, badaczy i przedstawicieli mediów jest traktowana jako operacyjna konieczność. Zakłada ona przejście w stronę współtworzenia polityk, w którym interesariusze mogą bezpośrednio wpływać na kształt unijnych ram przeciwdziałania FIMI

oraz protokołów reagowania kryzysowego. Podejście to wspierane jest mechanizmem „*respond-or-explain*", zobowiązującym Radę ECDR do formalnego uzasadnienia odrzucenia rekomendacji interesariuszy, co wzmacnia odpowiedzialność instytucjonalną i ogranicza ryzyko przekształcenia platformy w forum wyłącznie symboliczne.

Komisja Europejska przedstawiła również propozycję nowego mechanizmu finansowania. Program AgoraEU, stanowiący kluczowy filar finansowy Europejskiej Tarczy Demokracji, został formalnie zaproponowany w lipcu 2025 roku jako element projektu wieloletnich ram finansowych (MFF) na lata 2028–2034. Jego wprowadzenie oznacza zmianę paradygmatu poprzez konsolidację dotychczas rozproszonych programów Creative Europe oraz CERV (Citizens, Equality, Rights and Values) w jeden zintegrowany „superprogram". Połączenie to obejmuje wsparcie sektora kultury, mediów i audiowizualnego z inicjatywami na rzecz praworządności, wolności podstawowych oraz przeciwdziałania dyskryminacji.

Ostateczny kształt programu AgoraEU mają nadać wieloletnie ramy finansowe (*Multiannual Financial Framework*; MFF) na lata 2028–2034[11]. Rozważane są również innowacyjne mechanizmy finansowania[12], takie jak reinwestowanie kar nałożonych w ramach Aktu o usługach cyfrowych (DSA) i Aktu o AI lub przekierowanie środków wstrzymanych w ramach mechanizmu warunkowości praworządnościowej do programu, w celu wsparcia niezależnych mediów i organizacji społeczeństwa obywatelskiego.

Choć Unia Europejska przedstawia EUDS jako zdecydowany system obrony „*whole-of-society*", analiza krytyczna wskazuje, że ramy te w pewnym stopniu „zakrywają pęknięcia", opierając się w dużej mierze na niewiążących narzędziach miękkiego prawa oraz dobrowolnej koordynacji, zamiast bardziej zdecydowanych instrumentów legislacyjnych, postulowanych przez część ekspertów[13]. Najbardziej widoczne jest to w przypadku zarządzania ECDR. Pomimo postulatów Parlamentu Europejskiego i organizacji pozarządowych dotyczących utworzenia w pełni niezależnej agencji, ostateczna struktura pozostaje pod kontrolą Komisji, co rodzi obawy, że centrum może pełnić raczej funkcję koordynacyjną niż rzeczywistego ośrodka operacyjnego[14]

Zgodnie z wynikami ankiety przeprowadzonej wśród członków Counter Disinformation Network[15], działania krajowe w zakresie przeciwdziałania FIMI są niewystarczające. Pomimo istnienia odpowiednich regulacji, ich egzekwowanie pozostaje powolne i mało

skuteczne. Problem ten pogłębia niedobór zasobów: 61% interesariuszy wskazało brak stabilnego finansowania jako główną barierę dla utrzymania kadr, rozwoju technologicznego oraz skutecznej koordynacji. Jednocześnie coraz silniej podkreśla się potrzebę odejścia od reaktywnych działań w cyklach wyborczych na rzecz stałych struktur odporności oraz proaktywnego przeciwdziałania zagrożeniom.

Choć EUDS zapewnia niezbędne ramy prawne i strukturalne dla wszystkich 27 państw członkowskich, kluczowym pytaniem pozostaje, w jaki sposób uczynić cały system operacyjnie skutecznym w praktyce. Podczas seminarium w Helsinkach przyjęto założenie, że jednym z kluczowych czynników sukcesu są proaktywne działania państw na linii konfrontacji, takich jak korytarz B5+, w których wysoki poziom strategiczny przekłada się na działalność operacyjną w terenie.

Zdefiniowanie krajów B5+ jako "centrum operacyjnego" działań EUDS w ramach czterech głównych filarów

W celu skutecznego przeciwdziałania zagrożeniom FIMI oraz zagrożeniom hybrydowym wymierzonym w procesy demokratyczne Unia Europejska powinna zoperacjonalizować model „odstraszanie przez ukaranie" (*deterrence by punishment*) oraz „odstraszania poprzez odporność" (*deterrence by resilience*). Zwiększając koszty prowadzenia działań FIMI dla podmiotów wrogich oraz wzmacniając „odporność poznawczą" obywateli, należy jednoznacznie sygnalizować przeciwnikom, że ich operacje są skazane na niepowodzenie. Wymaga to podejścia *whole-of-society* w ramach szerszego ***modelu „whole-of-Europe"***: długoterminowego zaangażowania w łączenie sektorów, angażowanie obywateli oraz odbudowę zaufania do instytucji publicznych, tak aby spójność społeczna utrzymywała się również ponad podziałami politycznymi.

Uwzględniając ramy regulacyjne oraz obecny stan operacjonalizacji EUDS, jednym z kluczowych celów seminarium była analiza perspektyw krajów B5 oraz włączenie doświadczeń Ukrainy do szerszego regionalnego systemu odporności i reagowania. Integracja doświadczeń ukraińskich z mechanizmami koordynacji regionalnej zwiększa zdolność UE do wcześniejszego wykrywania i reagowania na zagrożenia hybrydowe.

To doświadczenie frontowe dostarcza praktycznych wniosków, które mają bezpośrednie znaczenie dla dalszej operacjonalizacji Europejskiej Tarczy Demokracji. Wykorzystanie tych doświadczeń pozwala Unii Europejskiej wzmocnić zdolności w zakresie wczesnego

wykrywania, skoordynowanej reakcji oraz długoterminowej odporności społecznej w przestrzeni informacyjnej.

W tym kontekście państwa B5 nie powinny być postrzegane jedynie jako odbiorcy polityk UE, lecz jako kluczowi współtwórcy ich rozwoju operacyjnego. Jako region znajdujący się na pierwszej linii zagrożeń hybrydowych i zagranicznej manipulacji informacyjnej mogą pełnić funkcję operacyjnego centrum Europejskiej Tarczy Demokracji, przekładając ramy strategiczne na adaptowalne praktyki, mechanizmy koordynacji oraz modele odporności możliwe do zastosowania w całej Europie.

1. Nowe Europejskie Centrum Odporności Demokratycznej

Państwa B5 mogą kształtować mandat Centrum poprzez promowanie modelu „*hub-and-spoke*", w którym jego rdzeń analityczny i operacyjny zasilany jest przez istniejące regionalne centra doskonałości (takie jak NATO StratCom COE w Rydze czy Hybrid CoE w Helsinkach). Poprzez ulokowanie łączników z regionu B5 w strukturach kierowniczych Centrum jego mandat mógłby zostać ukierunkowany na większą operacyjność, m.in. poprzez priorytetowe traktowanie wymiany informacji w czasie rzeczywistym oraz transgranicznej reakcji kryzysowej. Centrum powinno pełnić funkcję głównego mechanizmu skalowania modeli gotowości opartych na doświadczeniach Finlandii oraz tzw. „modelu bałtyckiego" odporności. Kraje B5 mogłyby również przewodzić Platformie Interesariuszy Centrum, zapewniając aktywne uczestnictwo organizacji społeczeństwa obywatelskiego w realizacji projektów.

2. Ochrona integralności przestrzeni informacyjnej

Wdrożenie proaktywnej architektury przeciwdziałania FIMI wymaga, aby region B5+ objął wiodącą rolę w zakresie prebunkingu oraz atrybucji technicznej. Region ten może rozwijać transgraniczne systemy wczesnego wykrywania. W zakresie regulacji platform cyfrowych B5+ powinien działać jako skoordynowany „blok wykonawczy", wykorzystując Akt o usługach cyfrowych (DSA) do egzekwowania szybszej moderacji treści oraz narzędzi przejrzystości dostosowanych do specyfiki językowej i lokalnych taktyk manipulacyjnych. W oparciu o działania DG JUST oraz organizacji takich jak International IDEA region może promować utworzenie Funduszu Odporności Wyborczej, którego celem byłoby budowanie stałej infrastruktury monitorowania ryzyka, tak aby wykrywanie zagrożeń było procesem ciągłym, a nie ograniczonym do okresu kampanii wyborczych.

3. Wzmacnianie instytucji, wyborów i niezależnych mediów

Integralność infrastruktury demokratycznej zależy od kondycji ekosystemu instytucjonalnego. W regionie Morza Bałtyckiego i poza nim najpoważniejsze ryzyka obejmują emocjonalne „zmęczenie wojną" oraz podatność poznawczą społeczeństw. Odporność demokratyczną należy traktować jako formę współczesnego „dobrostanu publicznego". Szczególną uwagę należy poświęcić państwom o ograniczonym zasięgu językowym, gdzie niezależne media często funkcjonują w warunkach strukturalnych ograniczeń finansowych oraz zwiększonej podatności na zewnętrzne operacje wpływu. W tym kontekście region powinien wspierać unijny mechanizm subsydiów dla małych rynków medialnych, którego celem byłoby zapewnienie stabilności wysokiej jakości dziennikarstwa oraz ograniczenie powstawania luk informacyjnych wykorzystywanych przez podmioty wrogie. W oparciu o współpracę Finlandii z DG JUST państwa B5 mogłyby wspierać wdrożenie jednolitego frameworku ochrony organów wyborczych, zapewniającego, że koncepcja „*whole-of-Europe*" jest wzmocniona infrastrukturą instytucjonalną oraz rygorystycznymi ramami prawnymi. Region B5+ może również promować wspólne standardy przejrzystości finansowania politycznego oraz mechanizmy identyfikacji podatności wykorzystywanych przez aktorów FIMI.

4. Wzmacnianie odporności społecznej i zaangażowania obywatelskiego

Region B5+ promuje specyficzny model odporności, w którym społeczeństwo obywatelskie pełni kluczową rolę systemu wczesnego ostrzegania i gotowości społecznej. UE powinna rozwijać regionalne inicjatywy, takie jak sieci „elfów"[16] monitorujących dezinformację oraz zdecentralizowane programy edukacji medialnej w szkołach i miejscach pracy. Lokalne sieci odporności stanowią pomost do szerszego zaangażowania obywatelskiego, pokazując, że odporna demokracja opiera się na narzędziach civic tech oraz oddolnym uczestnictwie, które mogą być skalowane na poziom całej UE.

Wykorzystując dynamikę korytarza B5, region ten może integrować swoje doświadczenia operacyjne z wynikami Europejskiego Panelu Obywatelskiego ds. Gotowości i Odporności z 2026 roku[17]. Panel ten, uruchomiony w marcu 2026 roku, gromadzi 150 losowo wybranych obywateli ze wszystkich 27 państw członkowskich, którzy formułują rekomendacje dotyczące wzmacniania systemów demokratycznych wobec kryzysów systemowych, takich jak pandemie, katastrofy klimatyczne czy wojna hybrydowa.

Wykorzystanie tych wniosków pozwala regionowi B5+ dostosować własne modele odporności do szerszych oczekiwań społecznych i wizji obywateli UE.

Odporność jednak nie jest bezkosztowa. Wymaga świadomej inwestycji w kapitał ludzki - swoistej „Agory" wymiany demokratycznej wspieranej finansowo. Na podstawie doświadczeń krajowych **region B5 powinien wspierać tworzenie koalicji biznesowej na rzecz demokracji**, w której przedsiębiorstwa podejmują dobrowolne zobowiązania dotyczące przestrzegania wartości demokratycznych i odpowiedzialności społecznej. Wkłady prywatne i pro bono mają uzupełniać budżet programu AgoraEU, zapewniając, że nawet w przypadku opóźnień w negocjacjach MFF dostępna pozostanie druga warstwa zasobów finansowych i eksperckich, wspierająca „pierwszych responderów" demokracji.

Perspektywa regionalna B5+

Poziom regionalny stanowi kluczowy punkt styku między strategią europejską a działaniami na poziomie krajowym. O ile ramy unijne, takie jak Europejska Tarcza Demokracji, wyznaczają kierunek strategiczny i dążą do koordynacji istniejących instrumentów, o tyle ich rzeczywista implementacja zależy od skutecznej współpracy oraz sprawnych mechanizmów koordynacji. W tym kontekście region Morza Bałtyckiego stanowi szczególnie sprzyjające środowisko operacyjne.

Region Morza Bałtyckiego posiada szereg przewag strukturalnych, w tym bezpośrednie doświadczenie w przeciwdziałaniu zagrożeniom hybrydowym wynikające z ciągłej ekspozycji na działania wrogie, a także silną sieć organizacji społeczeństwa obywatelskiego, niezależnych mediów i dziennikarzy śledczych, którzy rozwinęli wysokie kompetencje w zakresie wykrywania i analizy FIMI. Ponadto region ten stanowi ważny ośrodek instytucji regionalnych i międzynarodowych, obejmujący szeroką sieć projektów oraz inicjatyw unijnych ukierunkowanych na przeciwdziałanie zagrożeniom hybrydowym, komunikację strategiczną i cyberbezpieczeństwo.

Każda z tych zdolności tworzy wysoce rozwinięty ekosystem. Wyzwaniem pozostaje jednak efektywna współpraca w ramach systemu obejmującego różne zakresy kompetencji, modele zarządzania i formaty koordynacyjne. Sama obecność rozwiniętych zdolności nie przekłada się automatycznie na spójną odpowiedź regionalną - bez strukturalnej koordynacji i zintegrowanych mechanizmów reagowania nawet zaawansowani aktorzy mogą działać równolegle, zamiast funkcjonować jako element jednego systemu[18].

Pomimo znacznego postępu w zakresie monitorowania i analizy nadal istnieje istotna luka między wykrywaniem działań FIMI a zdolnością do skutecznego reagowania na poziomie regionalnym. Organizacje społeczeństwa obywatelskiego, instytucje badawcze oraz podmioty zajmujące się komunikacją strategiczną często dostarczają bardzo zaawansowanych analiz. Jednak ich przełożenie na konkretne działania — regulacyjne, prawne czy komunikacyjne - bywa niespójne i opóźnione, co tworzy przestrzeń operacyjną, w której sieci FIMI mogą się adaptować, utrzymywać aktywność i generować nowe podatności w środowisku informacyjnym.

Problem koordynacji odpowiedzi na FIMI nie wynika z braku narzędzi, lecz z ograniczeń systemowej współpracy. W całej UE poziom koordynacji między państwami członkowskimi znacząco się różni w zależności od systemów prawnych, struktur instytucjonalnych oraz percepcji zagrożeń. Problem ten pogłębia pionowy brak spójności między ramami unijnymi a ich wdrażaniem na poziomie krajowym, co spowalnia przepływ informacji między poziomami zarządzania. Jednocześnie ograniczenia wynikające z niewystarczających mechanizmów współpracy między administracją publiczną, organizacjami społeczeństwa obywatelskiego, platformami cyfrowymi i instytucjami badawczymi utrudniają skuteczną współpracę międzysektorową. Choć istnieją przykłady efektywnej koordynacji w ramach poszczególnych sektorów, trwała interoperacyjność międzysektorowa nadal pozostaje wyzwaniem, ograniczając przepływ informacji od etapu wykrywania i atrybucji do terminowych, skoordynowanych reakcji.

Brak pełnej systemowej koordynacji nie oznacza jednak jej całkowitego braku, zwłaszcza na poziomie regionalnym. Przeciwnie - region Morza Bałtyckiego wykazuje jedne z najbardziej zaawansowanych form współpracy w Europie. Wysiłki te są jednak często skoncentrowane w określonych obszarach i nie tworzą jeszcze w pełni zintegrowanego systemu reagowania.

Połączenie wysokich zdolności i utrzymujących się wyzwań koordynacyjnych sprawia, że region ten jest szczególnie dobrze przygotowany do wspierania operacjonalizacji na poziomie europejskim. Kraje B5 dysponują odpowiednimi narzędziami czy doświadczeniem, ale mierzą się przede wszystkim z wyzwaniem integracji i skutecznej egzekucji działań. Jednocześnie region nie tylko stanowi model idealnej reakcji, ale oferuje również jedne z najbardziej zaawansowanych obecnie struktur operacyjnych, adresujących kluczowe wyzwania związane z koordynacją, adaptacją i wdrażaniem, a tym samym dobrze przygotowanych do dalszego skalowania i adaptacji w innych państwach członkowskich UE.

Na poziomie regionalnym **przekształcenie roli społeczeństwa obywatelskiego w aktorów operacyjnych** - poprzez włączenie ich w łańcuch reagowania i zapewnienie, że ich działania bezpośrednio wpływają na kolejne etapy procesu instytucjonalnego — stanowi warunek wstępny operacjonalizacji regionalnej. W całym regionie organizacje społeczeństwa obywatelskiego rozwijają coraz większe zdolności w zakresie wykrywania operacji wpływu. Zmienia to rolę obywateli z biernych odbiorców informacji w aktywnych

uczestników środowiska informacyjnego. W tym kontekście obywatele nie są wyłącznie celem manipulacji, lecz również współtwórcami odporności, zdolnymi do identyfikowania, udostępniania i kontekstualizowania nowych wzorców działań manipulacyjnych.

W kontekście zaangażowania obywatelskiego szczególne znaczenie ma **aktywizacja młodzieży**. Fora młodzieżowe, programy przywódcze oraz inne inicjatywy regionalne wspierane m.in. przez Radę Państw Morza Bałtyckiego podkreślają znaczenie młodych ludzi jako współtwórców odporności systemu[19]. Równolegle różni aktorzy integrują kompetencje cyfrowe z programami edukacyjnymi dotyczącymi analizy informacji i edukacji medialnej. Łącznie inicjatywy te nie tylko wzmacniają długoterminową odporność społeczną, lecz także tworzą nowe sposoby funkcjonowania w coraz bardziej złożonym ekosystemie informacyjnym. Szersze zaangażowanie młodzieży ma również wyraźny wymiar strategiczny. Młodzi ludzie często jako pierwsi korzystają z nowych platform, formatów i sposobów komunikacji, wraz z ewolucją operacji wpływu. Biorąc pod uwagę, że to oni najwcześniej obserwują zmiany taktyk i narracji, są szczególnie dobrze usytuowani do ich identyfikacji. W ten sposób zwiększenie udziału młodych ludzi wzmacnia zdolność adaptacyjną systemu reagowania, poprawiając zarówno wczesne wykrywanie, jak i rozwój wiarygodnych narracji kontrujących.

Technologia jako obszar przekrojowy

Rozwój technologii, w szczególności sztucznej inteligencji, fundamentalnie przekształca środowisko FIMI. AI umożliwia generowanie, dystrybucję i targetowanie ogromnych ilości treści, co sprawia, że kampanie manipulacyjne mogą być prowadzone z niespotykaną dotąd szybkością, skalą i złożonością. Jednocześnie sztuczna inteligencja dostarcza narzędzi do wykrywania, analizy i przeciwdziałania zmanipulowanym treściom, tworząc dynamiczny model podwójnego zastosowania.

Wpływ AI nie ogranicza się jednak wyłącznie do tworzenia treści. Coraz większa część informacji docierających do odbiorców jest filtrowana przez systemy algorytmiczne, które porządkują i priorytetyzują treści, tworząc indywidualny kontekst informacyjny. W rezultacie systemy te nie tylko określają, jakie informacje są widoczne, lecz także wpływają na sposób ich interpretacji. Podmioty oddziałujące na te mechanizmy zyskują zatem strategiczne znaczenie, ponieważ współkształtują środowisko informacyjne oraz wynikające z niego percepcje.

Rywalizacja w przestrzeni informacyjnej nie ogranicza się już wyłącznie do narracji, lecz obejmuje również systemy, za pośrednictwem których informacje są selekcjonowane i interpretowane. Jednocześnie same te systemy stają się celem ataków. Zatruwanie danych (*data poisoning*) oraz manipulacja zbiorami treningowymi mogą zniekształcać wyniki analiz i podważać zaufanie do systemów automatycznych, wprowadzając kolejny wektor podatności do systemu reagowania.

Odpowiedź na te wyzwania wymaga inwestycji zarówno w zdolności technologiczne, jak i w mechanizmy ochronne. Aktorzy regionalni powinni wzmacniać zdolności w zakresie wykrywania i analizy, jednocześnie zapewniając integralność wykorzystywanych systemów. Ze względu na zróżnicowany poziom zaawansowania technologicznego w poszczególnych państwach kluczowe znaczenie ma współpraca regionalna, która pozwoli uniknąć fragmentacji oraz zapewni, że technologie będą wzmacniać odporność zbiorową.

Od ekosystemu do systemu

W kontekście regionu Morza Bałtyckiego połączenie istniejących struktur w spójny system operacyjny wymaga przełożenia zasad operacjonalizacji na praktyki regionalne. Koordynacja powinna zostać zinstytucjonalizowana poprzez powiązanie procesów wykrywania, analizy i reagowania. Niezbędne są wspólne praktyki i protokoły stosowane konsekwentnie w różnych przypadkach, co umożliwi powtarzalność działań. **Mierzalność wymaga z kolei wprowadzenia wskaźników oceniających zarówno skuteczność zakłócania działań przeciwnika, jak i wzrost odporności.** Kluczowe znaczenie ma także ciągłe uczenie się oraz zdolność adaptacji do zmieniającego się charakteru zagrożeń.

Fundamentalnym elementem tego modelu jest stworzenie szybszych i bardziej niezawodnych kanałów przejścia od informacji do działania. Obejmuje to integrację społeczeństwa obywatelskiego w procesy reagowania, wzmocnienie wymiany informacji transgranicznej oraz zapewnienie zgodności działań regionalnych z ramami UE i NATO, a także zdolność do ich współkształtowania. W tym sensie skuteczność modelu regionalnego nie zależy od tworzenia nowych inicjatyw, lecz od zdolności do aktywacji i połączenia istniejących zasobów w funkcjonujący system.

Region Morza Bałtyckiego już dziś funkcjonuje jako wysoce rozwinięty ekosystem podmiotów zaangażowanych w przeciwdziałanie FIMI. Same ekosystemy nie generują jednak automatycznie skoordynowanych rezultatów. Bez strukturalnej integracji ich

wpływ pozostaje rozproszony. Przejście od ekosystemu do systemu stanowi zatem kluczowe zadanie operacjonalizacji regionalnej. Oznacza ono przejście od działań równoległych do skoordynowanych, od niezależnych zdolności do zintegrowanych procesów oraz od reaktywności do proaktywności.

Poprzez połączenie aktorów, narzędzi i procesów w spójne ramy operacyjne region może działać w sposób trwały i skuteczny, wspierając Unię Europejską w ochronie przestrzeni informacyjnej.

Relacje polsko-ukraińskie jako pole walki w wojnie informacyjnej

Na tym tle Polska i Ukraina stanowią przykład doświadczeń operacyjnych, które mogą zostać adaptowane i skalowane w ramach szerszego formatu B5+, a także struktur europejskich. Oba państwa należą do najbardziej kluczowych, a zarazem najbardziej narażonych obszarów oddziaływania wrogich operacji wpływu. Ich znaczenie wynika z położenia geograficznego, historii, współpracy wojskowej, wsparcia humanitarnego, roli Polski jako logistycznego i politycznego hubu pomocy dla Ukrainy oraz miejsca Ukrainy w przyszłym europejskim porządku bezpieczeństwa. Z perspektywy rosyjskiego aparatu wpływu osłabianie wzajemnego zaufania między Polakami a Ukraińcami nie jest celem drugorzędnym - stanowi jeden z warunków ograniczenia zdolności Zachodu do prowadzenia spójnej polityki wobec rosyjskiej agresji. Długotrwała ekspozycja na tego typu działania zmusiła oba państwa do adaptacji do permanentnie wrogiego środowiska informacyjnego.

Wojna informacyjna jako operacja na percepcji i emocjach

Wojna informacyjna nie jest już wyłącznie rywalizacją o fakty. Jej głównym celem staje się coraz częściej kształtowanie percepcji - sposobu, w jaki społeczeństwa interpretują wydarzenia, oceniają intencje sojuszników, postrzegają własne instytucje i reagują emocjonalnie na kryzysy. W tym sensie dezinformacji nie należy rozumieć jedynie jako obiegu fałszywych lub wprowadzających w błąd treści. Stanowi ona instrument strategiczny służący wpływaniu na środowisko poznawcze i emocjonalne, w którym funkcjonują obywatele, instytucje i decydenci.

Celem wrogich działań informacyjnych często nie jest przekonanie odbiorców do jednej spójnej alternatywnej rzeczywistości. Znacznie częściej chodzi o wywołanie emocji takich jak strach, gniew, nieufność, zmęczenie, resentyment czy poczucie zdrady. Stany te mają znaczenie operacyjne, ponieważ osłabiają spójność społeczną, obniżają zaufanie do sojuszników i zwiększają polityczny koszt długofalowej współpracy.

Od ponad dekady rosyjskie operacje informacyjne uderzają w emocjonalne i historyczne fundamenty współpracy polsko-ukraińskiej. Logika tych działań jest jasna: jeśli uda się skłonić Polskę i Ukrainę do wzajemnego postrzegania się przez pryzmat nieufności, resentymentu i nierozwiązanych traum historycznych, ich zdolność do wspólnego

działania zostanie ograniczona. Atak wymierzony jest więc nie tylko w fakty, lecz przede wszystkim we wzajemny obraz obu społeczeństw.

Polska i Ukraina jako studia przypadków obrony przestrzeni informacyjnej

Doświadczenia Polski i Ukrainy należy analizować nie tylko przez pryzmat relacji bilateralnych, lecz także jako dwa komplementarne studia przypadków społeczeństw narażonych na długotrwałe operacje informacyjne. Oba państwa od ponad dekady pozostają celem rosyjskiego aparatu wpływu, choć charakter, intensywność i cele operacyjne tych działań różnią się między sobą. Ukraina doświadcza bezpośredniej, wojennej agresji informacyjnej, której celem jest podważenie legitymacji państwa, morale wojska oraz spójności społecznej. Polska z kolei jest celem działań jako państwo frontowe NATO i UE, kluczowy hub logistyczny pomocy dla Ukrainy oraz społeczeństwo, którego poparcie ma istotne znaczenie dla utrzymania polityki sojuszniczej.

To rozróżnienie ma fundamentalne znaczenie. Analiza bowiem nie powinna ograniczać się wyłącznie do pytania, w jaki sposób rosyjska propaganda wpływa na relacje polsko-ukraińskie, lecz obejmować również to, jak oba państwa wypracowały odmienne modele odporności instytucjonalnej i obywatelskiej wobec wrogich operacji wpływu.

Ukraina stanowi przykład obrony informacyjnej prowadzonej w warunkach pełnoskalowej wojny, w której komunikacja strategiczna, szybkie przekazy publiczne, mobilizacja cyfrowa i monitoring społeczny stały się elementami przetrwania państwa. Polska natomiast reprezentuje model odporności demokratycznej państwa sojuszniczego, systematycznie poddawanego próbom osłabienia zaufania publicznego, polaryzacji społecznej oraz podważania poparcia dla wsparcia Ukrainy.

W tym ujęciu oba przypadki dostarczają praktycznych wniosków dla szerszego regionalnego i europejskiego systemu odporności. Pokazują one, że obrona przestrzeni informacyjnej wymaga czegoś więcej niż jedynie fact-checkingu pojedynczych fałszywych treści. Wymaga koordynacji instytucjonalnej, współpracy ze społeczeństwem obywatelskim, systemów wczesnego ostrzegania, komunikacji strategicznej, edukacji medialnej, odpowiedzialności platform cyfrowych oraz długofalowej edukacji publicznej.

Polska: odporność w społeczeństwie frontowym

W przypadku Polski rosyjskie operacje informacyjne koncentrują się na osłabianiu poparcia dla Ukrainy, podważaniu zaufania do instytucji państwa oraz przedstawianiu zobowiązań sojuszniczych jako kosztownych, ryzykownych lub sprzecznych z interesem narodowym[20]. Celem nie jest bezpośrednie uczynienie społeczeństwa prorosyjskim - bardziej realistycznym efektem operacyjnym jest wywołanie zmęczenia, nieufności i emocjonalnego oporu wobec dalszego wsparcia Ukrainy.

W tym celu wykorzystywane są narracje oparte na napięciach ekonomicznych, migracyjnych, sporach historycznych, polaryzacji politycznej oraz obawach związanych z bezpieczeństwem. Kwestie takie jak import zboża, transport, rynek pracy, pomoc dla uchodźców, wydatki obronne czy ryzyko eskalacji stają się materiałem podatnym na manipulację. W tym modelu realne problemy polityczne są przekształcane w dowody zdrady, niekompetencji lub zewnętrznej manipulacji.

Doświadczenie Polski pokazuje również znaczenie współpracy instytucji publicznych ze społeczeństwem obywatelskim. Komunikacja państwa jest konieczna, lecz niewystarczająca. Organizacje pozarządowe, niezależne media, fact-checkerzy, badacze i lokalni aktorzy często szybciej identyfikują nowe narracje oraz skuteczniej docierają do grup odbiorców nieufnych wobec oficjalnego przekazu. W polskim ekosystemie podmiotów zaangażowanych w przeciwdziałanie FIMI istotną rolę odgrywa również sektor biznesowy. Współcześnie społeczna odpowiedzialność biznesu wykracza poza działania filantropijne, obejmując aktywne zaangażowanie w przyczynianie się do wzmacniania odporności społecznej. Przedsiębiorstwa i korporacje dysponują zasobami, kompetencjami organizacyjnymi oraz zdolnością do budowania partnerstw międzysektorowych, dzięki czemu może wspierać rozwój edukacji obywatelskiej, kompetencji cyfrowych i medialnych, krytycznego myślenia oraz kapitału społecznego. Działania te mają szczególne znaczenie w kontekście zagrożeń informacyjnych, ponieważ zwiększają zdolność obywateli do samodzielnej oceny wiarygodności informacji oraz ograniczają podatność na manipulację i dezinformację.

Istotnym elementem zaangażowania biznesu jest również wspieranie inicjatyw służących budowaniu zaufania społecznego, wzmacnianiu wspólnot lokalnych oraz poprawie dobrostanu psychicznego obywateli. Są to czynniki, które coraz częściej uznawane są za

fundament odporności społecznej, rozumianej jako zdolność społeczeństwa do adaptacji i skutecznego reagowania na sytuacje kryzysowe. Przykładem takiego podejścia jest działalność Fundacji PZU, która realizuje programy wspierające edukację, rozwój kompetencji społecznych, zdrowie psychiczne oraz aktywność obywatelską. Tego rodzaju inicjatywy pokazują, że sektor prywatny może pełnić rolę partnera strategicznego w budowaniu odporności społecznej i wzmacnianiu bezpieczeństwa informacyjnego państwa[21]. Efektywna koordynacja istniejących już działań wymaga jednak implementacji modelu „whole-of-society", w którym państwo wyznacza kierunek strategiczny, a aktorzy społeczni i prywatni wspierają monitoring, analizę, edukację i działania lokalne.

Ukraina: obrona informacyjna w warunkach wojny

Ukraina stanowi odmienny, lecz równie istotny przypadek. Od 2014 roku, a szczególnie po pełnoskalowej inwazji w 2022 roku, państwo to pozostaje celem operacji informacyjnych mających na celu osłabienie jego legitymacji, morale społeczeństwa, wiarygodności sił zbrojnych oraz wsparcia międzynarodowego. Rosyjskie narracje uderzają m.in. w kwestie korupcji, mobilizacji, infrastruktury energetycznej, kryzysu humanitarnego, przesiedleń oraz zaufania do przywództwa politycznego[22] [23] [24].

Doświadczenie Ukrainy pokazuje, że **obrona informacyjna staje się integralną częścią obrony państwa.** W warunkach wojennych kluczowe znaczenie mają szybkość i wiarygodność komunikacji. Instytucje publiczne muszą jednocześnie przeciwdziałać panice, wyjaśniać ryzyka, utrzymywać zaufanie społeczne oraz reagować na narracje przeciwnika. Jednocześnie społeczeństwo obywatelskie, sieci wolontariackie, dziennikarze, grupy OSINT i niezależne media odgrywają kluczową rolę w dokumentowaniu agresji, ujawnianiu manipulacji oraz wzmacnianiu odporności społecznej.

Skuteczne metodologie: od reakcji do odporności

Doświadczenia Polski i Ukrainy wskazują na zestaw metod, które mogą być rozwijane wspólnie i skalowane regionalnie. Pierwszą z nich jest system wczesnego ostrzegania oparty na monitoringu narracji. Drugą - prebunking, czyli uprzedzanie odbiorców o technikach manipulacji, zanim pojawią się konkretne fałszywe treści. Trzecią - komunikacja strategiczna wyjaśniająca decyzje publiczne w sposób szybki, jasny i empatyczny. Czwartą metodą jest integracja społeczeństwa obywatelskiego. Piątą -

edukacja medialna i cyfrowa, szczególnie wśród młodzieży oraz liderów lokalnych. Szóstą- uporządkowana współpraca z platformami cyfrowymi w zakresie zgłaszania treści manipulacyjnych i koordynacji reakcji.

Łącznie tworzą one model przechodzący od reaktywnego „prostowania fałszywych informacji" do proaktywnego i adaptacyjnego systemu odporności informacyjnej.

Rada Konsultacyjna ds. Odporności na Dezinformację Międzynarodowa jako model systemowy

W tym kontekście Rada Konsultacyjna ds. Odporności na Dezinformację Międzynarodową[25], powołana przy Ministerstwie Spraw Zagranicznych, stanowi istotny model instytucjonalny. Jej znaczenie nie polega wyłącznie na utworzeniu kolejnego organu doradczego, lecz na uznaniu, że przeciwdziałanie dezinformacji wymaga współpracy administracji publicznej, społeczeństwa obywatelskiego, środowisk akademickich, samorządów, mediów oraz sektora prywatnego. Siłą tego modelu jest przezwyciężanie fragmentacji. Instytucje państwowe dysponują narzędziami prawnymi i dyplomatycznymi, organizacje społeczne monitorują narracje i docierają do lokalnych społeczności, środowiska akademickie dostarczają analiz, sektor technologiczny - narzędzi, a samorządy posiadają wiedzę o lokalnych podatnościach. Model rady tworzy przestrzeń systemowej wymiany wiedzy, oceny zagrożeń oraz współpracy operacyjnej.

Podejście to wzmacnia legitymizację działań państwa, przyspiesza identyfikację zagrożeń i przesuwa akcent z reaktywnego zarządzania kryzysowego na długofalowe budowanie odporności. Łączy ono analizę strategiczną z praktycznym wdrażaniem. Doświadczenia tego modelu mogą również wspierać dalszą operacjonalizację struktur unijnych, takich jak Europejskie Centrum Odporności, pokazując wartość systemowej współpracy między państwem, społeczeństwem obywatelskim i pozostałymi aktorami ekosystemu informacyjnego.

CASIMIR PULASKI FOUNDATION
Ambasada Rzeczypospolitej Polskiej w Helsinkach
COUNCIL OF THE BALTIC SEA STATES
POLISH PRESIDENCY 2025–2026
PZU FUNDACJA
Sfinansowano ze środków Fundacji PZU

Przypisy

[1] Najnowsze informacje na temat EDS dostępne są na stronie Komisji Europejskiej https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660 oraz Parlamentu Europejskiego: https://www.europarl.europa.eu/legislative-train/package-european-democracy-action-plan/file-european-democracy-shield.

[2] Parlament Europejski (2025) *European Democracy Shield*. Legislative Train Schedule. Dostęp: https://www.europarl.europa.eu/legislative-train/package-european-democracy-action-plan/file-european-democracy-shield.

[3] Zob. Raport Europejskiej Służby Działań Zewnętrznych w sprawie manipulacji informacjami zagranicznymi i ingerencji (FIMI), który podkreśla zmianę w reakcjach na zakłócenia, obejmujących ujawnianie sieci, atrybucję i skoordynowane środki zaradcze. Chociaż stanowi to istotną zmianę w stosunku do wcześniejszych podejść skoncentrowanych na monitorowaniu, nie zostało ono jeszcze przełożone na w pełni operacyjny model. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.

[4] Zob. np. European External Action Service (EEAS) (2026) *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)*. Dostęp: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104617.; European Commission (2025) *Digital Services Act*. Dostęp: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act.; European Parliament (2024) *Defence of Democracy Package*. Legislative Train Schedule. Dostęp: https://www.europarl.europa.eu/legislative-train/spotlight-JD%2023-24/file-defence-of-democracy-package.; NATO (2025) *NATO's Approach to Counter Information Threats*. Dostęp: https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats.; NATO Strategic Communications Centre of Excellence (2025) *Official Website*. Dostęp: https://stratcomcoe.org/.

[5] EDS opiera się na pracach UE nad przeciwdziałaniem FIMI, prowadzonych od 2015 r. pod przewodnictwem Europejskiej Służby Działań Zewnętrznych (ESDZ), a także na ramach regulacyjnych UE dotyczących zagrożeń dla demokracji, np. ustawie o usługach cyfrowych (DSA); ustawie o sztucznej inteligencji (AI); rozporządzeniu w sprawie przejrzystości i targetowania reklam politycznych (TTPA).

[6] Komisja Europejska (2020) *European Democracy Action Plan*. Dostęp: https://ec.europa.eu/commission/presscorner/detail/ga/ip_20_2250.

[7] Komisja Europejska (2023) *Defence of Democracy Package*. COM(2023) 630 final. Dostęp: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023DC0630.

[8] European Partnership for Democracy (EPD) (2025) *European Democracy Shield*. Dostęp: https://epd.eu/what-we-do/policy/european-democracy-shield/.

[9] Parlament Europejski (2024) *Procedure File: European Democracy Shield*. Available at: https://oeil.europarl.europa.eu/oeil/el/procedure-file?reference=2024/2999(RSO).; 18 grudnia 2024 r. Parlament Europejski przegłosował powołanie Specjalnej Komisji ds. Europejskiej Tarczy Demokracji (EUDS).

[10] Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (2025) *Joint Communication* .Dostęp: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0791.; 12 listopada 2025 r. Komisja i Wysoki Przedstawiciel opublikowali wspólny komunikat pt. „*European Democratic Shield: Empowering Strong and Resilient Democracies*".

[11] Parlament Europejski formalnie przyjął swoje tymczasowe stanowisko 28 kwietnia 2026 r., proponując budżet w wysokości 10,72 mld euro, co stanowi wzrost o 25% w stosunku do pierwotnej propozycji Komisji wynoszącej 8,5 mld euro.

[12] Fundacja im. Stefana Batorego (2025) *Joint Letter: Call to Support the European Parliament's Proposal to Increase AGORAEU's Budget in the Next MFF*. Dostęp: https://www.batory.org.pl/oswiadczenie/joint-letter-call-to-support-the-european-parliaments-proposal-to-increase-agoraeus-budget-in-the-next-mff/

[13] Delors Centre (2025) *The European Democracy Shield: Papering Over the Cracks?* Dostęp: https://www.delorscentre.eu/en/publications/detail/publication/the-european-democracy-shield-papering-over-the-cracks.

[14] Brussels Times (2025) *Fight for Democratic Resilience: EU's Bold Centre at Crossroads of Urgency*. Dostęp: https://www.brusselstimes.com/opinions/1989324/fight-for-democratic-resilience-eus-bold-centre-at-crossroads-of-urgency?utm_source=Counter%20Disinformation%20Network&utm_campaign=6f671e8663-EMAIL_CAMPAIGN_2025_09_26_09_16_COPY_01&utm_medium=email&utm_term=0_-1235c0ed7e-647124417.

[15] Opinie zebrane w listopadzie 2025, miesięczny newsletter CDN, luty 2026, Alliance4Europe. https://mailchi.mp/alliance4europe/p5cfk84al4-18047860?e=cb4dbf6fad

[16] German Marshall Fund of the United States (GMF) (2025) *The Role of Cyber Elves Against Russian Information Operations*. Dostęp: https://www.gmfus.org/news/role-cyber-elves-against-russian-information-operations.

[17] Bürgerrat (2025) *EU Seeks Citizens' Support for Preparedness*. Dostęp: https://www.buergerrat.de/en/news/eu-seeks-citizens-support-for-preparedness/#:~:text=Sie%20befinden%20sich%20hier%3A,preparedness%20in%20a%20Citizens'%20Panel.

[18] Zob. Europejska Służba Działań Zewnętrznych, *4. Raport w sprawie manipulacji informacjami zagranicznymi i ingerencji (FIMI)* (2026) https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf; Centrum Doskonałości NATO ds. Komunikacji Strategicznej i Hybrydowe Centrum Doskonałości, *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM' (prepared in cooperation with Hybrid COE)*w którym podkreślono potrzebę ujednoliconych ram umożliwiających skoordynowane reakcje wielu podmiotów. https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-fence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253.

[19] Zob. Inicjatywy dla młodzieży Rady Państw Morza Bałtyckiego (RPMB) https://cbss.org/priorities/regional-identity/youth/.

[20] Digital Forensic Research Lab (DFRLab) (2025) *Election Report: Assessment of Foreign Manipulation and Interference in the 2025 Polish Presidential Election*. Dostęp: https://dfrlab.org/2025/08/25/election-report-assessment-of-foreign-manipulation-and-interference-in-the-2025-polish-presidential-election/.

[21] Zob. inicjatywy Fundacji PZU, m.in. zapowiedziana Akademia Odporności (https://fundacja.pzu.pl/nasze-dzialania/szczegoly/dolacz-do-akademii-odpornosci), program "Młodzi budują odporność społeczną" (https://fundacja.pzu.pl/nasze-dzialania/szczegoly/projekty-spoleczne-uczniow).

[22] Atlantic Council (2025) *Narrative Warfare*. Dostęp: https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/.

[23] Atlantic Council (2023) *Undermining Ukraine*. Dostęp: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/.

[24] Atlantic Council (2023) *Undermining Ukraine: How Russia Widened Its Global Information War in 2023*. Dostęp: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/.

[25] Ministerstwo Spraw Zagranicznych (2025) *Rada Odporności*. Available at: https://www.gov.pl/web/dyplomacja/rada-odpornosci.

Fundacja im. Kazimierza Pułaskiego (FKP) jest jednym z czołowym polskich think-tanków, który od prawie 20 lat specjalizuje się w polityce zagranicznej i bezpieczeństwie międzynarodowym.

Głównym obszarem aktywności Fundacji Pułaskiego jest dostarczanie analiz opisujących i wyjaśniających wydarzenia międzynarodowe, identyfikujących trendy w środowisku międzynarodowym oraz zawierających implementowane rekomendacje i rozwiązania dla decydentów rządowych i sektora prywatnego. Fundacja w swoich badaniach koncentruje się głównie na dwóch obszarach geograficznych: transatlantyckim oraz przestrzeni postsowieckiej.

Fundacja Pułaskiego skupia ponad 50 ekspertów i jest wydawcą analiz w cyklach: Komentarz Pułaskiego, Pulaski Policy Paper oraz Raport Pułaskiego. Od 2005 roku Fundacja przyznaje nagrodę Rycerz Wolności dla wybitnych postaci, które przyczyniają się do promowania wartości przyświecających generałowi Kazimierzowi Pułaskiemu tj. wolności, sprawiedliwości oraz demokracji. Jest też inicjatorem oraz organizatorem największego w regionie wydarzenia z zakresu bezpieczeństwa międzynarodowego – Warsaw Security Forum. Od 2017 roku prowadzi również polski oddział międzynarodowej sieci networkingowej Women in International Security Poland (WIIS Poland).

W 2022 roku, w odpowiedzi na inwazję Rosji na Ukrainę, wraz z grupą aktywistów ukraińskich, Fundacja im. Kazimierza Pułaskiego była współzałożycielem Międzynarodowego Centrum na rzecz Zwycięstwa Ukrainy (ICUV). Centrum ma na celu projektowanie i wdrażanie oddolnych, międzynarodowych kampanii rzeczniczych wspierających ukraiński wysiłek wojenny, odbudowę powojenną kraju, jak i rozliczenie rosyjskich zbrodni wojennych.

FKP od lat z powodzeniem utrzymuje swoją pozycję we wpływowym rankingu Global Go To Think Tank Index prowadzonym przez University of Philadelphia. W 2020 roku, Fundacja znalazła się na 1 miejscu listy think tanków w Polsce w kategorii Top Defense and National Security. Ponadto, FKP zajęła 2 miejsce wśród wszystkich polskich think tanków oraz ogólnie 22 miejsce w kategorii Top Think Tanks 2020 w Europie Środkowo-Wschodniej. Fundacja im. Kazimierza Pułaskiego jest laureatem nagrody "Think Tank

Awards 2017" w kategorii „Best EU International Affairs think tank" przyznawaną przez brytyjski magazyn "Prospect".

Fundacja Pułaskiego posiada status organizacji partnerskiej Rady Europy.

Dbając o najwyższy standard i jakość prowadzonych działań oraz ceniąc rzetelność pracy analitycznej, Fundacja im. Kazimierza Pułaskiego zobowiązuje swoich pracowników i współpracowników do przestrzegania Europejskiego Kodeksu Postępowania w Zakresie Rzetelności Badawczej z 2023 roku.