Pulaski Policy Papers

Pulaski International Commentary ISSN 2080-8852 Warsaw, 28.05.2026

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

# Frontline operationalization: : B5 countries + Ukraine as the Northeast corridor of democratic resilience

## Building societal and democratic resilience in the Baltic Sea countries

### Executive Summary

Hybrid threats, particularly foreign information manipulation and interference (FIMI), have become a permanent feature of Europe's security environment. As a result of their direct exposure to destabilization efforts, the B5 countries - Lithuania, Latvia, Estonia, Finland, and Poland - together with Ukraine, have developed practical response mechanisms, which may serve as an operational foundation for further development of the European Democracy Shield (EUDS).

The European Democracy Shield constitutes a central pillar of the European Union's evolving architecture for protecting democratic integrity. Its objective is to establish a durable framework for political, regulatory, and operational coordination in response to informational, cyber, and hybrid threats. The EUDS is structured around four interconnected operational pillars, namely the establishment of the new European Centre for Democratic Resilience (ECDR), safeguarding the integrity of the information space, strengthening institutions, elections and independent media, as well as boosting societal resilience and citizens engagement.

Despite the growing number of frameworks, programs, and initiatives aimed at countering FIMI and strengthening democratic resilience, a persistent operational gap remains between the increasing capacity to detect and analyze information threats and the ability to respond to them rapidly and in a coordinated manner. The challenge stems from

fragmented competencies, insufficient operational synchronization between states and sectors, and limitations affecting the development of technological and expert capacities. Operationalizing democratic resilience does not necessarily require a creation of entirely new structures, but rather a more effective integration of existing instruments into a coherent system of action. Efficient information-sharing, standardized response procedures, measurable indicators of effectiveness, and the strengthening of public legitimacy and trust are all essential components of such a system.

The regional perspective of the B5+ countries, as well as the experiences of Poland and Ukraine as states situated on the front line of hybrid threats and information operations, are particularly significant in this regard. Over time, the Baltic Sea region has developed resilience models based on cooperation between public administration, civil society, expert communities, independent media, and the private sector. Ukraine's experience is especially valuable, as operating under conditions of full-scale war led to developing a battle-tested expertise in countering influence operations, maintaining societal resilience, and responding rapidly to information manipulation. At the same time, Poland, as a key state on NATO's and the EU's eastern flank, remains a target of intensive disinformation campaigns aimed at weakening social cohesion and undermining public support for assistance efforts.

Effective operationalization of democratic resilience therefore depends less on establishing new institutions, but rather on improving coordination among existing mechanisms and shortening the path between threat identification and institutional response. The experiences of Poland and Ukraine demonstrate that the effective defence of the information space requires close cooperation between the state, civil society organizations, independent media, expert communities, and the private sector. Properly implemented whole-of-society model enables a transition from reactive counter-disinformation measures toward the long-term strengthening of societal and democratic resilience.

**Key recommendations:**

- Establish a permanent B5+ operational coordination framework on FIMI.
- Integrate frontline regional expertise into the operational development of the European Democracy Shield.
- Strengthen operational cooperation across governments, civil society, platforms, and research actors.
- Develop a regional societal resilience model based on a whole-of-society approach and cross-sectoral engagement, particularly the business sector.
- Strengthen preparedness for AI-enabled information manipulation.

## Recommendations

1. **Establish a permanent B5+ operational coordination framework on FIMI.** The B5+ countries, together with Ukraine, should develop a structured regional coordination framework focused on operational cooperation against FIMI and hybrid threats. Such a framework should support joint threat assessments, shared early-warning procedures, cross-border information exchange, coordinated prebunking efforts, and regional exercises focused on hostile information operations targeting allied cohesion.

2. **Integrate frontline regional expertise into the operational development of the European Democracy Shield.**

   The operational experience accumulated within the B5+Ukraine region should be systematically integrated into the further development of the European Democracy Shield and related EU resilience initiatives. The objective should be to scale adaptable operational practices that have already been tested under sustained pressure and can strengthen the implementation capacity of EU-level frameworks.

3. **Strengthen operational cooperation across governments, civil society, platforms, and research actors.**

   Effective responses to FIMI require faster and more reliable pathways from detection to action. EU and regional actors should therefore strengthen mechanisms that enable operational cooperation across institutional and sectoral boundaries. The priority should be to ensure that analytical findings can be translated more consistently into communicative, regulatory, legal, or enforcement responses across jurisdictions.

4. **Develop a regional resilience model based on the whole-of-society approach and cross-sectoral engagement, particularly the business sector.**

   Long term resilience depends not only on institutional capacity, but also on the ability of societies to recognize, contextualize, and adapt to evolving forms of manipulation. The B5+ region should therefore expand cooperation on media and digital literacy, youth engagement, support for independent media, and civil society-led resilience initiatives. To develop such a social resilience model, cross-sectoral engagement, including the business sector, is crucial. As the business sector enables the mobilization of resources, competencies and communication channels, its active engagement is essential for the implementation of the whole-of-society approach.

The experience of the B5 states demonstrates the effectiveness of such an approach, in which operationalization is a central component of enhancing resilience. Cooperation with the business sector is therefore crucial for all stakeholders, including the state.

5. **Strengthen preparedness for AI-enabled information manipulation**

The rapid development of AI-generated and algorithmically amplified content requires a more coordinated regional and European response. The B5+ region should support joint monitoring of AI-enabled manipulation techniques, stronger cooperation with platforms on synthetic media detection and escalation, and safeguards against the manipulation of AI systems and datasets themselves.

# Introduction

## About the seminar

This policy paper is based on presentations and discussions during a seminar organized by Casimir Pulaski Foundation on 27 March 2026 in cooperation with the PZU Foundation and Embassy of the Republic of Poland in Helsinki under the patronage of the Polish Presidency of the Council of the Baltic Sea States.

The driving force behind this seminar was the recognition that while the European Democracy Shield (EDS)[1] has emerged as a central pillar of EU policy, its real-world efficacy is rooted in the relentless effort by a specific group of nations. The EDS, a comprehensive policy and legal framework, aims at strengthening the integrity of the information sphere, including combating hybrid threats, disinformation and Foreign Information and Manipulation (FIMI), supporting democratic institutions, as well as improving societal resilience and fostering civil engagement.[2] For years the B5 countries - Estonia, Latvia, Lithuania, Finland, and Poland - have been the most proactive architects of democratic defense, often moving faster and more decisively than the broader institutional frameworks in Brussels.

The seminar "Building Societal and Democratic Resilience in the Baltic Sea Countries" brought together representatives from across the B5+Ukraine region, highlighting a broader shift toward the frontline operationalization of democratic resilience. Against this backdrop, the Baltic Sea region emerges as a northeastern corridor of European resilience against hybrid threats and FIMI.

The logic behind this B5+ Ukraine engine is based on the need to advance a "whole-of-society" approach that the European interior is only just beginning to grasp. While the EU institutions have provided a platform for collective action, it is the frontline states that have developed the actual technical and social antibodies required to survive and withstand the threats. By integrating Ukraine's unparalleled experience in neutralizing high-intensity FIMI threats, this corridor creates a unique synergy of battle-tested expertise and democratic agility.

In this context, the B5+ Ukraine group functions as the operational engine of the region. Their proximity to the threat has forced a transition from theory-based policy to a state of

permanent readiness, making them the natural leaders in securing the Baltic Sea region. The seminar aimed to focus on this phenomenon, ensuring that the collective actions of the EU are fueled by the frontline reality and the proactive spirit of the countries that understand the stakes best.

## Why B5+

The B5+ framework represents a fundamental shift in European security architecture, moving the center of gravity from the continent's traditional interior to a dedicated Northeast corridor of democratic resilience.

This strategic belt, comprising Estonia, Latvia, Lithuania, Finland, and Poland, finds its most vital and battle-hardened extension in Ukraine, **creating a B5+ Ukraine formation** that increases the West's de facto immune system. Because these nations operate in a permanent frontline reality, they serve as a laboratory for countering modern hybrid warfare, from systemic GPS jamming to the sophisticated FIMI campaigns that seek to erode social cohesion. Ukraine's inclusion is not merely symbolic but operationally essential, as its firsthand experience in identifying and neutralizing high-intensity disinformation offers an unparalleled blueprint for the rest of the continent.

This proximity to the threat dictates that the B5+ Ukraine corridor must serve as **the operational engine for the European Democracy Shield (EDS).** These frontline states operate with a high-readiness agility born of existential necessity, translating raw survival experience into actionable defense protocols. By integrating Ukraine's unique expertise in countering in particular cognitive warfare into the B5+ engine, the European Democracy Shield gains a high-velocity hub that secures the entire transatlantic community, ensuring that the defense of Western democracy is grounded in the most current, battle-tested realities of the 21st century.

## Operationalization: Toward a functional response model

Over the past decade, substantial progress has been made in identifying and analyzing foreign FIMI mechanisms. However, this progress has revealed a persistent discrepancy: the capacity to detect and analyze FIMI phenomena has outpaced the ability to act against it systematically and in coordination.

The asymmetrical relationship between identification and action defines the current response landscape. The EU and a few of its member states have established strategic frameworks and policy documents addressing FIMI, such as the EUvsDisinfo project, FIMI Toolbox, Digital Services Act (DSA), Artificial Intelligence Act (AI Act) or Defence of Democracy Package 2023, but the challenges remain when it comes to responding to this threat in a timely and coordinated manner. This represents an operational gap – a distance between strategic intent and capability, both in terms of disrupting[3] adversarial activity and enhancing societal resilience against it.

In this context, the term **operationalization** refers to building an operational and actionable capability that can operate under conditions characterized by speed, unpredictability, and adversarial adaptation. At its core, operationalization means turning strategic frameworks and normative commitments into coordinated, repeatable, and measurable actions.

The FIMI threat environment is transnational and technology-mediated, cutting across legal jurisdictions, institutional mandates, and societal domains. Therefore, operationalization cannot solely use traditional linear policy pipelines or traditional top-down hierarchical structures for its implementation; instead, operationalization needs to rely on a distributed, whole-of-society, integrated operating model that combines all the state institutions, civil society organizations, independent media and private sector actors.

Extensive frameworks at the EU and NATO levels already exist, [4] and the core challenge is not the absence of frameworks and tools, but the absence of their systematic and coordinated use. Legal instruments, regulatory mechanisms, analytical capacities, and communication strategies already exist. However, they lack connective structures that would systematically and repeatedly translate detection into action and action into sustained impact.

**Operationalization should enable the following capabilities:**

- **Coordination** - information and responsibilities move efficiently among institutions, sectors, and national boundaries;
- **Repeatability** - responses are standardized, scaled, and applied consistently across cases;
- **Measurability** - clear indicators of effectiveness, including the ability to assess disruption outcomes and resilience gains;
- **Adaptability** - the system can respond to evolving tactics and technological changes;
- **Social legitimacy** - ensuring that responses are perceived as credible, transparent, and trustworthy by the public, thereby preventing emotional manipulation.

Within the operationalization model two interrelated dimensions of action emerge: **resilience and disruption**, both representing complementary operational logics embedded within the same system.

Disruption focuses on the ability to act against the infrastructure of FIMI. Information manipulation campaigns rely on networks of financing, distribution channels, and proxy actors. These elements can be identified and targeted through existing legal, regulatory, and technical instruments. Operationalization, in this sense, requires the systematic use of these tools to constrain adversarial capabilities.

At the same time, operationalization must address the conditions that enable FIMI to succeed. This is the domain of resilience. A resilient information environment reduces the effectiveness of manipulation by limiting its ability to influence public perception and behavior. However, resilience cannot be treated as a passive societal feature. Operationalizing resilience involves shaping the information environment proactively: it should be actively built through policies, education systems, strategic communication, and institutional practices. Thus, disruption reduces the exposure of societies to manipulation, while resilience reduces the impact of the manipulation that occurs.

The effectiveness of this model ultimately depends on the operationalization of the whole-of-society approach. It requires the integration of a diverse set of actors into a system with clearly defined roles, shared protocols, and trusted channels of cooperation.

**This includes:**

- Institutionalized coordination mechanisms that ensure information flows from detection to decision and response;
- Shared standards for data exchange and attribution, enabling interoperability across actors and jurisdictions;
- Trust-based networks that allow for rapid collaboration between public institutions, civil society, and private sector entities;

In this model, effectiveness depends on connectivity, agility, and access to relevant information. Civil society actors, for example, often serve as early detectors of emerging FIMI activity, while state institutions possess enforcement capabilities. Operationalization requires linking these functions into a continuous and sustained process.

Operationalization in the FIMI context is about utilizing what is already for use. It does not mean creating new frameworks but ensuring that existing ones function as an integrated system. This means closing the gap between knowledge and action, aligning tools with processes, and enabling coordinated responses at the speed required by the threat environment.

## Looking for a more active model of deterrence within the European Democracy Shield - the B5+ as the "operational engine"

### Examining the EU's institutional initiatives and development of the European Democracy Shield

The EDS represents the strategic culmination of the European Union's long-standing institutional efforts to safeguard its democratic integrity against the dual pressures of internal instability and external hybrid threats, particularly FIMI.[5] The EDS serves as a comprehensive pan-European "legislative architecture" that builds upon the foundations of the 2020 European Democracy Action Plan [6] and the 2023 Defence of Democracy Package.[7] Following the 2024 European elections, Commission President Ursula von der Leyen transformed these evolving strategies into a centralized structure,[8] a move solidified by the European Parliament's establishment of the Special Committee on the European Democracy Shield [9] and a formal joint communication in late 2025.[10]

This shield is operationalized through four primary pillars that foster a "whole-of-society" defense system, beginning with **the European Centre for Democratic Resilience**, which is intended to act as the collective's operational heart by pooling resources to detect and respond to threats. This is complemented by **initiatives to safeguard the information space** through the enforcement of the Digital Services Act and the AI Act, alongside the creation of an independent European Network of Fact-Checkers to maintain the integrity of public debate. Furthermore, the EDS focuses on **strengthening core institutions by protecting political actors and media independence** through the Media Resilience Programme, while simultaneously boosting societal resilience by investing in digital literacy and civic engagement for all citizens. Other whole-of-society actions include a high-level event on democracy and an annual award for democratic innovation, and support for voluntary commitments by the private sector to build a business coalition for democracy.

**Actions of the European Commission, to be rolled out by 2027, fall under four main categories:**

- A new European Centre for Democratic Resilience;
- Safeguarding the integrity of the information space;
- Strengthening our institutions, fair and free elections, and free and independent media;
- Boosting societal resilience and citizens' engagement.

During the General Affairs Council session on 24 February 2026, EU Ministers - at the invitation of the Commission and the Council Presidency - **officially inaugurated the European Centre for Democratic Resilience (ECDR**). Structurally, the Centre is envisioned to function as a collaborative hub between the European Parliament, the Commission, and the European External Action Service, with the active participation of all 27 Member States.

The ECDR is designed as an evolving, voluntary hub where Member States collaborate based on their specific needs and national expertise. Working in tandem with the EEAS Rapid Alert System, the Centre unifies existing networks and intends to host a dedicated stakeholder platform to facilitate dialogue between EU institutions, academia, and civil society. The newly established European network of fact-checkers will also be another component of this ecosystem. Ultimately, the Centre has an ambition to transform reactive defenses into a proactive early warning system, enhancing situational awareness and providing the operational support necessary for rapid, coordinated responses to disinformation and hybrid threats.

One of the expected key elements in the ECDR scheme is **the Stakeholder Platform,** which is announced to constitute a vital bridge between the EU's institutional architecture and the real-world expertise needed to counter hybrid threats. As the ECDR relies on voluntary cooperation, a decentralized network of civil society, researchers, and media practitioners is an "operational necessity." It proposes a fundamental shift toward co-development, where stakeholders are expected to have an opportunity to directly shape the EU's FIMI blueprints and crisis protocols. This approach is backed by a "respond-or-explain" mechanism, requiring the ECDR Board to formally justify any rejection of

stakeholder advice, thereby ensuring institutional accountability and preventing the platform from becoming a symbolic forum.

Finally, the European Commission introduced the proposal of a funding scheme. **The AgoraEU program**, which serves as the definitive financial cornerstone of the European Democracy Shield, was formally introduced in July 2025 as a centerpiece of the proposed 2028–2034 Multiannual Financial Framework (MFF). Introduction of the program signals a paradigm shift by consolidating the previously fragmented Creative Europe and CERV initiatives into a singular, high-capacity "super-program". This merger brings together support for the cultural, media, and audiovisual sectors with initiatives dedicated to the rule of law, fundamental freedoms, and the fight against discrimination and gender-based violence.

By early May 2026, this structural evolution had redefined the role of the cultural and civic sectors, transitioning them from isolated soft power assets into integrated components of national and democratic security. This unified framework now provides a streamlined "single point of entry" designed to empower independent media, artists, and civil society actors as the primary frontline defenders of the European information space. The AgoraEU has advanced to a critical stage in the 2028–2034 Multiannual Financial Framework (MFF) negotiations.[11] There were several innovative revenue proposals,[12] to bridge the gap, such as reinvesting digital fines from the Digital Services Act (DSA) and AI Act, or redirecting funds withheld via the Rule of Law Conditionality Mechanism into the program to protect independent media and civil society on the ground.

While the European Union has framed the EDS as a decisive "whole-of-society" defense, critical analysis from policy observers suggests that the framework occasionally "papers over the cracks," relying heavily on non-binding "soft-law" tools and voluntary coordination rather than the aggressive legislative measures some experts advocated for.[13] This tension is most evident in the governance of the European Centre for Democratic Resilience. Although the European Parliament and various NGOs pushed for a fully independent agency, its final structure remains under Commission management, leading to expert warnings that the hub risks becoming a coordination center rather than a decisive operational authority.[14] Furthermore, experts have pointed out an internal blind spot, arguing that the shield focuses on foreign threats while potentially side-stepping the politically sensitive issue of democratic backsliding within Member States themselves.

Based on the feedback from Counter Disinformation Network members[15] regarding the European Democracy Shield, respondents view national efforts against FIMI as insufficient, noting that while legislation exists, enforcement remains slow and ineffective. This systemic weakness is exacerbated by a critical lack of resources, with 61% of stakeholders identifying **sustainable funding as the primary bottleneck** hindering talent retention, technological scaling, and coordination. Furthermore, there is a strong call to shift the focus from reactive, election-cycle interventions to **the establishment of permanent resilience structures and proactive threat prevention.**

While the EDS provides the necessary legal and structural framework for all 27 Member States, the question is how to make the whole new system work in practice. During the seminar in Helsinki, our assumption was that one of the key measures to **success is proactive leadership of frontline entities**, such as the B5+ corridor, to translate the high-level mandate into immediate operational realities on the ground.

## Reframing the B5+ countries as the "operational engine" for the EDS actions under four key pillars of EDS

To effectively counter FIMI and hybrid threats aimed at impacting democratic processes, the European Union should operationalize a model of **deterrence by punishment** and **deterrence by resilience**. By raising the costs for threat actors on conducting FIMI activities and strengthening the cognitive immunity of our citizens, we should demonstrate to adversaries that their operations are destined to fail. This requires a "whole-of-society" approach within the "whole-of-Europe" framework: a long-term commitment to connecting sectors, engaging citizens, and rebuilding trust in public institutions so that societal cohesion persists even across political divides.

Considering the regulatory framework and the current state of EDS operationalization, one of the central objectives of the seminar was to analyze the perspectives of the B5 countries and incorporate Ukrainian experience into broader regional resilience and response. By integrating Ukrainian experience into regional coordination mechanisms, the EU improves its capacity to detect and respond to hybrid threats at earlier stages, before they can produce broader destabilizing effects across the European information environment.

The countries of the B5+Ukraine region possess extensive operational experience in identifying, analyzing, and responding to hybrid threats under sustained pressure. This frontline exposure provides practical lessons that are directly relevant to the further operationalization of the European Democracy Shield. By drawing on these experiences, the EU can strengthen its capacity for earlier detection, coordinated response, and long-term societal resilience in the information environment.

In this context, the B5 should not be viewed merely as recipients of EU policy, but as key contributors to its operational development. Positioned at the frontline of hybrid threats and foreign information manipulation, the region can serve as an operational engine of the European Democracy Shield, translating strategic frameworks into adaptable practices, coordination mechanisms, and resilience models applicable across the broader European context:

### 1. A new European Centre for Democratic Resilience

The B5 can shape its mandate by advocating for **a "hub-and-spoke" model where the Centre's core intelligence is fed by existing regional excellence centers** (such as the NATO StratCom COE in Riga or Hybrid CoE in Helsinki)., The Centre's mandate can be steered toward operational actionability by embedding B5 liaison officers within the Centre's leadership and prioritizing real-time information sharing and cross-border crisis response. The Centre should serve as the primary mechanism for scaling the preparedness model based on the Finnish framework, and the "Baltic model" of resilience. The B5 could lead the Centre's Stakeholder Platform, ensuring that civil society organizations are active partners in project implementation.

### 2. Safeguarding the integrity of the information space

Adoption of a proactive counter-FIMI architecture requires the B5+ to lead on prebunking and technical attribution. The region can drive the development of cross-border early detection systems. In terms of platform regulation, the B5+ should act as a collective "enforcement bloc", utilizing the Digital Services Act (DSA) to demand that platforms provide faster, language-specific moderation and transparency tools that account for the nuances of regional manipulation tactics. Building on the work of DG JUST and organizations like IDEA International, the region can champion an "Electoral Resilience

Facility". This would focus on building the institutional infrastructure for risk monitoring, ensuring that detection is constant rather than limited to the weeks preceding an election.

### 3. Strengthening institutions, elections, and independent media

The integrity of our democratic infrastructure depends on the health of our institutional ecosystems. In the Baltic Sea region and beyond, the most pressing risks are "war fatigue" and the cognitive vulnerability of the populace. We must treat democratic resilience as a form of "welfare" for the 21st century - particular attention should be given to smaller language markets, where independent media outlets often face structural financial pressures and increased exposure to external influence operations In this context, the region could advocate for EU-wide Small Market Media Subsidies, aimed at ensuring that high-quality journalism remains viable in vulnerable media environments and information vacuums are not easily exploited by adversarial actors. Building on collaboration between Finland and DG JUST, the B5 could help deploy a **unified framework for protecting election authorities,** ensuring that the "Whole-of-Europe" notion is backed by hardened institutional capacity and rigorous legal frameworks against adversarial influence. The B5+ could also promote common standards for transparency in political funding and mechanisms for identifying vulnerabilities that may be exploited by FIMI actors.

### 4. Boosting societal resilience and citizens' engagement

The B5+ promotes a specific model of resilience, one in which civil society acts as a vital component of early warning and societal preparedness. The EU should amplify regional successes such as civil society "Elves" networks[16] monitoring disinformation, and decentralized media literacy programs embedded in both schools and workplaces. These local resilience networks serve as a bridge to broader engagement, demonstrating that a resilient democracy is built on civic tech tools and grassroots participation that can be exported as a blueprint for the rest of the EU.

Building on the momentum of the B5 corridor, the region is positioned to integrate their frontline expertise with the high-level findings of the 2026 European Citizens' Panel on Preparedness and Resilience.[17] This EU-wide panel, launched in March 2026, brings together 150 randomly selected citizens from across all 27 Member States to provide the Commission with direct recommendations on fortifying democratic systems against systemic crises, including pandemics, climate disasters, and hybrid warfare. By utilizing

the insights generated from this pan-European assembly, the B5+ corridor can refine its own resilience models, ensuring that their operational "high-readiness engine" is perfectly aligned with the democratic expectations and collective vision of the broader European population.

Resilience, however, does not come for free. It requires intentional investment in human capital — an "Agora" for democratic exchange with financial support. Based on national experience, the B5 region should strongly support fostering a **business coalition for democracy**, where private companies are encouraged to make voluntary commitments to uphold democratic values and social responsibility. These private and pro bono contributions are intended to complement the budget proposed for the AgoraEU program, ensuring that even if public funds are delayed in MFF negotiations, a secondary layer of private resources and professional expertise remains available to protect democratic "first responders".

## B5+ regional perspective

The regional level serves as an essential juncture between European-level strategy and national-level action. While the EU frameworks like the European Democracy Shield provide strategic direction and seek to align existing instruments, the way they are ultimately implemented across countries and sectors relies on effective coordination. Within this framework, the Baltic Sea region serves as an excellent operational environment.

The Baltic Sea region has a number of structural advantages, including first-hand experience in countering hybrid threats stemming from its continuous exposure to hostile pressures, as well as a strong network of civil society groups, independent media, and investigative journalists, who have advanced their ability to detect and analyze FIMI. Furthermore, the region is a hotspot for various regional and international institutions, compromising a broader network of EU-level projects and initiatives with scope focused specifically on countering hybrid threats, strategic communications and cyber security.

Separately, these assets represent a greatly capable ecosystem. However, the challenge lies in an efficient cooperation within the system of various mandates, governance frameworks and coordination formats. Therefore the existence of capabilities does not automatically translate into a consistent regional response - without structured coordination and integrated response mechanisms, even advanced actors may operate in parallel rather than as part of a fully integrated system.[18]

Although monitoring and analysis have improved significantly, there remains a significant gap between detection of FIMI activities and the ability to respond to them effectively at the regional level. Civil society organizations, research institutions, and strategic communicators often produce highly sophisticated analytical products. However, the translation of those products into concrete responses, whether regulatory, legal, or communicative, is often inconsistent and delayed, which leaves FIMI networks with operational gaps in which they can adapt, persist, and create new vulnerabilities within the information environment.

The challenge of coordinating responses to FIMI does not stem from a lack of tools, but from limitations in coordination across systems. Throughout the EU, horizontal

cooperation between Member States varies widely based on differences in legal systems, institutional structures, and perception of threats. Compounding this problem is a vertical disconnect between EU frameworks for addressing FIMI and the implementation of those frameworks at the national levels, which slows down the flow of information and feedback across levels of government. Simultaneously, the limitations stemming from the lack of effective coordination mechanisms between government agencies, civil society organizations, platforms, and research institutions hampers effective cross-sectoral interaction; while there are examples of effective coordination within specific sectors, sustained cross-sector interoperability has proven to be challenging, thus limiting the flow of information from detection and attribution to timely coordinated responses.

However, the lack of systemic coordination does not imply its complete absence, especially at regional level. On the contrary, the Baltic Sea region demonstrates some of the most advanced forms of cooperation in Europe. However, these efforts are often concentrated within specific domains and do not yet amount to a fully integrated, system-level response.

The mix of advanced capabilities, such as characterized by a "total defense" mindset that integrates civilian and military sectors, and remaining coordination challenges makes the region well suited to drive operationalization at the European level. The B5 does not lack the tools or experience, but rather integration and execution are their main challenges. On the other hand, rather than identifying a perfect response model, the region offers one of the most advanced operational frameworks currently available - one that is already addressing the core challenges of coordination, adaptation, and implementation, and is therefore well positioned to develop and refine the approach that can be scaled and adopted across other EU member states.

On the regional level, reframing civil society as operational actors through incorporating them into the response chain, and ensuring their outputs contribute directly to downstream actions across institutional domains is a prerequisite for regional operationalization. Across the region, civil society actors have developed increasing capabilities to detect influence operations. This shifts citizens from passive recipients of information to active participants in the information environment. In this context, citizens are not only targets of manipulation, but contributors to resilience, capable of identifying, sharing, and contextualizing emerging manipulation patterns.

Within the context of citizen engagement, engaging the youth remains one of the key areas of activities. Youth forums, leadership programs and other regional initiatives supported by organizations such as the Council of the Baltic Sea States highlighted the value of activating youth as contributors to building resilience.[19] Similarly, various actors are working to integrate digital competencies into their training and educational programs for media literacy and analysis. Collectively, these initiatives not only enhance long-term societal resilience, but also create new means of navigating an increasingly complex information ecosystem.

Furthermore, broader youth engagement carries a clear strategic dimension. They are often the first to engage with new platforms, formats and modes of communication as influence operations evolve. Considering that they will likely see tactical and narrative changes at the earliest stage of their occurrence, they are well positioned to identify such changes. Thus, greater youth engagement enhances the adaptive capacity of the response system, increasing both early detection and the development of credible counter-narratives.

### Technology as a cross-cutting domain

The evolving developments of technologies, particularly in the area of artificial intelligence, are fundamentally transforming the FIMI environment. AI utilizes major advances in the ability to generate, disseminate, and target large volumes of content, which essentially enables manipulation campaigns to happen at an unprecedented rate, volume, and complexity. Simultaneously, AI provides respective tools with which to detect, analyze, and respond to manipulated content, creating the dual-use dynamic.

More and more, information is conveyed to the public via algorithmic systems that filter and prioritize content in order to create an individual context. Thus, not only does the use of these systems determine how much of the underlying information is made "visible," but they also dictate how the information becomes understood upon being exposed to it. Consequently, those entities that exert influence over algorithmic systems are strategically significant, as their exertion of influence creates and influences the information environment and the perceptions derived from that information environment.

Competition in the information domain is therefore no longer limited to narratives, but also extends to the systems through which information is curated and understood. At the

same time, these systems themselves are becoming targets. Data poisoning and manipulation of training datasets can distort analytical outputs and undermine trust in automated systems, introducing another vector of vulnerabilities into the response framework.

Addressing these challenges requires investment and defenses. Regional actors should strengthen technological capabilities for detection and analysis, while also ensuring the integrity of these systems. Due to the variation in technological capabilities by country, strengthening regional cooperation is critical to avoid fragmentation of technology within the region and ensure that technology positively impacts collective resilience.

### From ecosystem to system

Within the context of the Baltic Sea region, connecting existing structures into a coherent operational system requires translating the principles of operationalization into applicable regional practices. Coordination should be institutionalized through linking detection, analysis, and response. Shared practices and protocols that are consistently applied across cases are needed for repeatability. Measurability requires indicators that evaluate both disruption outcomes and resilience gains. Continuous learning, as well as the capability to adapt and respond to changes in threats, is essential for adaptability.

A fundamental aspect of this model will be the establishment of faster and more reliable channels from information to action. This includes integrating civil society into response processes, strengthening cross-border information sharing, and ensuring that regional efforts are aligned with, and capable of informing, EU and NATO frameworks. In this sense, the effectiveness of the regional model depends not on the creation of new initiatives, but on the ability to activate and connect existing capabilities into a functioning system.

The Baltic Sea region already functions as a highly capable ecosystem of actors engaged in countering FIMI. However, ecosystems do not automatically produce coordinated outcomes. Without structured integration, their impact remains fragmented. The transition from ecosystem to system is therefore the central task of regional operationalization. The necessary transition involves moving from parallel activities to coordinated actions; from independent capabilities to integrated processes; and from reactive responses to proactive strategies. By putting together actors, tools, and

processes into a coherent operational framework, the region can act in a sustained and effective way and drive the EU in defending the information space.

## Polish-Ukrainian relations as a battlefield of information warfare

Against this backdrop, Poland and Ukraine illustrate the kind of operational experience that is adaptable and scalable within the broader B5+, as well as European frameworks. Significance of both states stems from geography, history, military cooperation, humanitarian support, Poland's role as a logistical and political hub for assistance to Ukraine, and Ukraine's position in the future European security order. From the perspective of the Russian influence apparatus, weakening mutual trust between Poles and Ukrainians is not a secondary objective. It is one of the conditions for limiting the West's ability to sustain a coherent policy towards Russian aggression. The sustained exposure has also forced both states to adapt to a persistent hostile information environment.

### Information warfare as an operation against perception and emotion

Information warfare is no longer merely a contest over facts. Its primary objective is increasingly the shaping of perception: how societies interpret events, assess the intentions of allies, evaluate their own institutions, and respond emotionally to crises. In this sense, disinformation should not be understood only as the circulation of false or misleading content. It is a strategic instrument designed to influence the cognitive and emotional environment in which citizens, institutions, and decision-makers operate.

The purpose of hostile information activity is often not to convince an audience of one coherent alternative reality. More frequently, it seeks to generate fear, anger, distrust, fatigue, resentment or a sense of betrayal. These emotional states are operationally useful because they weaken social cohesion, reduce confidence in allies, and make long-term cooperation politically more costly.

For more than a decade, Russian information operations have targeted the emotional and historical foundations of Polish-Ukrainian cooperation. The logic is clear: if Poland and Ukraine can be made to perceive each other through suspicion, resentment and unresolved historical trauma, their ability to act together will be reduced. The attack is therefore directed not only at specific facts, but at the mutual image of both societies.

### Poland and Ukraine as case studies in defending the information space

The Polish and Ukrainian experiences should be treated not only through the lens of bilateral relations, but as two complementary case studies of societies exposed to long-term hostile information operations. Both states have been targeted by the Russian influence apparatus for more than a decade, although the nature, intensity and operational objectives of these activities differ. Ukraine has been subjected to direct wartime information aggression aimed at undermining state legitimacy, military morale and social cohesion. Poland, in turn, has been targeted as a frontline NATO and EU state, a key logistical hub for assistance to Ukraine, and a society whose public support is essential for sustaining allied policy.

This distinction is important. The analytical focus should not be exclusively limited to how Russian propaganda targets Polish-Ukrainian relations, but how Poland and Ukraine developed different models of institutional and civic resilience to hostile influence.

Ukraine offers a case of information defense under conditions of full-scale war, where strategic communication, rapid public messaging, digital mobilization and civil society monitoring have become elements of national survival and resistance. Poland offers a case of democratic resilience in an allied state exposed to persistent attempts to weaken public trust, polarize society, discredit support for Ukraine and exploit sensitive domestic debates.

Seen in this way, both cases provide practical lessons for a broader regional and European framework. They show that defending the information space requires more than fact-checking individual falsehoods. It requires institutional coordination, cooperation with civil society, early warning, strategic communication, media literacy, platform accountability and sustained public education. These lessons are particularly relevant for a potential B5+ format, where Poland, Ukraine and regional partners could develop shared methodologies, coordinate early warning systems, and build a common resilience architecture against foreign information manipulation and interference.

### The case of Poland: resilience in an allied frontline society

In the Polish case, Russian information operations have focused[20] on weakening public support for Ukraine, undermining trust in state institutions and portraying allied commitments as costly, risky or contrary to national interests. The objective is not necessarily to make Polish society openly pro-Russian. Given Poland's historical

experience and broad awareness of Russian imperial policy, such an objective would have limited prospects. A more realistic and operationally useful goal is to increase fatigue, suspicion, and emotional resistance to continued support for Ukraine.

This has been pursued through narratives exploiting economic grievances, migration-related tensions, historical disputes, political polarization and fears connected with security. Issues such as grain imports, transport, labor markets, refugee assistance, defense spending or the risk of escalation are used as material for manipulation. In this model, real policy challenges are reframed as evidence of betrayal, incompetence or external manipulation. A sectoral dispute is presented as a national grievance; a social cost becomes proof that solidarity is irrational; a political debate becomes a weapon against allied cohesion.

The Polish case also demonstrates the importance of public institutions working with civil society rather than acting in isolation. State communication is necessary, but insufficient on its own. Civil society organizations, independent media, fact-checkers, researchers and local actors are often better positioned to identify emerging narratives, monitor niche channels and reach audiences that may distrust official messaging. Within Poland's ecosystem of actors engaged in countering FIMI, the business sector plays an important role. The social responsibility of the business sector extends beyond philanthropy, and includes active engagement in strengthening social resilience. Businesses and corporations possess the resources, organizational competencies and the ability to build cross-sectoral partnerships, through which they can support the development of civic education, digital and media competencies, critical thinking and social capital. These activities are particularly important within the context of information threats, as they increase citizens' ability to independently assess the credibility of information, reducing one's susceptibility to manipulation and disinformation.

Business engagement is not only limited to the aforementioned capabilities. Supporting initiatives that build social trust, strengthen local communities, and improve the mental well-being of citizens are equally important elements of the sector's contribution to resilience-building. These factors are increasingly recognized as the foundation of social resilience, understood as society's ability to adapt and effectively respond to crisis situations. For instance, the work of the PZU Foundation implements programs supporting education, the development of social skills, mental health, and civic

engagement, which demonstrates that the private sector can serve as a strategic partner in building social resilience and strengthening the state's information security. [21] At the same time, the effective coordination of existing efforts requires the implementation of a whole-of-society model, in which the state provides strategic direction while civil society and private-sector actors contribute to monitoring, analysis, education, and local-level engagement.

### The case of Ukraine: information defense under wartime pressure

Ukraine represents a different, but equally important, case study. Since 2014, and especially after the full-scale invasion in 2022, Ukraine has faced information operations designed to weaken the state's legitimacy, erode public morale, discredit the armed forces, generate panic and undermine international support. Russian narratives have targeted not only military developments, but also corruption, mobilization, energy infrastructure, humanitarian suffering, displacement and trust in political leadership. [22] [23] [24]

The Ukrainian experience shows how information defense becomes inseparable from national defense. In wartime conditions, the speed and credibility of communication are critical. Public institutions must counter panic, explain risks, maintain trust, and respond to hostile narratives without overloading society with fear. At the same time, Ukrainian civil society, investigative communities, volunteer networks, digital activists and independent media have played an essential role in documenting Russian aggression, exposing manipulation, supporting international advocacy, and strengthening social resilience.

This case highlights the importance of distributed resilience. No single institution can defend the information space alone. Effective response depends on networks: public authorities, local communities, journalists, OSINT groups, digital volunteers, educators and international partners. Ukraine's experience also demonstrates that counter-disinformation is not only defensive. It can support strategic communication, international solidarity and the documentation of war crimes, while reinforcing the legitimacy of democratic resistance.

### Effective methodologies: from reaction to resilience

The Polish and Ukrainian cases point to several practical methods that can be developed jointly and expanded regionally. The first is an early warning system based on narrative

monitoring, including identification of recurring themes, emotional triggers, coordinated amplification and cross-platform dissemination. The second is prebunking, which prepares audiences for manipulation techniques before specific falsehoods appear. The third is strategic communication that explains policy decisions clearly, quickly and empathetically, especially when social costs are involved.

The fourth methodology is civil society integration. NGOs, fact-checkers, research centers, local media and community organizations should be treated as core elements of the resilience system. The fifth is media and AI literacy, especially among young people, journalists, educators and local leaders. The sixth is structured cooperation with social media platforms, including escalation channels for manipulated audiovisual content, impersonation, coordinated inauthentic behavior and AI-enabled disinformation, among other tactics.

Together, these methodologies move the response beyond reactive debunking. They create a preventive and adaptive model of information resilience.

## The Polish Council for Resilience to International Disinformation as a systemic model

In this context, the Polish Council for Resilience to International Disinformation, [25] established at the Ministry of Foreign Affairs, represents an important institutional model. Its significance lies not simply in the creation of another advisory body, but in the recognition that countering disinformation requires cooperation across government, civil society, academia, local authorities, media, and the private sector.

The strength of this model is that it addresses one of the main weaknesses of many national counter-disinformation systems: fragmentation. State institutions have legal, diplomatic and security instruments. Civil society organizations monitor adversarial narratives and tactics and often reach communities that are less receptive to official communication. Academic institutions provide research and methodology. The technology sector can provide analytical tools. Local authorities understand community-level vulnerabilities. A council-based model creates a space for systematic exchange of knowledge, threat assessment, policy recommendation and practical cooperation.

This approach is effective for several reasons.

First, it strengthens the legitimacy of state action. Counter-FIMI policies are more credible when they are developed in dialogue with independent experts and civil society, not imposed solely through administrative communication. Second, it enables faster identification of emerging threats. Third, it helps shift the response from reactive crisis management to long-term resilience building. The aim is not only to correct false claims, but to reduce the vulnerability of society to manipulation. Fourth, it creates a bridge between strategic analysis and practical implementation. Recommendations can be translated into training, educational programs, communication procedures, grant mechanisms and cooperation with platforms.

The Polish model is therefore particularly relevant for states exposed to long-term hostile information activity. It recognizes that information security is not the responsibility of one ministry, one agency or one group of experts. It is a whole-of-society challenge.

The experience developed through Polish resilience coordination mechanisms could also inform the further operationalization of emerging EU-level resilience structures, including the European Centre for Democratic Resilience. The Polish experience demonstrates the value of structured cooperation between public institutions, civil society, researchers, independent media, and strategic communication actors in identifying vulnerabilities and responding to hostile influence activities.

Embassy of the Republic of Poland in Helsinki
POLISH PRESIDENCY 2025–2026
FUNDACJA
Financed by the PZU Foundation

## Endnotes

[1] Most updated information on EDS from the European Commission https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660 and European Parliament: https://www.europarl.europa.eu/legislative-train/package-european-democracy-action-plan/file-european-democracy-shield.

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

[3] See European External Action Service, 4th Report on Foreign Information Manipulation and Interference (FIMI), which highlights a shift toward disruption-oriented responses, including exposure of networks, attribution, and coordinated countermeasures. While this marks an important evolution from earlier monitoring-focused approaches, disruption has yet to be translated into a fully operational model. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.

[4] See i.e. European External Action Service (EEAS) (2026) *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)*. Available at: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104617.; European Commission (2025) *Digital Services Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act.; European Parliament (2024) *Defence of Democracy Package*. Legislative Train Schedule. Available at: 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*. Available at: 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*. Available at: https://stratcomcoe.org/.

[5] The EDS further builds on the EU's evolving work to counter FIMI, led by the European External Action Service (EEAS) since 2015, as well as the EU's regulatory framework to threats against democracy, eg. Digital Services Act (DSA); the Artificial Intelligence (AI) Act; regulation on transparency and targeting of political advertising (TTPA).

[6] European Commission (2020) *European Democracy Action Plan*. Available at: https://ec.europa.eu/commission/presscorner/detail/ga/ip_20_2250.

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

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

[9] European Parliament (2024) *Procedure File: European Democracy Shield*. Available at: https://oeil.europarl.europa.eu/oeil/el/procedure-file?reference=2024/2999(RSO).; On 18 December 2024, Parliament voted to set up a Special committee on the European Democracy Shield (EUDS).

[10] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025) *Joint Communication*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0791.; On 12 November 2025, the Commission and the High Representative published a joint communication on the 'European Democratic Shield: Empowering Strong and Resilient Democracies'.

[11] The European Parliament formally adopted its interim position on April 28, 2026, proposing a €10.72 billion budget—a 25% increase over the Commission's initial €8.5 billion proposal.

[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*. Available at: 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?* Available at: 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*. Available at: 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] Feedback collected in Nov. 2025, CDN monthly newsletter, February 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*. Available at: https://www.gmfus.org/news/role-cyber-elves-against-russian-information-operations.

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

[18] See European External Action Service, 4th Report on Foreign Information Manipulation and Interference (FIMI) (2026), which advances the FIMI Deterrence Playbook and emphasizes linking analysis to coordinated responses and operational tools. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web

%20version_1.pdf; NATO Strategic Communications Centre of Excellence & Hybrid CoE, Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework 'DISARM' (2022), which highlights the need for standardized frameworks to enable coordinated multi-actor responses. https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253.

[19] See Council of the Baltic Sea States (CBSS) youth engagement initiatives. 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*. Available at: https://dfrlab.org/2025/08/25/election-report-assessment-of-foreign-manipulation-and-interference-in-the-2025-polish-presidential-election/ .

[21] See PZU Foundation's activities, i.e. 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*. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/.

[23] Atlantic Council (2023) *Undermining Ukraine*. Available at: 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*. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/.

[25] Ministry of Foreign Affairs of the Republic of Poland (2025) *Council for Resilience: Joint Initiative by MFA and Civil Society Organisations Against International Disinformation Begins Operation*. Available at: https://www.gov.pl/web/diplomacy/council-for-resilience-joint-initiative-by-mfa-and-civil-society-organisations-against-international-disinformation-begins-operation

**The Casimir Pulaski Foundation** is an independent, non-for-profit, non-partisan Polish-think tank conducting research on different aspects of European and Transatlantic security, with a special focus on Central and Eastern Europe.

The Foundation brings together dozens of international experts in various fields (foreign policy, defence, energy, democratic resilience) and publishes analysis describing and explaining international events, identifying trends in the European and Transatlantic security environment and recommending solutions for government decision-makers and the private sector.

The Casimir Pulaski Foundation is also the initiator and main organizer of the Warsaw Security Forum conference, which since 2014 annually gathers over 1500 stakeholders from more than 60 countries in order to elaborate shared responses to common transatlantic security challenges.

Each year the Foundation presents the "Knight of Freedom" award to outstanding figures who contribute to the promotion of the values of General Casimir Pulaski, such as freedom, justice and democracy. It is also the home to the Polish branch of the Women in International Security network.

The Casimir Pulaski Foundation has been ranked as the first among Polish Think Tanks dealing with defence and national security according to the 'Global Go To Think Tank Index' report in 2018, 2019 and 2020 respectively. The Foundation also has a status of a partner organization of the Council of Europe.

For the sake of the highest standard and quality of the research carried out and valuing the reliability of analytical work, the Casimir Pulaski Foundation obliges its employees and collaborators to comply with the European Code of Conduct for Research Integrity of 2023.