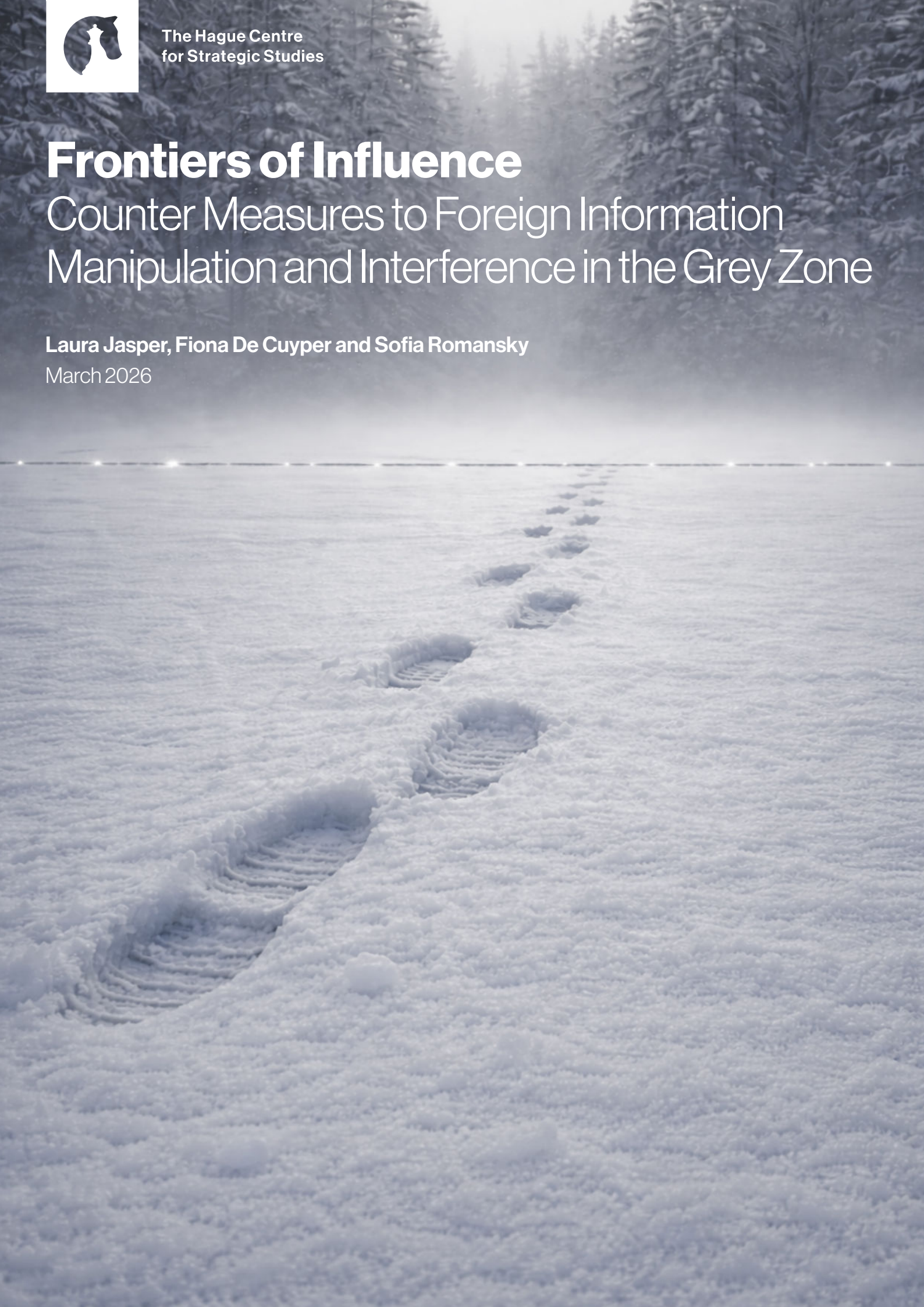


The Hague Centre
for Strategic Studies

Frontiers of Influence

Counter Measures to Foreign Information Manipulation and Interference in the Grey Zone

Laura Jasper, Fiona De Cuyper and Sofia Romansky

March 2026

The Hague Centre
for Strategic Studies

Frontiers of Influence

Counter Measures to Foreign Information Manipulation and Interference in the Grey Zone

Authors:
Laura Jasper, Fiona De Cuyper and Sofia Romansky

Contributors:
Lennart Cramer and Emma Genovesi

Quality Assurance:
Paul Sinning

The cover image was AI-generated
with OpenAI's ChatGPT.

March 2026

The research for this report was completed in December 2025. Events or developments that occurred between completion and publication did not influence the findings.

The authors would like to specifically thank Björn de Heer and all participants of the Strategic Capability Game for sharing their expertise and experience which have significantly contributed to the overall content and quality of this research paper.

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, not should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

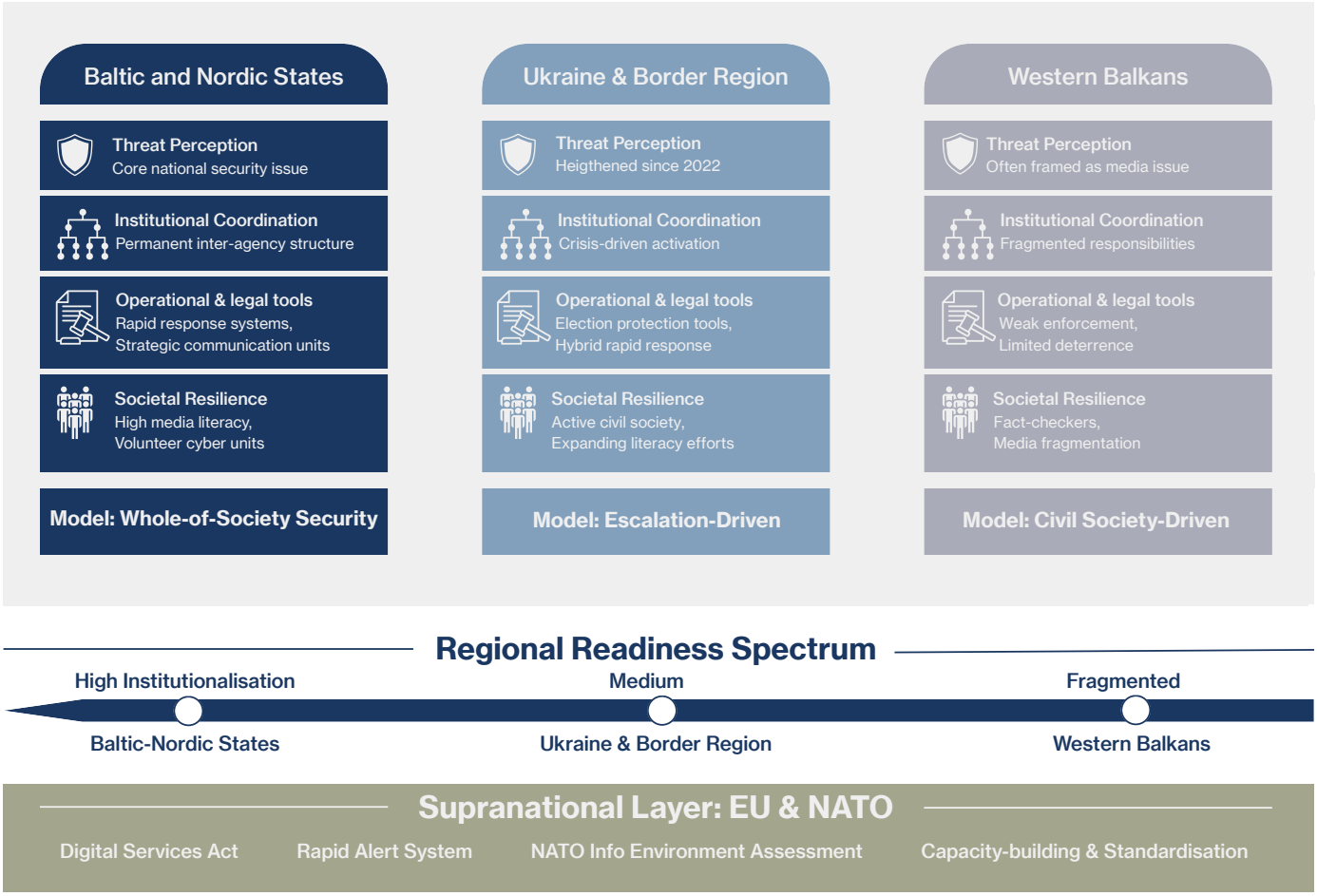
Table of Contents

Executive Summary

In an era where more than 70% of the world is online, the information environment has become a primary arena for geopolitical competition. Our latest report explores how Foreign Information Manipulation and Interference (FIMI) is moving beyond "fake news" to trigger real-world behavioural effects.

Rather than a traditional linear study, this report functions as a comparative volume of national experiences across Europe's Eastern borders. Based on a comparative study of 10 nations, stretching from the Baltic-Nordic region to the Western Balkans, the report identifies three distinct "Response Models" currently shaping European security:

Comparative Regional Readiness Against FIMI



This schematic overview compares the regional approaches to counter Foreign Information Manipulation and Interference (FIMI) across the three distinct European contexts analysed in this report: the Baltic-Nordic states, Ukraine and its border region, and the Western Balkans. The overview illustrates the clear variation in institutionalisation, coordination capacity, and societal resilience.

The Baltic-Nordic states (Estonia, Lithuania, Finland) demonstrate the highest level of readiness, characterised by permanent inter-agency coordination, embedded strategic communication structures, strong legal enforcement tools, and deeply integrated whole-of-society models. Ukraine and its neighbouring states (Poland, Moldova, Romania) display tiered readiness: Ukraine itself operates at a highly integrated wartime level, while Poland, Moldova and Romania show medium but uneven institutionalisation, often activated during electoral or crisis periods.

In contrast, the Western Balkans (Albania, North Macedonia, Bosnia and Herzegovina) showcase more fragmented and civil society-driven responses, with weaker enforcement capacity and structural vulnerabilities such as media fragmentation and lower institutional trust. The supranational layer at the base of the visual, in turn, highlights the enabling role of EU and NATO frameworks in strengthening coordination, regulatory alignment, and shared situational awareness across all regions.

To move beyond reactive measures, states must implement a proactive, layered defence integrating strategic communication, regulatory enforcement, and deep societal resilience. As such, the following factors come up in relation to resilience levels:

High Resilience Factors	Low Resilience Factors
Integrated state-NGO coordination	Isolated or purely reactive state action
Mandatory media literacy in schools	High reliance on unverified social media
Rapid, centralised response centres	Lack of dedicated institutional budgets
High public trust in institutions	Deep scepticism of state actors

The report concludes with the need for strategic alignment between national efforts and the supranational frameworks of the EU and NATO.

The supranational layer at the base of the visual, in turn, highlights the enabling role of EU and NATO frameworks.

1. Introduction

Information has long determined the outcome of conflict both on, and off the battlefield. As such, the contemporary information environment has become a central arena of geopolitical competition. Digital platforms and data-driven targeting have significantly widened the scope for external actors to instrumentalise information flows for strategic ends. In response to the rapidly developing information landscape, the concept of Foreign Information Manipulation and Interference (FIMI) emerged to capture the deliberate and coordinated use of information activities by external actors to influence or disrupt the political, social or institutional processes of a target state. Coined by the European External Action Service in 2022, FIMI is more concretely defined as a largely lawful yet harmful set of practices that can distort or undermine core democratic norms, political decision-making, and institutional procedures.[1]

While FIMI is often considered a digital phenomenon, its effects increasingly bridge digital-physical boundaries.

External manipulation of information is not a new phenomenon. For instance, the Soviet Union's Cold War disinformation campaigns laid much of the conceptual groundwork.[2] However, the scale, speed, reach and integration of such activities into multi-domain strategic competition is reaching new heights. As of 2023, over 67% of the world's population has access to the internet, rendering modern societies ever more reliant on digital infrastructure and media, and ever more exposed to potential FIMI activity.[3] The use of social media platforms, increasing global connectivity, artificial intelligence, and algorithmic amplification have dramatically expanded the possibilities for FIMI actors: modern FIMI operations are increasingly automated through the use of bot farms (computer programmes that imitate human online activity at scale) or large language models, for instance.[4] These activities rely on manipulative methods and are carried out across borders in a coordinated fashion by states, non-state actors, or their affiliated proxies, whether operating domestically or abroad.[5] FIMI operations can be used next to kinetic operations such as in the war in Ukraine with the goal to undermine Ukraine's resolve and battlefield successes or to discourage material support of Ukraine's allies such as Finland by framing aid as useless in the fate of an inevitable Russian victory.[6]

While FIMI is often considered a digital phenomenon, its effects increasingly bridge digital-physical boundaries, and its perpetrators increasingly operate in the physical domain. Information campaigns can mobilise protests, undermine trust in institutions, and shape public perceptions ahead of elections, inciting real-life behavioural effects. For example, the

1 *1st EEAS Report on Foreign Information Manipulation and Interference Threats* (European Union External Action, 2023).

2 Calder Walton, 'What's Old Is New Again: Cold War Lessons for Countering Disinformation', *Texas National Security Review* 5, no. 4 (2022), https://tnsr.org/2022/09/whats-old-is-new-again-cold-war-lessons-for-countering-disinformation/.

3 International Telecommunication Union, "World Bank Open Data," World Bank Open Data, n.d., https://data.worldbank.org.

4 Filip Bryjka, 'EU Adopts Approach to Countering Foreign Information Manipulation and Interference', PISM, 19 June 2024, https://pism.pl/publications/eu-adopts-approach-to-countering-foreign-information-manipulation-and-interference.

5 National Coordinator for Security and Counterterrorism, "Chimaera: An Analysis of the 'hybrid Threat' Phenomenon," 9; Romansky et al., "New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape," 4; Giannopoulos, Smith, and Theocharidou, "The Landscape of Hybrid Threats," 6.

6 Dominic Saari et al., 'The Disinformation Landscape in Finland'.

connection between online disinformation campaigns and physical protests.[7] Accordingly, FIMI should be seen not only as the dissemination of fake news or social media bots, but rather as a strategic instrument that operates across diplomacy, law, economic levers, and even kinetic proxies, effectively blurring the boundaries between "information" and "overt" action.

As FIMI actions are expanding from mere digital to more tangible consequences, including the interference of democratic processes, the need for the development of robust countermeasures besides monitoring and detection capabilities becomes increasingly more imperative. Which requires a shift away from ad-hoc efforts that remain largely reactive in nature, towards a pro-active, layered defence which integrates situational awareness, societal resilience, and regulatory disruption. This is particularly relevant for countries amongst Europe's Eastern borders, who find themselves in increasingly high-pressure environments. By evaluating countermeasures under different national contexts, we are able to look at both the frictions and synergies that exist between national and supranational mandates.

FIMI should be seen not only as the dissemination of fake news or social media bots, but rather as a strategic instrument.

The report does not advance a single linear argument like a traditional research report but rather functions as an edited volume that brings together comparative country experiences. The primary goal is to showcase what is possible across countries with varying levels of resilience, from high-capacity states like Estonia to localised NGO-driven efforts like in North Macedonia. Second, due to offensive actors tailoring their FIMI campaigns to exploit country-specific vulnerabilities and achieve context-specific goals, analysing a wide spectrum of target countries helps with understanding the diverse and adaptive nature of the threat. This also enables an assessment of how different countermeasures work under varying contexts. Understanding these diverse modalities allows for the development of a proactive, layered defence rather than a reactive, one-size-fits-all approach.

By examining different national contexts, the report highlights how countermeasures function under different political, institutional, and societal conditions. This comparative perspective supports the development of a proactive, layered defence model rather than a reactive, one-size-fits-all approach. The aim of this research is thus to establish a better shared awareness and understanding of how FIMI countermeasures are deployed in different contexts at Europe's Eastern borders. It therefore discusses the different threats and corresponding roles and responsibilities to create a more resilient information environment. In addition, it is the aim to gain insight into the possible additional capacities needed to maintain, restore or scale up the resilient functioning of countermeasures. Including who should implement actions across the national and international level.

Structurally, the report is organised into two main components:

1. Country case studies organised by region. The core of the report consists of regionally grouped country chapters. After discussing the selection of countries and regional focus, each country case study explores: (1) the historical context and contemporary geopolitics, (2) targets and tactics, (3) countermeasures and impact. This structure allows readers to both understand each national context on its own terms and draw cross-regional comparisons.

7 However, the results are mixed and hinge on a number of other factors. See Bryjka, 'EU Adopts Approach to Countering Foreign Information Manipulation and Interference', 14.

2. Rather than a conventional conclusion, the final chapter synthesises insights in the form of structured "lessons learned." These are divided into two levels:
   - Country-level assessment, focusing on institutional design, inter-agency coordination, legal frameworks, public communication strategies, and the role of civil society.
   - Strategic alignment, addressing how individual national efforts interface with and are reinforced by supranational structures, particularly within the frameworks of the European Union and NATO.

Strategic Capability Game

In October 2025 HCSS convened several key stakeholders from government, civil society, and academia from across Europe, for a Strategic Capability Game on FIMI countermeasures. The objective of the game was to test whether current roles, responsibilities, and response mechanisms are well-aligned to address complex influence operations in a cooperative manner.

Through a tabletop exercise, participants engaged in moderated discussions, responding to dynamic scenario 'injects' that simulated hybrid threats. The scenario based gamified analysis followed a set of 4 stages. The participants first discussed the situation according to the scenario. In this stage they reflected upon the most important hostile actor, their allies and motives. In the second stage, participants discussed the strategy in terms of desired end states and objectives. In the third stage, called the solution stage, the exercise unfolded around the injects that provided a fictional but realistic European security context marked by escalating tensions.

Each inject required participants to assess and deploy a range of capability cards, spanning diplomacy, operations, cyber defence, public affairs, legal measures, and engagement to formulate coherent responses across domains. The analytical approach focused on how participants' proposed actions contributed to five resilience dimensions: capacity, recovery, continuity, upscaling, and response speed.

The final stage of the game was the synchronisation stage. Here, participants debriefed together based on three questions: What would you have wished you'd have done 5 years ago, which was considered a red line back then? What is considered a red line now, but we might regret not doing in 5 years' time? In terms of threats, what are the biggest known-knowns and known-unknowns coming up in the next 5 years?

The takeaways of this Strategic Capability Game feed into the analysis of this report.

2. In the field

Russia's ongoing invasion of Ukraine illustrates that contemporary conflict extends beyond the battlefield. Alongside the application of conventional military force, the Kremlin systematically deploys what many Western analysts describe as "cognitive warfare": the use of coordinated information campaigns designed to influence the perceptions, reasoning, and behaviour of foreign populations through narratives that advance Russia's geopolitical objectives.[8] These campaigns target not only Ukraine but also its European allies, and form part of Russia's persistent efforts to interfere in Western political processes, including but not limited to elections. The study of effective responses to such FIMI operations has thus become a strategic imperative. Understanding what countermeasures work, and why, is essential for governments seeking to protect social cohesion, democratic resilience, and national security.

From NATO's eastern flank to the Western Balkans, these countries occupy strategically sensitive positions where information has become a contested domain.

Despite the expanding literature on and proliferation of countermeasures, significant gaps remain in our understanding of what works effectively. Existing comparative studies show that some countries appear more resilient to disinformation, often those with weaker populist movements or lower social media consumption, but these findings mainly point to structural factors that change slowly and do not directly assess the impact of specific interventions.[9] As a result, the field lacks a systematic analysis of concrete countermeasures designed to address the evolving threat of FIMI, and of how local political and societal conditions shape their effectiveness. Given that widely used tools like factchecking are deployed across diverse environments, understanding why they succeed in some contexts and fail in others is critical. Otherwise, cross-national disparities remain difficult to explain.

Turning from conceptual frameworks to the realities of implementation, this chapter examines how states across Europe confront FIMI in practice. The ten case studies that follow highlight the varied ways in which national responses are shaped by geography, historical experience, institutional capacity, and exposure to hostile influence. From NATO's eastern flank to the Western Balkans, these countries occupy strategically sensitive positions where information has become a contested domain of security, diplomacy, and democratic resilience. Together, they show that FIMI is not an abstract threat but a persistent feature of contemporary geopolitical competition, often intertwined with cyber operations, societal polarisation, and broader hybrid tactics. Countermeasures cannot be directly transplanted or employed from one country to another due to differences in context, political landscapes, legal and policy frameworks. This disparity, however, is the reason to study diverse cases as it broadens the understanding of which countermeasures work under what conditions.

8 Oliver Backes and Andrew Swab, *Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States* (Harvard Kennedy School Belfer Center for Science and International Affairs, 2019), https://www.belfercenter.org/sites/default/files/2024-12/Cognitive%20Warfare%20%3D%20The%20Russian%20Threat%20to%20Election%20Integrity%20in%20the%20Baltic%20States.pdf; Press, 'A Primer on Russian Cognitive Warfare', *Institute for the Study of War*, 30 June 2025, https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/.

9 Humprecht et al., 'Resilience to Online Disinformation'.

Difference in terminology

Addressing the challenges of FIMI is further exacerbated by the absence of a unified framework for identifying and responding to such activities. Terminology varies widely not only across countries but also between major organisations such as NATO and the EU, and even among different agencies within individual governments.

For instance, similarly to the EU, NATO has adopted the term Information Manipulation and Interference by Foreign Actors (IMIF), referring to coordinated and manipulative actions by foreign state or non-state actors that threaten the political processes, procedures, and values of target states.[10] This is largely subsumed by what NATO refers to as information threats, which also capture broader phenomena such as disinformation campaigns and hostile information operations.[11] In practice, FIMI and IMIF are closely related in their core purpose: detecting, characterising, and countering intentional information interference by foreign actors. For the purposes of this study and for coherence, the term FIMI will be used throughout the report.

As new technologies enable novel forms of manipulation, and as countermeasures proliferate in response, defining the nature, mechanisms, and boundaries of FIMI has become increasingly difficult. Information manipulation is not new, but digital communication tools have expanded its reach and complexity, prompting the emergence of new terms for long-standing practices and thereby fragmenting the conceptual landscape.

Although overarching frameworks, such as the EU's Digital Services Act, are intended to establish common definitions, national-level interpretations often diverge. This produces gaps between agreed terminology and operational understanding. Moreover, shared definitions frequently remain confined to expert communities, creating barriers to coherent planning, training, and capability development. These discrepancies also hinder international cooperation. The lack of a common lexicon becomes particularly evident when examining differing national approaches, each shaping the design of countermeasures and influencing how effectiveness is assessed.[12]

10 'NATO's Approach to Counter Information Threats', NATO, 2 March 2025, https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats.

11 NATO, 'NATO's Approach to Counter Information Threats: Public Summary'.

12 Laura Jasper, *Balancing Act: Ethical and Legal Dilemmas of Behavioural Influencing in Military Operations*, with Nathan Lokhorst and Michel Rademaker (HCSS, 2023), https://hcss.nl/report/balancing-act-ethical-legal-dilemmas-behavioural-influencing-in-military-operations/.

2.1. The Baltic and Nordic states: High awareness and robust responses

The Baltic-Nordic region offers a unique and instructive lens through which to examine contemporary FIMI countermeasures. Estonia, Lithuania, and Finland each occupy strategically exposed positions in proximity to Russia and face recurring geopolitical pressures. Combined with evolving ties to NATO and the EU, this renders them persistent targets of hostile influence campaigns seeking to exploit historical grievances, linguistic and societal fault lines, and broader European security tensions.

The three countries illustrate distinct pathways in responding to FIMI operations, shaped by their institutional maturity, societal resilience, and perceptions of national vulnerability.

Despite these shared pressures, the three countries illustrate distinct pathways in responding to FIMI operations, shaped by their institutional maturity, societal resilience, and perceptions of national vulnerability. From long-standing information defence traditions to rapidly evolving legal, technical, and civic innovations, each case shows how they mobilise a mix of governmental, societal, and international tools to strengthen the security of their information landscapes.

2.1.1. Estonia

Historical context and contemporary geopolitics

As a small country situated on NATO's eastern flank, Estonia has faced sustained disinformation and interference operations since regaining independence. Its vulnerability is shaped by a legacy of Soviet occupation and the presence of a sizeable Russian-speaking minority, which constitutes roughly one quarter of Estonia's population.[13] One of the most serious early incidents occurred in 2007, when the relocation of the Bronze Soldier statue (depicting a Red Army soldier) to a military cemetery outside Tallinn sparked intense riots, largely attended by Russian-speaking residents.[14] These unrests were fuelled by a disinformation campaign falsely claiming that the monument was to be destroyed. The riots were subsequently accompanied by large-scale cyberattacks targeting Estonian institutions and businesses, marking one of the first major cases of cyber-enabled hybrid pressure in Europe.[15]

Targets and tactics

The primary focus of Russian-affiliated disinformation operations is the exploitation of Estonia's domestic vulnerabilities and leveraging Russia's geopolitical influence vis-à-vis the small Baltic state. One recurring narrative portrays life in Estonia as having been prosperous under Soviet rule. For instance, following the nomination of former Prime Minister Kaja Kallas as the EU High Representative for Foreign Affairs in June 2024, she became the target of a Russian disinformation campaign. A photograph circulated widely online showing Kallas

13 Josephine Koch, 'Russian Minorities in Estonia and Latvia: Combating Discrimination', The Borgen Project, 26 August 2024, https://borgenproject.org/russian-minorities-in-estonia-and-latvia/.; Dmitri Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia* (National Centre of Defence & Security Awareness, 2024), 7, https://kaitsen.ee/wp-content/uploads/2024/10/NCDSA-Resilience-to-FIMI-Research-Report-Estonia-Dmitri-Teperik.pdf.

14 Ivo Juurvee and Mariita Mattiisen, *The Bronze Soldier Crisis of 2007* (Tallinn, Estonia, 2020).

15 Damien McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC News* (Tallinn), 27 April 2017. ; https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf (p. 53)

sitting comfortably with her family as a teenager, implying that Soviet-era repression could not have been that severe despite her public testimony about her family's deportation to Siberia.[16]

Other prominent narratives depict Estonia's NATO membership as a threat to national security, warning that the country risks being drawn into conflict with Russia. Such messaging has been directed particularly at communities near NATO training grounds.[17] Additional campaigns claim that Estonia is merely dependent on foreign policy directives from the United States or the European Union, or that its economy is fragile and suffering from poor governance.[18]

Russia remains the primary perpetrator of disinformation campaigns and foreign interference targeting Estonia, although China has more recently expanded its reach as well. In contrast to Russian tactics, Chinese operations tend not to rely primarily on social media or traditional broadcasting. Instead, they often take more indirect forms, such as encouraging self-censorship in academic and infrastructural cooperation. For instance, a report critical of collaboration between Huawei and the University of Tartu was reportedly banned by the university, highlighting the subtler nature of Chinese tactics.[19]

Countermeasures and Impact

To address FIMI operations, Estonia deploys a mix of top-down institutional coordination and bottom-up societal engagement, reflecting a strong whole-of-society approach involving various stakeholders.

At the strategic level, Estonia's National Defence Development Plan dedicates an entire chapter to the importance of strategic communication as a tool of information defence and prevention against hostile influence.[20] This framing underlines the extent to which Estonia perceives FIMI as a core national security issue, alongside conventional military threats. The plan emphasises the development of situational awareness tools within the information space and stresses the importance of lifelong learning opportunities to strengthen information literacy. Particular attention is given to the potential vulnerability of non-ethnolinguistic Estonians, with an emphasis on engagement and the dissemination of accurate information within these communities.[21]

Institutionally, multiple ministries contribute to counter-FIMI efforts, including the Ministries of Foreign Affairs, Defence, Education, and Communications. To guide this constellation of actors, the Government Office of Estonia serves as the primary coordinating body.

---

16 'Kaja Kallas: Siberis läbielatu andis mu vanavanematele võime pisiasjade pärast mitte ülearu tuju kaotada', Delfi, accessed 28 November 2025, https://www.delfi.ee/artikkel/68306993/kaja-kallas-siberis-labielatu-andis-mu-vanavanematele-voime-pisiasjade-parast-mitte-ulearu-tuju-kaotada.; Marta Vunš, 'Puust ja Punaseks | Just nii käivitas Kreml Kaja Kallase vastu massiivse valeinfokampaania', Eesti Päevaleht, accessed 28 November 2025, https://epl.delfi.ee/artikkel/120305241/puust-ja-punaseks-just-nii-kaivitas-kreml-kaja-kallase-vastu-massiivse-valeinfokampaania.

17 Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia*, 8.; Kaili Malts, 'The Disinformation Landscape in Estonia', EU DisinfoLab, 1 October 2025, 4, https://www.disinfo.eu/publications/disinformation-landscape-in-estonia/.;Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia*, 7.

18 Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia*, 7.

19 Frank Jüris Teperik Dmitri, 'Chinese Influence in Estonia', CEPA, 9 August 2022, https://cepa.org/comprehensive-reports/chinese-influence-in-estonia/.

20 'Strategic Communication | Riigikantselei', accessed 3 December 2025, https://riigikantselei.ee/en/strategic-communication.

21 Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia*, 10.

To facilitate cross-sector cooperation, each ministry has at least one trained specialist responsible for FIMI-related tasks, and these officials meet weekly to coordinate their efforts.[22]

Estonia also integrates non-governmental actors into its information defence. The Estonian Defence League, for example, includes a voluntary cyber unit that brings together cyber-security professionals, experts working within critical infrastructure, and citizens seeking to contribute to national cyber resilience.[23] This model is widely regarded as an innovative approach to volunteer-based cyber defence.[24] The Defence League also initiated the non-profit organisation Propastop, staffed by volunteers who actively monitor the Russian information space in real time for narratives targeting Estonia.[25]

Beyond these longstanding initiatives, Estonia has adopted more direct regulatory measures as well. The Consumer Protection and Technical Regulatory Authority (TTJA), for instance, has ordered the suspension of several Russian and Belarusian broadcasting channels and news websites on the grounds that they supported Russia's invasion of Ukraine, risked inciting violence against Ukrainians, and posed a threat to national security.[26] Estonia's parliament further amended the Information Society Services Act to allow TTJA to block foreign-based information services publishing content that incites hatred or justifies war crimes – measures explicitly linked to limiting hostile information interference.[27]

Estonia also integrates non-governmental actors into its information defence.

In parallel, Estonia has sought to strengthen its domestic information ecosystem by improving access to credible journalism for Russian-speaking communities. A special grant of approximately €2.8 million was made available for private and public media outlets to hire native Russian journalists, thereby expanding the availability and credibility of non-Kremlin controlled Russian-language news within Estonia.[28] Although Estonia has no legislation explicitly targeting disinformation, its National Security Concept identifies disinformation campaigns and foreign interference as threats to social cohesion and constitutional order.[29] The document emphasises strategic communication and psychological resilience as essential defensive tools, providing the foundation for subsequent strategic documents, including the National Defence Development Plan and the Cybersecurity Strategy.[30]

Apart from these sectoral approaches, one of Estonia's most widely recognised strengths in resisting FIMI lies in its high levels of media literacy. In 2026, Estonia ranked sixth among 41 European countries in media literacy indicators.[31] This is partly due to educational emphasis:

22 Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia*, 12–13.

23 Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia*, 13–14.

24 Andris Spruds et al., *Societal Security in the Baltic Sea Region: Expertise Mapping and Raising Policy Relevance* (Latvian Institute of International Affairs, 2018), 104–5, https://liia.lv/en/publications/societal-security-in-the-baltic-sea-region-expertise-mapping-and-raising-policy-relevance-716.

25 'What Is Propastop? – Propastop', accessed 28 November 2025, https://www.propastop.org/en/2017/03/06/what-is-propastop/.

26 ERR | ERR, 'Estonian Tech Regulator to Restrict Access to Seven Russian Websites', ERR, 16 March 2022, https://news.err.ee/1608533494/estonian-tech-regulator-to-restrict-access-to-seven-russian-websites.

27 'Estonia: Freedom on the Net 2024 Country Report', Freedom House, accessed 3 December 2025, https://freedomhouse.org/country/estonia/freedom-net/2024; Karin Kangro, 'Riigikogu võttis vastu 12 seadust', Riigikogu, 19 July 2022, https://www.riigikogu.ee/istungi-ulevaated/riigikogu-vottis-vastu-12-seadust/.

28 Kenneth R. Rosen, 'Estonia's Answer to Russian Disinformation Is to Fund Real Journalism', *Coda Story*, 20 February 2023, https://www.codastory.com/newsletters/estonia-public-media-russian-disinformation/.

29 Malts, 'The Disinformation Landscape in Estonia'.

30 Teperik, *Code of Resilience: Building a Functional Ecosystem for Countering FIMI in Estonia*, 10.

31 https://osis.bg/wp-content/uploads/2026/01/Media-Literacy-Index-2026.pdf (p. 7)

high school students must complete a mandatory 35-hour "media and influence" course.[32] Estonia's resilience is further reinforced by strong media autonomy and comparatively high interpersonal trust among citizens.[33]

Taken together, these structural factors (high media literacy, institutional coordination and an embedded culture of shared responsibility) have successfully contributed to limiting the tangible impact of FIMI operations in Estonia to date.

2.1.2. Lithuania

Historical context and contemporary geopolitics

Lithuania is a front-line NATO and EU member state bordering the Russian exclave of Kaliningrad and allied Belarus. Once ruled by Moscow during the Soviet era, it is now firmly Western-aligned and hosts a NATO battlegroup as part of NATO's Enhanced Forward Presence initiative to deter Russian aggression. This strategic position, combined with historic grievances such as Soviet occupation and anti-Soviet resistance, makes Lithuania a prime target for Moscow's information warfare.

Targets and tactics

The overwhelming majority of FIMI in Lithuania originates from Russia and its proxies.[34] Lithuania's intelligence agencies have repeatedly warned that Russian intelligence and propaganda organs seek to sway public opinion and political processes via information and cyber means. In recent years, Belarus has also acted in concert with the Kremlin's efforts (especially during the 2021 migrant crisis), but Russia remains the central orchestrator of hostile influence campaigns.[35]

Russian information operations against Lithuania are intense and multifaceted, blending disinformation, propaganda, and cyber tactics.[36] A large, coordinated propaganda ecosystem – encompassing state-run media outlets such as RT and Sputnik, social networks like Telegram, and local pro-Kremlin websites disseminated false narratives designed to tarnish Lithuania's international image, justify Kremlin regional ambitions, and undermine Lithuania's political legitimacy and independence. Russian narratives can be subsumed to fall broadly around four core themes: 1) Lithuania's national self-identity and historic trajectory, 2) its membership in western political alliances, 3) the efficacy and integrity of government, and 4) domestic societal issues and contestations.[37] For example, the Kremlin insists the Baltic states "willingly

32 https://www.thenorthernvoices.com/post/How-Estonia-is-Leading-the-Fight-Against-Disinformation-with-Innovative-Media-Literacy-Programs; Amy Yee, 'The Country Inoculating against Disinformation', 31 January 2022, https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation.

33 https://bti-project.org/en/reports/country-report/EST

34 https://www.disinfo.eu/wp-content/uploads/2023/06/20230521_LT_DisinfoFS.pdf (p. 3)

35 Elegijus PAULAVIČIUS and Darius JAUNIŠKIS, *National Threat Assessment 2022* (State Security Department of the Republic of Lithuania (VSD), 2022), 74, https://www.vsd.lt/wp-content/uploads/2022/04/ANGL-el-_.pdf.

36 Minna Ålander, 'Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression', Carnegie Endowment for International Peace, accessed 14 November 2025, https://carnegieendowment.org/research/2024/11/russia-gray-zone-aggression-baltic-nordic?lang=en.

37 Backes and Swab, *Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States*, 14.

joined" the USSR and paints today's Lithuania as a Nazi sympathising state that discriminates against Russians.[38]

During the COVID-19 pandemic, Russian outlets pushed claims that the virus was a Western bioweapon brought to Lithuania by NATO troops, while simultaneously amplifying anti-vaccine and anti-lockdown messages.[39] 2021 saw contentious anti-lockdown protests in Lithuania, some of which turned violent. Lithuania's State Security Department warned that *"pro-Kremlin actors and Covid conspiracy theorists"* were trying to radicalise these gatherings.[40] Later in the year, as Belarus (backed by Russia) sent waves of migrants to Lithuania's border, a barrage of disinformation accompanied the hybrid assault – such as fake reports of border guards injuring migrants.[41] Other recurring falsehoods depict Lithuania as a "failed state" in economic terms and claim that Lithuanian policies such as decoupling from the Russian energy grid would impoverish Lithuanians.[42]

Russia's 2022 invasion of Ukraine marked an inflection point, with waves of inauthentic comments on LRT's social media following Lithuania's implementation of an EU sanctions package against Russia in June 2022.[43] Moreover, Russian sources falsely accused Lithuania of establishing a blockade of Kaliningrad.[44] Despite the repeated Russian-backed attacks, the Lithuanian information space has remained remarkedly resilient. Since the start of the invasion in 2022, public support for Ukraine has remained overwhelming, suggesting that the Kremlin's influence efforts failed to shift the broader narrative.[45]

Countermeasures and impact

Mirroring approaches from other Baltic nations or Ukraine, Lithuania has adopted a *"whole-of-government"* approach which mobilises several agencies in a coordinated effort to counter FIMI.[46] The lead agency for identifying and assessing information threats is the State Security Department (VSD), which provides annual threat assessments and public warnings.[47] The Ministry of National Defence and its Strategic Communications divisions also play a key role: the armed forces monitor information incidents, issuing prompt debunking of fake news about the military. Lithuania's Cybersecurity and Telecommunications regulators

38 'Russia Seeks to Discredit Lithuania, Increasingly Accusing It of Rewriting History, Promoting Nazism, and Spreading Russophobia', *Lietuvos Respublikos Valstybės Saugumo Departamentas*, n.d., accessed 20 November 2025, https://www.vsd.lt/en/reports/influence-activities-against-lithuania/russia-seeks-to-discredit-lithuania-increasingly-accusing-it-of-rewriting-history-promoting-nazism-and-spreading-russophobia/.

39 Richard Weitz and Aurimas Lukas Pieciukaitis, *Moscow's Disinformation Offensive During COVID-19: The Case of Lithuania*, 2 ; Geir Hågen Karlsen, 'Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe', *Palgrave Communications* 5, no. 1 (2019): 10, https://doi.org/10.1057/s41599-019-0227-8.; Laura Kayali and Mark Scott, 'Anti-Vax Conspiracy Groups Lean into pro-Kremlin Propaganda in Ukraine – POLITICO', 17 March 2022, https://www.politico.eu/article/antivax-conspiracy-lean-pro-kremlin-propaganda-ukraine/.

40 *Lithuania Monthly: Kremlin Narratives Exploit Protests to Undermine Democracy - CRI*, Uncategorized, 3 December 2024, https://balticdisinfo.eu/lithuania-monthly-kremlin-narratives-exploit-lithuanian-protests-to-undermine-democracy/.

41 Brock Mays, *Disinformation Landscape in Lithuania* (EU DisinfoLab, 2023), 5, https://www.researchgate.net/profile/Cahit-Erdem/publication/324783924_The_relationship_between_media_literacy_and_critical_thinking_a_theoretical_and_emprical_review/links/5b9bda7f45851574f7cb3199/The-relationship-between-media-literacy-and-critical-thinking-a-theoretical-and-emprical-review.pdf.

42 LRT.lt,BNS, 'Russian Propaganda Targets Baltics' Energy Policies – Study', Lrt.Lt, 6 June 2024, https://www.lrt.lt/en/news-in-english/19/2290799/russian-propaganda-targets-baltics-energy-policies-study.

43 https://www.debunk.org/posts-related-to-kaliningrad-sanctions-targeted-by-social-media-bots-and-trolls

44 https://www.bbc.co.uk/news/world-europe-61901764

45 https://www.kyivpost.com/interviews/70225

46 Kinga Dudzińska, 'PISM', The Lithuanian Model in the Fight against Disinformation, 23 May 2019, https://pism.pl/publications/The_Lithuanian_Model_in_the_Fight_against_Disinformation?utm_

47 Elegijus PAULAVIČIUS and Darius JAUNIŠKIS, *National Threat Assessment 2022*.

complement these efforts by addressing the technical and media dimensions – notably the Radio and Television Commission of Lithuania (LRTK), which oversees broadcast and online content.[48]

During crises, the LRTK has exercised special powers under emergency law to shut down channels or sites disseminating dangerous disinformation.[49] Thus, in the days following Russia's full-scale invasion, the LRTK could suspend or penalise any outlet disseminating war propaganda, disinformation, or calls to undermine Lithuanian sovereignty. Under this mandate, numerous Kremlin-linked websites and TV rebroadcasts were blocked. The parliament also amended laws to criminalise explicit forms of information aggression. Notably, in 2023 lawmakers advanced a bill targeting automated online disinformation tools distributing false information such as SIM bots or SIM swarms.[50]

Lithuania has emphasised societal resilience as the first line of defence against FIMI.

In 2023, the National Crisis Management Centre (NKVC) was created, approved by the government as a 24/7 operational hub for crisis response. The NKVC's mandate spans national security threats, including Russia's disinformation ecosystem, which has been recognised as a primary national security concern.[51] Additionally, Lithuania aligns with the EU codes of practice that encourage social media platforms to self-regulate misinformation and hate speech.[52] Overall, normative and cooperative approaches – from guidelines for journalists to information sharing networks - underpin Lithuania's non-coercive tools. Apart from these efforts, Lithuania has emphasised societal resilience as the first line of defence against FIMI. To that end, media literacy education has been expanded in schools and libraries, often in partnership with NGOs and the Ministry of Education, to "inoculate" the public against fake news and enhance citizen's ability to discern disinformation.

Internationally, Lithuania's response is closely coordinated with EU and NATO partners. It actively contributes to EU collective measures by feeding data to the EU's East StratCom Task Force (EUvsDisinfo) and implementing EU-wide decisions, like banning Kremlin-backed media outlets RT and Sputnik in 2022. Regionally, Lithuania works with its Baltic neighbours and Poland to share intelligence on influence operations. It also participates in NATO's Strategic Communications initiatives and training, and Lithuanian experts are seconded to NATO's StratCom Centre of Excellence. Importantly, Lithuania has also started exporting its know-how beyond Europe by sharing knowledge with, for example, Taiwan, which it helped build a comprehensive counter-disinformation system modelled on Lithuania's own successes.[53] This underscores its growing reputation as a leader in this field.

---

48 Chris Dziadul, 'Lithuania Blocks Russian TV IP Addresses', *Broadband TV News*, 14 September 2023, https://www.broadbandtvnews.com/2023/09/14/lithuania-blocks-russian-tv-channel-ip-addresses/.

49 'The Radio and Television Commission of Lithuania Is Coordinating Actions to Suspend the Retransmission of All Russian TV Programmes Related to GazpromMedia in Lithuania. | Radio and Television Commission of Lithuania', 21 April 2025, https://www.rtk.lt/en/news/the-radio-and-television-commission-of-lithuania-is-coordinating-actions-to-suspend-the-retransmission-of-all-russian-tv-programmes-related-to-gazpromme-dia-in-lithuania.

50 BNS, 'Lithuanian Lawmaker Proposes Criminalising Disinformation', Lrt.Lt, 10 November 2025, https://www.lrt.lt/en/news-in-english/19/2741214/lithuanian-lawmaker-proposes-criminalising-disinformation.

51 Nerijus Maliukevičius, *Fortifying Democracies: Lithuania's Comprehensive Approach to Counter Disinformation and Propaganda* (Eastern Europe Studies Centre, n.d.), 3, https://www.gssc.lt/wp-content/uploads/2024/04/v02_Maliukevicius_Fortifying-Democracies_EN_A4-2.pdf.; https://www.disinfo.eu/wp-content/uploads/2023/06/20230521_LT_DisinfoFS.pdf (p. 10)

52 Nerijus Maliukevičius, *Fortifying Democracies: Lithuania's Comprehensive Approach to Counter Disinformation and Propaganda*, 8.

53 Elzė Pinelytė, 'Patience and Perseverance: Lessons from Lithuania's Engagement with Taiwan', Global Taiwan Institute, 19 March 2025, https://globaltaiwan.org/2025/03/patience-and-perseverance-lessons-from-lithuanias-engagement-with-taiwan/.

Aside from coordinated efforts at the national and international level, Lithuania has fostered an environment of cooperation between public and private actors. For example, media literacy education has been expanded in schools and libraries, often in partnership with NGOs and the Ministry of Education.[54] Independent media outlets and NGOs also function as *de facto* partners to the government by monitoring and debunking false narratives in real time, such as the NGO Debunk.org which works closely with journalists and volunteers ("Elves") to flag disinformation and shares its findings with authorities and the public.[55]

2.1.3. Finland

Historical context and contemporary geopolitics

Finland shares a historically sensitive border with Russia, shaped by conflict, cautious cooperation and evolving border management practices since the Second World War. Although Helsinki has kept a relatively stable relationship with Moscow throughout the Cold War and after the dissolution of the Soviet Union, tensions increased after Russia facilitated the movement of third-country nationals towards the Finnish border in 2015.[56]

Russia's full-scale invasion of Ukraine in 2022 fundamentally altered bilateral relations, pushing Finland to abandon its long-standing policy of military non-alignment and join NATO in 2023. As a result, Finnish-Russian relations are now at their lowest point in decades, with contact largely limited to minimal technical border coordination.[57] Against this backdrop, Finland has become an increasingly visible target of Russian FIMI operations, largely focussed on targeting the Finnish central government, foreign and security policy, and its defence industry.[58]

Targets and tactics

Russian FIMI activities targeting Finland encompass a broad range of narratives. These include false claims regarding child custody cases, COVID-19 conspiracy theories, anti-NATO messaging, warnings of economic hardship resulting from support for Ukraine, and the amplification of far-right radicalisation and xenophobic "Great Replacement" ideologies.[59]

One prominent operation affecting Finland is the "Doppelganger" campaign, which replicates the appearance of trusted media outlets through fake news websites in order to disseminate manipulated content.[60] Such campaigns have targeted government institutions, the

54 Government of the Republik of Lithuania, 'Over a hundred grades from schools across Lithuania put their skills to test in first-ever disinformation literacy exam', 5 March 2025, https://lrv.lt/en/news/over-a-hundred-grades-from-schools-across-lithuania-put-their-skills-to-test-in-first-ever-disinformation-literacy-exam/.

55 Brock Mays, *Disinformation Landscape in Lithuania*, 9.

56 https://fiia.fi/wp-content/uploads/2023/11/Comment12_-Russias-hybrid-operation-at-the-Finnish-border.pdf (p.1)

57 René Nyberg, *Securing Borders After a Breach of Confidence: Russian-Finnish Relations* (Carnegie Politika, 2024), https://carnegieendowment.org/russia-eurasia/politika/2024/09/russia-finland-border-security?lang=en.

58 *Supo: Russia Remains Top of Finland's Security Threat Concerns* (YLE, 2025), https://yle.fi/a/74-20147334.

59 'Overview of Information Influence Activities', Finnish Government, January 2025, https://valtioneuvosto.fi/en/government-communications/overview-of-information-influence-activities.; 'What Can Countries Do to Tackle Threats of Disinformation Using Education and Technology? Finland Provides One Answer', *NHK Wold-Japan News* (NHK Wold-Japan News), 21 March 2025, https://www3.nhk.or.jp/nhkworld/en/news/backstories/3891/.

60 *NHK Wold-Japan News*, 'What Can Countries Do to Tackle Threats of Disinformation Using Education and Technology? Finland Provides One Answer'.

general public, and independent fact-checkers. Finnish journalist have also been singled out. Jessika Aro, for instance, faced sustained harassment after exposing Kremlin-linked troll networks.[61] In addition to externally coordinated campaigns, a small but active domestic online network identifying itself as "Truth Seekers" disseminates conspiracy narratives, particularly via social media platform X. These actors promote "deep state" narratives and have spread misinformation regarding Finland's NATO accession, falsely claiming that public opinion was manipulated and election results were falsified. The network also operates alternative media outlets, such as MV-lehti and Z-news, which amplify pro-Kremlin messaging. These platforms are reportedly administered by Finnish nationals residing either in Russia or in Russian-occupied Ukrainian territories.[62]

Russian disinformation has specifically targeted non-Finnish speaking communities in Finland through foreign-language content on social media platforms. Such content, often more difficult for authorities to monitor, appeals to minorities in Finland who may not be proficient in Finnish and primarily rely on social media for information instead of traditional news outlets. Through these channels, narratives have included claims of an imminent war at the Finnish border and accusations that the United States coerced Finland into joining NATO.[63]

Countermeasures and impact

Finland's approach to countering FIMI entails a combination of national coordination, civil society engagement, and international cooperation. Since 2014, the Prime Minister's Office has coordinated a national network to monitor and respond to foreign disinformation.[64] This network includes NGOS, state agencies, independent media watchdogs, and public broadcasters.[65] The Finnish Broadcasting Company YLE, for instance, operates a specialised fact-checking unit equipped with advanced information retrieval tools to verify online narratives, and YLE cooperates closely with other media operators to strengthen collective resilience.[66]

Civil society actors also play an important role. The NGO Faktabaari reinforces Finland's fact-checking capacity and promotes evidence-based public debate. It conducts project-based initiatives to enhance digital information literacy, including raising awareness of algorithmic amplification and AI-generated content.[67]

Institutionally, Finland has established the Knowledge Centre on Information Resilience under the National Emergency Supply Agency (NESA), which traditionally manages the strategic reserves such as fuel and medical supplies. The Centre develops tools to counter harmful influence, builds technical capabilities to detect online disinformation operations,

61 Dominic Saar et al., *Disinformation Landscape in Finland* (EU DisinfoLab, 2025), 11, https://www.disinfo.eu/wp-content/uploads/2025/04/20250402_Disinfo-landscape-in-Finland-V2.pdf.

62 Dominic Saari et al., *The Disinformation Landscape in Finland* (EU Disinfo Lab, 2025), 3–4, https://www.disinfo.eu/publications/disinformation-landscape-in-finland/.

63 'Disinformation Campaigns Target Finland's Foreign Language Speakers, Nato Fears', *News*, 6 July 2022, https://yle.fi/a/3-12525251.

64 *Countering Disinformation: News Media and Legal Resilience*, Hybrid CoE Paper 1 (Hybrid CoE Paper 1, 2019), https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

65 Dominic Saar et al., *Disinformation Landscape in Finland*.

66 Andrea Hogberg, 'Yle perustaa tiedon varmentamiseen erikoistuvan tiimin', text, Yle Viestintä, accessed 26 November 2025, https://yle.fi/aihe/a/20-10007870.

67 Dominic Saari et al., *The Disinformation Landscape in Finland*, 8.

and provides information security training.[68] It is also expected to publish regular reports assessing information campaigns and preparedness measures.

At the supranational level, Finland closely cooperates with EU and NATO partners. A notable example is simulation exercises hosted at Helsinki's European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), where participants replicate coordinated responses to disinformation campaigns by Russia and China. These exercises underscore Finland's emphasis on preparedness and international coordination in addressing hybrid threats.[69]

The concept of "information defence" was formally introduced in Finland's 2021 Government Defence Report. While the report defined the concept, it did not provide a detailed operational strategy. To date, Finland continues to lack specific legislation enabling the criminalisation of disinformation campaigns, partly reflecting the country's strong commitment to protecting the freedom of expression and whistleblower protections.[70] Nevertheless, Finland places strong emphasis on preventive resilience-building. Its internationally recognised media literacy framework integrates critical thinking into education and incorporates AI tools to identify disinformation sources.[71] Since 2014, thousands of professionals and citizens have received training to strengthen resistance to primarily Russian-sourced misinformation. Finland's approach in this regard prioritises institutional trust, coordinated national defence, and cognitive resilience.[72]

Finland places strong emphasis on preventive resilience-building.

Overall, Finland's efforts have significantly limited the effectiveness of hostile influence operations. High levels of trust in media and public institutions contribute to transparency and resilience. However, challenges remain regarding ongoing and evolving disinformation operations, such as the Doppelganger campaign.[73] Research from the University of Helsinki indicates that societal polarisation has increased, albeit remaining moderate by international comparison.[74] Moreover, while Russian disinformation campaigns against Finland are described as aggressive, Finland is not considered a primary target compared to other states.[75] It remains uncertain whether Finland's resilience would hold under sustained, high-intensity information pressure or whether its strong resilience makes it a less attractive target in the first place. Taken together, Finland's model – shaped by historical experience, public trust, and proactive governance – has reduced the impact and spread of disinformation. Nevertheless, Finnish officials underline that information warfare is an ongoing challenge which is growing in complexity and therefore necessitates sustained vigilance and adaptation.[76]

68 'The National Emergency Supply Agency Will Continue to Produce Information on Harmful Information Campaigns - Huoltovarmuuskeskus', accessed 26 November 2025, https://www.huoltovarmuuskeskus.fi/en/a/the-national-emergency-supply-agency-will-continue-to-produce-information-on-harmful-information-campaigns.

69 Anne-Françoise Hivert, *Finland Launches Experiment on Countering Disinformation Attacks*, 5 June 2022, https://www.lemonde.fr/en/international/article/2022/06/05/in-finland-democracies-have-been-organizing-their-response-to-hybrid-threats_5985716_4.html.

70 Dominic Saari et al., *The Disinformation Landscape in Finland*, 9.

71 *NHK Wold-Japan News*, 'What Can Countries Do to Tackle Threats of Disinformation Using Education and Technology? Finland Provides One Answer'.

72 Eliza Mackintosh, *Finland Is Winning the War on Fake News. Other Nations Want the Blueprint*, (Helsinki), n.d., https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.; Dominic Saar et al., *Disinformation Landscape in Finland*.

73 *NHK Wold-Japan News*, 'What Can Countries Do to Tackle Threats of Disinformation Using Education and Technology? Finland Provides One Answer'.

74 Dominic Saar et al., *Disinformation Landscape in Finland*, 2.

75 'Finland Not a Primary Target of Russian Disinformation Influence, Says Government Report', YLE News, 22 January 2025, https://yle.fi/a/74-20138645.

76 Eliza Mackintosh, *Finland Is Winning the War on Fake News. Other Nations Want the Blueprint*.

2.1.4. **Reflections**

Across Estonia, Lithuania, and Finland, historical experience with Russian influence and contemporary geopolitical pressures have driven the countries to treat FIMI as a core national security concern. Moreover, their approaches converge on a whole-of-society model: coordinated government institutions, active civil society participation, empowered independent media, and sustained investments in media literacy form mutually reinforcing layers of resilience.

Rapid-response mechanisms and cross-sector coordination have proven essential in limiting the impact of real-time disinformation incidents, while forward-looking strategies (including education, technical monitoring capabilities, and societal cohesion) help prevent hostile narratives from gaining traction. Each country's experience illustrates both gains and limits, while maintaining trust, engaging vulnerable communities, avoiding overreach, and keeping pace with evolving tactics remain ongoing challenges.

Together, these case studies show that enduring resilience requires not only technical and institutional capacity, but also a culturally embedded commitment to openness, critical thinking, and shared responsibility for protecting the information space.

These case studies show that enduring resilience requires not only technical and institutional capacity, but also a culturally embedded commitment.

2.2. Ukraine and its border region: Heightened urgency and maturing responses

The countries along Ukraine's borders – Poland, Moldova, and Romania – form a critical buffer zone where the impacts of Russia's war against Ukraine extend far beyond the battlefield. This region sits at the intersection of historical fault lines, contemporary geopolitical realignments, and a rapidly evolving information ecosystem. As a result, it has become a crucial theatre for FIMI activity. Understanding this landscape requires attention not only to the diverse contexts of these cases but also to the ways in which the conflict in Ukraine reshapes their vulnerabilities and responses.

Across these neighbouring countries, Russia's aggression has amplified existing pressures on institutions, media environments, and the public, while also provoking new forms of societal resilience and strategic adaptation. Together, these cases highlight why Ukraine's borderlands represent a testing ground for how states confront, absorb, and counter external information threats in an era characterised by hybrid conflict.

2.2.1. **Ukraine by Sofia Romansky**

A comprehensive account of the conflict dynamics surrounding Russia's invasion of Ukraine requires attention for both the kinetic and digital battlefields.[77] Arguably, over the past four years, many of the most consequential confrontations between Ukraine and Russia have taken place not only on the front lines, but within the information space, targeting the hearts and minds of domestic and international audiences. As such, Ukraine constitutes a particularly pressing case study for examining the complexities of Russian FIMI. First, Ukraine is the only case in contemporary Europe where Russian FIMI unfolds in an overt wartime context, rather than in the ambiguous, hybrid settings more commonly associated with influence operations. This has forced both Ukraine and Russia to adapt their approaches to informational offense and defence, creating novel interactions and integrations between digital and conventional domains of warfare. Second, Ukraine's experience of Russian information-based influence is uniquely shaped by longstanding historical, cultural, and linguistic ties. This context is inseparable from an analysis of where Russian FIMI succeeds and fails when it comes to Ukraine. Finally, while Ukrainian citizens, both civilian and combatant, remain a primary target of dedicated information campaigns, Russia's FIMI in Ukraine affects its broader strategic and diplomatic aims and communication. Subsequently, European observers of Russia's invasion also become indirect targets. This way, the effects of Russian FIMI in Ukraine spill over across the region and into the global information environment, amplified by the geopolitical significance of the war and the international attention it continues to attract.

The effects of Russian FIMI in Ukraine spill over across the region and into the global information environment.

Historical Context and Contemporary Geopolitics

Ukraine and Russia share deep, complex, and often asymmetrical historical, cultural, and linguistic ties that have contributed to the creation and exploitation of long-standing structural vulnerabilities in Ukraine's information environment.[2] Ukraine's historical positioning is marked by being on the periphery of empires, most notably the Russian Empire and, later, the Soviet Union.[78] Throughout these eras, Ukraine was viewed in Russian political thought not as a distinct entity, but as an integral part of so-called 'greater Russia'. This perception led to a continuous suppression of Ukrainian national identity, culture, and language in favour of Slavic unity under Moscow.[4] Following the collapse of the USSR, Ukraine aspired for democratic self-determination and integration with Western institutions. Since the turn of the century, Ukrainians have affirmed these goals through pro-European Union and anti-Russian demonstrations, perhaps most notably through the 2004 Orange Revolution and 2013-2014 Euromaidan protests. In this context, historical propaganda and revisionism form the bedrock of Russia's political engagement with Ukraine, reinforcing narratives of fraternal unity while simultaneously undermining Ukrainian sovereignty and Western alignment.

While Russia's use of information operations as a concrete tool of influence in Ukraine long predates the 2014 annexation of Crimea and the 2022 full-scale invasion, the scale of these tactics has intensified with these most recent crises. With each escalation, Russia expanded and adapted its techniques and tactics. These shifts have been shaped not only by technological change, witnessed in the rise of social media and generative artificial intelligence (AI), but also by geopolitical developments, most significantly, Ukraine's progressive alignment

77 Irene Etzersdorfer, 'Jeffrey Mankoff: Russia's War in Ukraine. Identity, History and Conflict. Washington, D.C.: Center for Strategic and International Studies (CSIS), April 2022,' *SIRIUS – Zeitschrift Für Strategische Analysen* 6, no. 4 (2022): 439–40, https://doi.org/10.1515/sirius-2022-4008.

78 Mark Bassin et al., *Between Europe and Asia: The Origins, Theories, and Legacies of Russian Eurasianism*, vol. 233 (University of Pittsburgh Press, 2015).

with the European Union and NATO.[79] These moves are viewed by Moscow as a direct threat to its regional influence.[80] From the Association Agreement crisis in 2013, to Ukraine's formal recognition as an EU candidate in June 2022, and the launch of accession talks in June 2024, Ukraine's Euro-Atlantic trajectory has triggered a concerted Russian effort to delegitimise and destabilise this path. Russian responses have been ideologically underpinned and discursively justified by a resurgence of narratives associated with the "one people" trope and the "Russkiy mir" (Russian world), which frames Ukraine as part of a shared civilisational space rooted in Orthodox Christianity, the Russian language, and a shared historical trajectory. [81] In the 2022 invasion, this manifested in the use of emotionally charged and historically resonant, if not at times mutually contradictory, frames: Ukraine as a genocidal threat to ethnic Russians and Russian speakers; Ukraine as a helpless puppet of NATO in the context of post-Cold War NATO expansion and the broken assurances perceived by Russia; and Ukraine as a neo-Nazi state, invoking the memory of the Great Patriotic War and framing the invasion as a continuation of Russia's WWII legacy of fighting fascism. [82] These narratives share an underlying goal of attempting to render Russian actions morally unassailable and politically legitimate. [83]

While these narratives are not uniformly persuasive, some are familiar to Ukrainians, particularly in regions with closer historical or linguistic ties to Russia. In this way, Russia's information strategies are rooted in long-standing ideological constructs and tailored to the unique societal dynamics of Ukraine.

Targets and Tactics

While not the primary focus of this case study, it is essential to recognise how Russia's information manipulation tactics since the 2014 laid the groundwork for many of the actions observed during and following the 2022 full-scale invasion of Ukraine. [84] Specifically, disinformation campaigns which denied Russian involvement in the annexation of Crimea, instead presented as a spontaneous local movement, and the prevalence of pro-Russian narratives in the Luhansk and Donetsk oblasts of Ukraine (collectively known as the Donbas region), can be seen as key precursors. Starting from 2014, Russia gained notoriety for its use of social media bots to amplify the visibility and reach of pro-Russian content and conduct false flag operations, capitalising off of digitally mediated informational ambiguity. Simultaneously, Russian state-backed media outlets continued to play a central role in reinforcing an anti-Ukrainian narrative, consistently questioning and undermining Ukraine's claim to sovereignty. Overall, this contributed to an increasingly more muddied information ecosystem, sowing seeds of political polarisation both within and beyond Ukraine.

What has remained consistent throughout more than a decade of conflict are the three broad categories of targets of Russian information's operations: 1. Ukrainian civilians, 2. Ukrainian combatants, and 3. groups outside of Ukraine. Civilians in Ukraine are exposed to delegitimising political narratives which target existing grievances and undermine trust

79 John Biersack and Shannon O'lear, 'The Geopolitics of Russia's Annexation of Crimea: Narratives, Identity, Silences, and Energy', *Eurasian Geography and Economics* 55, no. 3 (2014): 247–69.

80 Etzersdorfer, 'Jeffrey Mankoff'.

81 Alexander Brotman, 'Ukraine and the Shifting Geopolitics of the Heartland', *Geopolitical Monitor*, 21 September 2022, https://www.geopoliticalmonitor.com/ukraine-and-the-shifting-geopolitics-of-the-heartland/.

82 Ecaterina Locoman and Richard R Lau, 'Narratives of Conflict: Russian Media's Evolving Treatment of Ukraine (2013–2022)', *Media, War & Conflict* 18, no. 3 (2025): 325–47.

83 Locoman and Lau, 'Narratives of Conflict: Russian Media's Evolving Treatment of Ukraine (2013–2022)'.

84 Keir Giles, *Russian Cyber and Information Warfare in Practice | Chatham House – International Affairs Think Tank* (Chatham House, 2023), 65, https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice.

in the Ukrainian government and its allies. Claims accusing Ukrainian politicians of nationalist and fascistic corruption, as well as reference to the oppression or even genocide of Russian-speaking or ethnically Russian Ukrainian citizens serves to amplify doubts within the population, undermine cohesion, and reduce resistance to Russian influence. Meanwhile, combatants face tactical-level disinformation designed to create confusion and sabotage operational effectiveness. Notably, during the early stages of the 2022 invasion, Russian disinformation targeted the Ukrainian military with misinformation about troop movements and manipulated intelligence to disrupt Ukrainian responses. Finally, groups outside of Ukraine are also targeted to a lesser and often indirect extent, with Russian FIMI having ripple effects on both diasporic communities and foreign political landscapes. Ukrainian diasporas, particularly those consisting of refugee communities in Europe, experience a blend of information warfare aimed at furthering Russian political goals, seeing both narratives that mirror those in Ukraine as well as those targeting Ukraine's allies. Importantly, these diaspora communities also serve as resilience points, helping to expand Ukraine's information network and counter Russian narratives. In this way, Russia's information operations not only undermine morale inside Ukraine but also target European cohesion and the continent's support for Ukraine.

In the concrete context of the 2022 full-scale invasion of Ukraine, it is important to note how Russia's information strategies evolved as the war progressed. Initially, information operations were heavily concentrated in targeted campaigns, where Russian and Ukrainian narratives, as well as counter narratives, clashed directly. Early in the war, Russian disinformation focused on shaping first potent impressions of the invasion while simultaneously discrediting Ukrainian leadership. Within the first days a deepfake video emerged online depicting President Volodymyr Zelenskyy purportedly ordering Ukrainian troops to surrender.[85] The Ukrainian Centre for Strategic Communication had warned of such videos earlier and acted quickly to publicly discredit and remove clips on major platforms. Albeit the information impact of the video was likely limited, with its crude appearance, it still served as a disruption. Notably, Russian hackers had concurrently targeted the TV Channel Ukraine 24, posting a still from the deepfake video alongside a fictitious summary.[86] This move had two functions: on the one hand it prevented the flow of information to Ukrainian audience from the key centralised news channel, and on the other hand, it aimed to capitalise on the legitimacy of this source in order to peddle false information.[87] More memorable, however, were Zelenskyy's responses to disinformation. When days into the invasion rumours started to spread that Zelenskyy and key official had fled the country, the president shared a handheld video from Kyiv with the message "we are all here".[88] As (at the time) Prime Minister Denys Shmyhal holds up his iPhone to show the time and date, this video stands as an example of the stark contrast between simple and credible messaging and blunt, synthetic media.[89]

Another key example that brought together many of the core Russian narratives involved the way that the battle for the Azovstal steel plant in Mariupol became a focal point in 2022. Russian outlets portrayed the Azov Regiment as 'neo-Nazis' and terrorists responsible for

85 Justin Hendrix, 'Purported Deepfake of Ukrainian President Zelensky Aired on Television Station Website | TechPolicy.Press', Tech Policy Press, 16 March 2022, https://techpolicy.press/purported-deepfake-of-ukrainian-president-zelensky-aired-on-television-state-website.

86 Tom Simonite, 'A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be', Tags, *Wired*, n.d., accessed 3 December 2025, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.

87 'Ukraina 24 TV's Ticker Tape Hacked, Streaming Fakes about Zelenskyy's "Capitulation"', IMI, 16 March 2022, https://imi.org.ua/en/russias-crimes/ukraina-24-tvs-ticker-tape-hacked-streaming-fakes-about-zelenskyys-capitulation.

88 Emma Ockerman, 'Ukrainian President Just Dropped a Defiant Video From the Streets of Kyiv', VICE, 25 February 2022, https://www.vice.com/en/article/ukrainian-president-zelenskyy-video-kyiv-we-are-here/.

89 *Ukrainian President Volodymyr Zelensky: 'We Are Still Here'*, n.d., 00:32, accessed 3 December 2025, https://www.youtube.com/watch?v=wgCNKhtZYks.

crimes in the Donbas region, alluding back to the pretext used to justify the invasion and the liberation of Mariupol.[90] Ukraine countered the narrative by framing the defenders of Azovstal as emblematic of national resistance, resilience, and heroism, 'strong as steel' like the rest of the Ukrainian people. Ukrainian authorities also actively debunked the neo-Nazi narrative, with even the Azov regiment itself making public statements. [91] Yet, the information still spread worldwide, broadly accompanied by rising concerns about nationalist movements in Ukraine. Ultimately, when Azovstal and Mariupol were captured, Russia used it the victory to reinforce internal support and vigour for its campaign.

Similar information tactics were also used in cohort with physical force to shape the outcomes of battles by disrupting Ukrainian command structures and sowing confusion among both military personnel and the public. Most of the Russian tactics involved false reporting on frontline achievements and movements by manipulating the sequence of events and data. Perhaps one of the most notorious cases of narrative clash to emerge from the first months of the war was around the sinking of the Moskva. In April 2022 Ukrainian officials reported that the flagship of the Black Sea fleet was hit by two Ukrainian-made Neptune anti-ship missiles near Odessa. [92] Immediately, a Russian counter-narrative emerged claiming that the ship sank due to a fire and, subsequently, poor weather conditions, focusing on debunking Ukrainian claims as any attribution to Ukrainian success would jeopardise the perceived strength of Russia air deterrence.[93] Meanwhile, Ukraine capitalised on the symbolic significance of defeat given the ship's namesake and operational importance.[94] In turn, this narrative battle directly affected the tactical manoeuvring of the Black Sea Fleet: all ships moved away from the shore, amphibious attacks on Odessa's became less probable with the loss of a key node in the navy's command and control structure, and forced a re-evaluation of delivery patterns for other ships.[95] As such, the ambiguity of Russian communication in an attempt to save face likely played directly into the hands of Ukraine.

As the conflict extended, Russian information efforts became more diffuse and less reliant on "grand narratives". The early high-impact narratives like 'genocide' and 'denazification' as well as information around 'impressive' moments gave way to subtler tactics, as Ukrainian resistance to Russian disinformation grew and the priority shifted from shaping impressions of the invasion to maintaining informational dominance and keeping up appearances in a protracted conflict.[96] In August 2025, news started to spread that Russian hacker groups Killnet, Palach Pro, User Sec, and Beregini had successfully accessed and leaked data from the Ukrainian

---

90 Todd Prince, 'Russia's Capture Of Azovstal: Symbolic Success, "Pyrrhic" Victory?', Russia, *Radio Free Europe/Radio Liberty*, 15:18:50Z, https://www.rferl.org/a/azovstal-russia-ukraine-captured/31856565.html.

91 Veronika Lutska, 'Azov Contra Fake: Exposing the Loudest Lies of Russian Propaganda', *Russia's War in Ukraine*, 21 March 2024, https://war.ukraine.ua/articles/azov-contra-fake-exposing-the-loudest-lies-of-russian-propaganda/; 'AZOV CONTRA FAKE | Myths about Azov Brigade', Avoz Contra Fake, accessed 3 November 2025, https://www.azovcontrafake.com.

92 Digital Forensic Research Lab, 'Russian War Report: Competing Narratives about the Sinking of Russia's Moskva Warship', *Atlantic Council*, 15 April 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-competing-narratives-about-the-sinking-of-russias-moskva-warship/.

93 Sofia Romansky et al., *The Parallel Front: An Analysis of the Military Use of Information in the First Seven Months of the War in Ukraine* (The Hague Centre for Strategic Studies, 2022), 17; *Russian Warship: Moskva Sinks in Black Sea*, 14 April 2022, https://www.bbc.com/news/world-europe-61114843.

94 The Federal, 'Big Blow to Putin as Russian Warship Moskva Sinks in Black Sea', 15 April 2022, https://thefederal.com/international/big-blow-to-putin-as-russian-warship-moskva-sinks-in-black-sea.

95 'How Big a Loss to Russia Is the Sinking of the Moskva Missile Cruiser?', Europe, *Reuters*, 15 April 2022, https://www.reuters.com/world/europe/how-big-loss-russia-is-sinking-moskva-missile-cruiser-2022-04-15/.

96 Microsoft Threat Intelligence, *A Year of Russian Hybrid Warfare in Ukraine: What We Have Learned about Nation State Tactics so Far and What May Be on the Horizon*, Microsoft Security Compliance and Identity (2023), https://nsarchive.gwu.edu/sites/default/files/documents/s9zfme-rssdn/2023-03-15-Microsoft-A-year-of-Russian-hybrid-warfare-in-Ukraine-MS-Threat-Intelligence.pdf.

General Staff, with the key number reporting that 1.7 million Ukrainian soldiers were dead or missing, with a broader threat that the groups possessed mases of information on the Ukrainian Special Operations Forces and Main intelligence Directorate.[97] The Ukrainian Centre for Countering Disinformation immediately responded to this information, debunking it by outlining how the claim was both factually impossible, as "As of January 2025, according to the words of Ukrainian President Volodymyr Zelenskyy, the size of the Ukrainian army was 880 thousand people", sharing actual casualty statistics, and stating the aim of this disinformation: "to demoralise Ukrainians, convince the world of the "exhaustion and inefficiency of the Ukrainian Armed Forces," and weaken its international support."[98] Nonetheless, this does not exclude the reality that some sensitive documents were still accessed, and that these were in turn used to legitimise fictious data.[99] Ultimately, the leaked information itself was likely less impactful than the fact that Ukrainian organisations were immediately forced to redirect attention and precious human resources to managing the information environment.

Additional examples of this shift include the increasing use of spoofed domains and Doppelgänger websites, which replicated trusted media outlets to confuse and mislead the public.[100] Crucially, this tactic reached beyond Ukraine, with international platforms Le Monde, The Guardian, Ansa, Der Spiegel, and Fox News being targeted.[101] These efforts were supplemented by proxy "fact-check" brands designed to lend credibility to the disinformation being spread.[102] Further tactics have continued to employ bots and artificial amplification of content on social media, especially Telegram, which became indispensable as part of Ukraine's information environment as well as a part of defence, as Telegram hosted channels that connected civilians and combatants for live updates about attacks.[103] While still underpinned by broader symbolic themes, these adapted tactics aimed to capitalise on specific contentious content.

Countermeasures and Impact

Ukraine's response to Russian information manipulation since 2022 has been marked by adaptability, bottom-up multi-actor coordination, and rapid innovation across government, industry, and civil society. Multiple national agencies have taken on central roles in countering Russian disinformation, including the Ministry of Defence, the Centre for Strategic Communications and Information Security, and the Security Service of Ukraine in the

97 This source contains fake news, and is referenced as an example of FIMI rather than a source William Moore, 'Ukraine's Military Losses: 1.7 Million Soldiers Exposed by Hackers', *Military Affairs*, 20 August 2025, https://voennoedelo.com/en/posts/id391-ukraine-s-military-losses-1.7-million-soldiers-exposed-by-hackers.

98 Ivan Slychko, 'Fake about 1.7 Million Dead and Missing AFU Soldiers in the War against Russia | Центр Протидії Дезінформації', Центр Протидії Дезінформації, 20 August 2025, https://cpd.gov.ua/en/international-threats-en/usa/fake-about-1-7-million-dead-and-missing-afu-soldiers-in-the-war-against-russia/.

99 Mared Gwyn Jones, 'Verifying Russian Claim That Ukraine Has Lost 1.7 Million Soldiers', My-Europe_my-Europe-Series, *Euronews*, 27 August 2025, 119400, http://www.euronews.com/my-europe/2025/08/27/verifying-russian-propagandists-claim-that-ukraine-has-lost-17-million-soldiers.

100 USCYBERCOM Public Affairs, 'Russian Disinformation Campaign "DoppelGänger" Unmasked: A Web of Deception', U.S. Cyber Command, 9 March 2024, https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/.

101 'What Is the Doppelganger Operation? List of Resources', *EU DisinfoLab*, n.d., accessed 3 November 2025, https://www.disinfo.eu/doppelganger-operation/.

102 'Fake: No Information War Is Being Waged against Russia', War on Fakes, 31 May 2022, https://web.archive.org/web/20220531134511/https:/waronfakes.com/civil/fake-no-information-war-is-being-waged-against-russia/.

103 Peter Schrijver, 'Ukrainian Intelligence's Use of Telegram in Wartime', *International Journal of Intelligence and CounterIntelligence*, 8 July 2025, 1–27, https://doi.org/10.1080/08850607.2025.2522222; Elizaveta Chernenko and William H. Dutton, 'The Role of Telegram in Wartime Ukraine: Trust, Utility, and Controversy', SSRN Scholarly Paper no. 5669030 (Social Science Research Network, 26 October 2025), https://doi.org/10.2139/ssrn.5669030.

development and implementation of both capabilities.[104] Their efforts included bolstering hard law tools against FIMI, such as legal restrictions on foreign outlets identified as spreading propaganda and enforcing sanctions against media actors linked to Russian intelligence.[105] More soft law efforts, such as coordinated messaging guidelines, fact-checking networks, and media literacy programs,[106] have further been supported by supranational partners, such as the EU's East StratCom Task Force, the NATO StratCom Centre of Excellence, and coordinated platform-level interventions from private companies.[107] Simultaneously, firms such as Reface and knowledge organisations like the Centre for Countering Disinformation have expanded Ukraine's capacity to threat detection, digital activism, and counter messaging especially during the high-intensity early phase of the invasion.[108]

Ukraine's experience illustrates how the pressure of an existential threat can accelerate changes in approaches and responses to multi-domain threats.

Ukraine's experience illustrates how the pressure of an existential threat can accelerate changes in approaches and responses to multi-domain threats. Faced with simultaneous kinetic, cyber, and informational challenges, Ukrainian authorities have had to make difficult choices about where to allocate already limited resources, balancing immediate defensive needs with longer-term resilience-building. Measuring the impact of Russian information operations in this context is inherently difficult, as their effects are diffuse, cumulative, and closely intertwined with developments on the battlefield and in diplomacy. Yet Ukraine's layered response demonstrates that while no single intervention can neutralise disinformation, their combined effect raises the cost of manipulation and limits its reach.

One of the most distinct features of Ukraine's approach to information defence has been its bottom-up agility. Rather than relying solely on state-produced and sanctioned, top-down communications, Ukrainian authorities have embraced spontaneous and emotionally resonant content produced by ordinary citizens and frontline actors. The, now iconic, messaging around 'Snake Island' is a telling example. On the first day of the invasion the Moskva ordered Snake Island, a 17 hectare Ukrainian outpost in the North-Western Black, to surrender to which Ukrainian border guards responded "go f*ck yourself".[109] Beyond its strategic and operational importance, and despite its capture by Russia, this real-time battlefield exchange was almost instantaneously transformed into a national symbol of resistance and inspiration for all Ukrainians, not because it was scripted but because military personnel, government communications teams, and online communities collaborated to create a unifying narrative.[110] This illustrates that effective counter-FIMI is not always about perfect truth conditions. Rather, narrative resilience relies on legitimacy, salience, resonance, and distribution, not just facticity.

---

104 Todd C. Helmus and Khrystyna Holynska, *Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict* (RAND Corporation, 2024).

105 Hanna Shtepa, 'Ukraine Introduces Extensive Sanctions Packages against Russian Media Personalities', *Global Sanctions and Export Controls Blog*, 20 January 2023, https://sanctionsnews.bakermckenzie.com/ukraine-introduces-extensive-sanctions-packages-against-russian-media-personalities/; *Russian Media Organisations Banned for Three Years in Ukraine* (Council of Europe, 2016), https://rm.coe.int/ukraine-reply-en-russian-media-organisations-banned-for-three-years-in/16808c9a28.

106 'Anti-Fake', Центр Стратегічних Комунікацій, 26 August 2025, https://spravdi.gov.ua/en/anti-fake/.

107 'Questions and Answers about the East StratCom Task Force | EEAS', accessed 3 November 2025, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en; 'Program of Work', NATO Strategic Communications Centre of Excellence, accessed 3 November 2025, https://stratcomcoe.org/projects/program-of-work.

108 'Reface Stands with Ukraine. How We Work in a Wartime', *Reface Blog*, 17 March 2022, https://reface.ai/blog/reface-stands-with-ukraine/; 'Center for Countering Disinformation', Center for Countering Disinformation, accessed 3 November 2025, https://cpd.gov.ua/en/.

109 Romansky et al., *The Parallel Front: An Analysis of the Military Use of Information in the First Seven Months of the War in Ukraine*, 11.

110 Antonia Colibășanu et al., *The Strategic Importance of Snake Island* (Center for European Policy Analisys, 2022), https://cepa.org/comprehensive-reports/the-strategic-importance-of-snake-island/; Veronika Iutska, 'Snake Island, Cotton and More: 6 Symbols of the War', *Russia's War in Ukraine*, 11 October 2022, https://war.ukraine.ua/articles/snake-island-cotton-and-more-6-symbols-of-the-war/.

Yet another key lesson can be drawn from the case Ukraine on resilience. There is a profound psychological toll to prolonged conflict which contributes to fatigue and vulnerability. When confronted with a relentless stream of often contradictory information, and where misjudgement in the case of combatants could even mean life or death, the trust of individuals in institutions and information sources will gradually erode. While FIMI plays a role in this, such erosion must also be understood as a human consequence of living in a state of warfare, where uncertainty becomes endemic. This is why certain frames may still persist, as alternative understandings of reality might be easier to digest. But in the same way as Ukrainian authorities responded in a diffuse way, such strategy has a counter effect: individuals' interaction with information is also diffusing. And so, Ukraine is confronted with more ambient disinformation based on confirmation bias related to internalised sentiments, rather than consequences of concerted actions by Russia or other malicious actors. This is a threat in its own right, and far more difficult to combat.

Ultimately, the war in Ukraine demonstrates that hybrid information tactics do not disappear when conventional conflict erupts, they adapt. Russian messaging has been closely synchronised with kinetic, cyber, and diplomatic actions, forming a systemic campaign rather than isolated incidents. Ukraine's evolving countermeasures show that national resilience depends not only on defensive capabilities but also on societal cohesion, adaptable narrative strategies, and international support.

Ultimately, the war in Ukraine demonstrates that hybrid information tactics do not disappear when conventional conflict erupts, they adapt.

2.2.2. **Poland**

Historical context and contemporary geopolitics

Although Polish-Ukrainian relations have historically been marked by grievances and contested memory, Warsaw has emerged as one of Kyiv's strongest supporters since Russia's full-scale invasion of Ukraine. Poland has provided substantial material assistance, for instance, and has hosted large numbers of Ukrainian refugees.[111]

Given its geopolitical position as an EU and NATO member on the Alliance's eastern flank, as well as its prominent support for Ukraine, Poland has become a key target for adversarial hybrid strategies aimed at destabilising both national institutions and undermining broader Western cohesion.[112] Until relatively recently, disinformation was not widely recognised as a central policy concern in Poland. However, since 2015, migration has become a polarising issue in domestic politics, creating fertile ground for manipulation.[113] Over time, Poland has increasingly been exposed to FIMI activities, including coordinated disinformation campaigns, dark web recruitment efforts, and organised propaganda dissemination. These activities tend to intensify during election periods and are amplified across platforms such as X, Facebook, YouTube, TikTok, and Telegram. The primary source of FIMI activities targeting Poland is Russia, with some additional attribution to China.[114]

Targets and tactics

Russia's full-scale invasion of Ukraine marked a turning point in Poland's online disinformation landscape. In the early stages of the war, Russian-linked networks spread false information across social media platforms in an effort to incite anti-Ukrainian sentiment. Analysts observed that many of the accounts disseminating war-related falsehoods had previously been involved in spreading disinformation about COVID-19, suggesting continuity within pro-Kremlin influence ecosystems.[115] Despite the rapid influx of Russian disinformation, Polish society initially demonstrated considerable resilience. In the first months of the war, many Polish citizens sheltered Ukrainian refugees, reinforcing public solidarity and limiting the immediate impact of hostile narratives.[116] However, as economic tensions between Poland and Ukraine emerged in late 2023, this coincided with a noticeable increase in anti-Ukrainian rhetoric, including portrayals of Ukrainians as "greedy, overly privileged, and taking jobs away from Poles".[117]

Poland has long been vulnerable to cyber and psychological operations. Notable FIMI tactics have included the dissemination of translated Russian propaganda through networks such

111 Andrian Prokip, 'A New Crack in Polish-Ukrainian Relations Poses Risks for Both Countries | Wilson Center', 5 October 2023, https://www.wilsoncenter.org/blog-post/new-crack-polish-ukrainian-relations-poses-risks-both-countries.

112 Izabela Surwillo and Veronika Slakaityte, 'Power Moves East: Poland's Rise as a Strategic European Player | DIIS', 5 November 2024, https://www.diis.dk/en/research/power-moves-east-polands-rise-as-a-strategic-european-player.

113 Mateusz Zadroga, *Disinformation Landscape Poland* (EU DisinfoLab, 2025), 21, https://www.disinfo.eu/wp-content/uploads/2025/10/20251027_Disinfo-landscape-in-Poland-V2.pdf.

114 'Poland among Key Targets of Russian, Chinese Disinformation, EU Report Finds', 100 Lat Polskiego Radia, 20 March 2025, https://www.polskieradio.pl/395/7784/artykul/3499088,poland-among-key-targets-of-russian-chinese-disinformation-eu-report-finds.

115 Mateusz Zadroga, *The Disinformation Landscape in Poland* (EU Disinfo Lab, 2025), 4, https://www.disinfo.eu/publications/disinformation-landscape-in-poland/.

116 Zadroga, *The Disinformation Landscape in Poland*, 2.

117 Zadroga, *The Disinformation Landscape in Poland*, 4.

as the so-called "Polish Pravda" ecosystem, attempts to recruit Polish citizens via the dark web with financial incentives to spread pro-Russian content, and the publication of fabricated media reports mimicking credible outlets in order to undermine electoral integrity.[118] The Doppelgänger campaign has been particularly prominent, manipulating and republishing mainstream articles to distort public perception and inflame societal divisions. Political actors (including the Civic Platform party), electoral stakeholders, journalists, and public service media have been frequent targets. Techniques have ranged from doxing and harassment to misinformation aimed at reducing voter turnout and eroding confidence in democratic processes.[119] Other disinformation campaigns have also exploited domestic issues, including the status of Ukrainian refugees or women's reproductive rights.

Countermeasures and impact

In response to FIMI operations, Poland has developed a multi-layered counter-FIMI approach combining national and supranational instruments.

At the national level, the Ministry of Foreign Affairs has linked FIMI countermeasures to the establishment of a Resilience Council, engaging NGOs and academic institutions, with a second council planned under the Ministry of Digitalisation.[120] Additional oversight bodies, including the Committee for Special Services, the National Defence committee, and the Administration and Internal Affairs committee, regularly review FIMI-related developments.[121]

A central operational actor is Poland's National Research and Academic Network (NASK), which hosts a dedicated centre for analysing disinformation during election periods.[122] In coordination with the Ministry of Digital Affairs, NASK monitors the online information environment during "electoral silence" - the legally mandated period without campaigning prior to elections. [123] This monitoring functions as an early warning system capable of identifying sophisticated bot networks as well as more conventional threats such as incitement to violence. During the 2025 national elections, NASK identified alleged foreign-financed political advertisements on Facebook and successfully requested their removal by Meta.[124] Beyond its operational role, NASK also invests in long-term resilience by strengthening digital competencies among students, teachers, parents, and law enforcement officials through educational programmes and cybersecurity workshops.[125]

At the supranational level, the EU has played a significant role. Mechanisms such as the Rapid Alert System (RAS), the FIMI Information Sharing and Analysis Centre (FIMI ISAC), and the Counter-FIMI Toolbox enhance situational awareness, facilitate information exchange, and coordinate responses, particularly in the electoral context.[126] Poland's approach combines

---

118 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report* (FIMI-ISAC, ISD, Debunk.org, Counter Disinformation Network, Alliance4Europe, 2025), 6–7, https://fimi-isac.org/wp-content/uploads/2025/05/POLISH-CERA.pdf.

119 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 7.

120 Onno Hansen-Staszyński, *(15) The Polish Resilience Council(s)* (Saufex EU, 2024), https://saufex.eu/post/15-The-Polish-Resilience-Councils.

121 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 40.

122 'Protecting Internet Users', accessed 10 December 2025, https://www.nask.pl/en/institute/for-you.

123 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 50.

124 Karl Badohal, 'Poland Finds What It Says May Be Foreign-Funded Election Interference', Europe, *Reuters*, 14 May 2025, https://www.reuters.com/world/europe/poland-uncovers-what-it-says-may-be-foreign-funded-election-interference-2025-05-14/.

125 'Protecting Internet Users', accessed 10 December 2025, https://www.nask.pl/en/institute/for-you.

126 'Countering Foreign Information Manipulation and Interference (FIMI) - Polish Platform for Homeland Security', 26 June 2024, https://ppbw.pl/en/countering-fimi/.

soft and hard law instruments. Soft law tools (such as guidelines, recommendations, and public awareness campaigns) form the backbone of media literacy initiatives and institutional briefings. Hard law measures include the enforcement of EU Regulation 2024/900 on political advertising transparency.[127] Domestically, the provisions of the Polish Criminal Code have been applied to prosecute public incitement to aggression (Art. 117 §3) and participation in disinformation activities on behalf of foreign intelligence services (Art. 130 §).[128]

However, Poland lacks comprehensive legal competences to systematically prosecute the dissemination of disinformation. Existing provisions primarily address defamation, hate speech, the promotion of totalitarian ideologies, or Holocaust denial. Broader public harm resulting from false information is generally recognised as unlawful only during election periods.[129] Civil society actors play a crucial complementary role. Poland's first major independent fact-checking organisation, Demagog, monitors misleading narratives, debunks false claims, and analyses political promises. In addition to its investigative work, Demagog conducts workshops and seminars to enhance fact-checking skills and media literacy. Since its establishment, the organisation has delivered training to approximately 18,000 participants, while around 4,000 users have engaged with its digital education platform.[130] Other organisations, such as AFP Sprawdzam, FakeNews.pl, and Pravda Association, also verify public claims related to COVID-19, the war in Ukraine, migration, LGBTQ+ issues, women's rights, and public health.[131]

Poland's counter-FIMI efforts can broadly be divided into mitigation and prevention.

Poland's counter-FIMI efforts can broadly be divided into mitigation and prevention. Mitigation measures include sanctions against Russian media outlets and the enforcement of criminal law provisions. However, these have been constrained by the adversaries' ability to shift operations to Telegram and the dark web.[132] Preventive measures include strategic communication, expert monitoring, and diplomatic outreach. While Poland has successfully disrupted certain influence operations, recurring campaigns such as Doppelgänger demonstrate ongoing vulnerabilities.[133] Threat actors continue to adapt, and no confirmed deterrent has effectively curtailed dark web recruitment efforts. Structural challenges inconsistent enforcement of sanctions on digital platforms, slow institutional adaptation to emerging tactics, limited public-private operational infrastructure, and a shortage of specialised personnel trained in disinformation analysis. Moreover, public trust in media and political institutions remains fragile, influenced by longstanding debates over media independence and judicial reforms.[134] This environment provides opportunities for disinformation actors to exploit legal grey zones and the opacity of social media ecosystems.

Taken together, Poland's experience illustrates both progress and constraint: while institutional capacity and civil society engagement have expanded considerably, persistent structural weaknesses and adaptive adversaries continue to test the resilience of Poland's information environment.

127 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 40–41.

128 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 42–43.

129 Zadroga, *The Disinformation Landscape in Poland*.

130 'Transparency Center', March 2025, https://disinfocode.eu/reports/demagog/5?chapterId=50&commitmentId=250.

131 Zadroga, *The Disinformation Landscape in Poland*, 16.

132 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 41.

133 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 41.

134 Kinga Margas et al., *Poland: Country Election Risk Assessment (CERA) | FIMI Response Team Report*, 38, 58.

2.2.3. **Moldova**

Historical context and contemporary geopolitics

Since gaining independence from the Soviet Union in 1991, Moldova has been a sustained target of Russian disinformation campaigns. These efforts have intensified following Russia's full-scale invasion of Ukraine and the increasingly pro-European orientation of Moldova's government.[135]

Beyond socio-economic fragilities and energy dependencies, one of Moldova's structural vulnerabilities lies in the unresolved status of the self-declared autonomous region of Transnistria.[136] Owing to its linguistic, political, and social ties with Russia, Transnistria functions as a staging ground for Russian information operations and coordination efforts. This dynamic has become more pronounced since Moldova received EU candidate status in 2023 and began reducing its dependence on electricity and gas supplied via Transnistria.[137]

Targets and tactics

Although Moldova has been exposed to a range of disinformation narratives – including conspiracy theories surrounding George Soros or claims advocating unification with Romania – Russia remains the principal threat actor. Moscow employs a combination of overt and covert tactics, including security-related rhetoric from Russian diplomatic representatives, cyberattacks, bomb threats, and coordinated disinformation campaigns amplified through pro-Russian politicians and media proxies in autonomous regions.[138]

A notable example was the coordinated disinformation campaign surrounding Moldova's constitutional amendment on future EU treaty adoption and the presidential elections held in November 2024.[139] This campaign combined digital interference with psychological pressure tactics. Cyberattacks targeted the Central Election Commission, while a series of false bomb threats disrupted Moldovan diplomatic missions abroad, apparently aiming to discourage diaspora voters from supporting pro-European President Maia Sandu.

Additionally, forged correspondence, supposedly from EU institutions, was circulated among officials and businesses, falsely claiming that the EU intended to relocate migrants from the Middle East to Moldova in order to stabilise its labour market. Telegram users were also recruited via a chatbot named "STOP EU/СТОП ЕС", which reportedly offered financial incentives to publish anti-EU content and vote against European integration.[140] The campaign

135 Anastasia Pociumban, 'Moldova's Response to Hybrid Attacks: A Learning-by-Doing Strategy', *HCSS*, 31 October 2023, 3, https://hcss.nl/report/moldovas-response-to-hybrid-attacks/.

136 Samorukov, 'In Odesa's Shadows: What Is Russia's Strategy in Moldova?', Carnegie Endowment for International Peace, accessed 8 September 2025, https://carnegieendowment.org/research/2024/10/moldova-russia-strategy?lang=en.

137 Anastasia Pociumban, 'Moldova's Response to Hybrid Attacks', 8.

138 Petru Culeac, *Moldova Policy Alert: Disinformation and Foreign Interference in Moldovan Elections* (Moldova Development Institute, n.d.), 2, accessed 2 September 2025, https://epde.org/wp-content/uploads/2024/10/Moldova-Policy-Paper-2-Disinformation-and-Foreign-Interference-in-Moldovan-Elections-1.pdf. Anastasia Pociumban, 'Moldova's Response to Hybrid Attacks', 3.;Culeac, *Moldova Policy Alert: Disinformation and Foreign Interference in Moldovan Elections*, 3.

139 Culeac, *Moldova Policy Alert: Disinformation and Foreign Interference in Moldovan Elections*, 3.; Jakub Pieńkowski, *Sandu Wins, Constitutional Referendum Passes in Moldova* (PISM, n.d.), accessed 3 September 2025, https://pism.pl/publications/sandu-wins-constitutional-referendum-passes-in-moldova.

140 Filip Bryjka, *Russian Interference Nearly Overwhelmed Moldovan Presidential Election-Referendum Vote* (The Polish Institute of International Affairs, 2024), https://pism.pl/publications/russian-interference-nearly-overwhelmed-moldovan-presidential-election-referendum-vote.

was allegedly financed by the pro-Russian oligarch Ilan Şor. Beyond funding disinformation campaigns, Moscow has supported political actors opposing Moldova's pro-EU trajectory. Chief amongst those was the Șor Party, which Moldova's Constitutional Court declared unconstitutional after repeated sanctions for illegal campaign financing.[141]

Countermeasures and impact

The European Union plays a central role in combatting the growing risks of interference in Moldova. To strengthen the country's cybersecurity capacity, the Union deployed the EU Partnership Mission to Moldova (EUPM). Its mandate includes advising Moldovan authorities on the development and implementation of strategies to counter disinformation and foreign interference, particularly in the context of the parliamentary elections of September 2025.[142] A central component of its work involves strengthening crisis response mechanisms, including support for the establishment of a National Crisis Management Centre. Cybersecurity and counter-FIMI capacity-building form core pillars of the mission's activities.

The EUPM also played a facilitating role in supporting the creation of new institutions, including Moldova's Cybersecurity Agency and the Centre for Strategic Communication and Countering Disinformation. In 2024 and June 2025, Moldova and the EUPM also conducted hybrid threat simulation exercises involving representatives from major technology platforms such as Google, Meta, and TikTok, alongside fact-checkers and civil society organisations.[143]

At the national level, Moldova has sought to strengthen its legislative framework and institutional capacity to counter FIMI. Amendments to the Audiovisual Media Services Code aim to protect media pluralism, increase transparency of ownership, and introduce sanctions against outlets repeatedly violating media and electoral regulations.[144] Law No. 143, implemented in June 2022, further restricted the transmission of audiovisual content produced in states that have not ratified the European Convention on Transfrontier Television, particularly where such content incites hatred or military aggression.[145]

Moldovan authorities have also suspended several television stations and websites for spreading disinformation deemed to threaten national security.[146] While these measures reduced the reach of Russian-aligned broadcasting with large domestic audiences, disinformation activity has increasingly shifted to online platforms such as Telegram, where regulatory oversight and scrutiny is more limited.[147] Following the experience of electoral interference in 2024, Moldova proposed draft Law No. 381, introducing stricter penalties for electoral fraud and tighter rules on political party registration. However, the OSCE Office for

141 Culeac, *Moldova Policy Alert: Disinformation and Foreign Interference in Moldovan Elections*, 7.

142 'About EU Partnership Mission in the Republic of Moldova | EEAS', accessed 3 September 2025, https://www.eeas.europa.eu/eupm-moldova/about-eu-partnership-mission-republic-moldova_en?s=410318.

143 'Commission Services and Moldovan Authorities Conduct a Stress Test on Potential Digital Hybrid Threats to Election Integrity Ahead of Moldova's Parliamentary Elections | Shaping Europe's Digital Future', accessed 3 September 2025, https://digital-strategy.ec.europa.eu/en/news/commission-services-and-moldovan-authorities-conduct-stress-test-potential-digital-hybrid-threats.

144 Joseph Matveyenko, *Assessing the Impact of Disinformation on Minority Communities in Moldova* (Media Enabling Democracy, Inclusion and Accountability in Moldova (MEDIA-M) project, 2023), 4, https://freedomhouse.org/sites/default/files/2023-12/fh-pb_19-Disinformation-Moldova-Minorities_Eng-v2.pdf.; Culeac, *Moldova Policy Alert: Disinformation and Foreign Interference in Moldovan Elections*.

145 'Moldova Adopts New Anti-Disinformation Law | CSOMETER', 6 July 2022, https://csometer.info/updates/moldova-adopts-new-anti-disinformation-law.

146 Culeac, *Moldova Policy Alert: Disinformation and Foreign Interference in Moldovan Elections*, 7.

147 Culeac, *Moldova Policy Alert: Disinformation and Foreign Interference in Moldovan Elections*, 3.

Democratic Institutions and Human Rights cautioned that certain terms, such as "extremism" were insufficiently defined and risked suppressing legitimate dissent.[148]

To improve inter-agency coordination, Moldova has established the Centre for Strategic Communication and Combating Disinformation in 2023, recently placed under the authority of the presidency.[149] The Centre is tasked with developing countermeasures against FIMI and disinformation campaigns, facilitating cooperation with civil society, and enhancing strategic communication.[150] While European partners, including Lithuania, have expressed interest in supporting Moldova's development of early warning systems and communication strategies, institutional development and staffing constraints remain ongoing challenges.[151]

To improve inter-agency coordination, Moldova has established the Centre for Strategic Communication and Combating Disinformation in 2023.

In recognition of the convergence between cyberattacks and information operations, Moldova adopted a new cybersecurity law aligned with EU standards on network and information system security. This legislation introduces compliance obligations for institutions and service providers, thereby strengthening resilience among critical infrastructure operators. The drafting process was supported by Estonia's e-Governance Academy and funded through the EU's Moldova Rapid Assistance Project.[152]

Assistance from the e-Governance Academy also contributed to the establishment of the National Agency for Cyber Security, which is responsible for implementing cybersecurity policy, establishing an incident response team, coordinating across institutions, and promoting public awareness and cybersecurity education.[153] Alongside institutional strengthening, Moldova has invested in media literacy initiatives. The EU-funded project "Building Resilience in Moldova" (BRIM) aims to raise awareness of disinformation threats and increase access to reliable information, particularly for vulnerable groups. The Independent Centre for Countering Disinformation (ICDC) coordinates implementation with local stakeholders.[154] Similarly, the Institute for War and Peace Reporting (IWPR), in partnership with the Centre for Independent Journalism, has launched initiatives to enhance societal resilience. These include monitoring social media narratives, producing podcasts, and publishing educational materials on Mediacritica, an online media literacy platform.[155]

Despite these efforts, experts assess the overall effectiveness of Moldova's countermeasures as mixed. The suspension of broadcasting licences for six major pro-Russian television channels linked to Ilan Şor in December 2022 reduced domestic viewership of Russian programming, yet the content remains accessible online. Moreover, the suspension did not

148 Urgent Opinion on the Draft Law of the Republic of Moldova No. 381 of 17 December 2024 "On Amendments to Certain Normative Acts on the Effective Combat Against the Phenomenon of Electoral Corruption and Related Aspects" (2025), 2, https://www.osce.org/sites/default/files/f/documents/4/9/593486.pdf.

149 Iurie Tataru, 'Moldova's Disinformation Center Now under Presidency', 12 August 2025, https://moldova1.md/p/54940.

150 Denis Cenusa, 'Moldova's Handling of Russian Disinformation: Building New Tools and Uprooting Old Patterns', Geopolitics and Security Studies Center, GSSC (Previously Known as Eastern Europe Studies Centre, EESC), 2 May 2024, https://www.gssc.lt/en/publication/moldovas-handling-of-russian-disinformation-building-new-tools-and-uprooting-old-patterns/.

151 Denis Cenusa, 'Moldova's Handling of Russian Disinformation'.

152 'Moldova Adopted the EU-Backed Cybersecurity Law | EEAS', accessed 10 December 2025, https://www.eeas.europa.eu/delegations/moldova/moldova-adopted-eu-backed-cybersecurity-law_en?s=223.

153 'Moldova Establishes National Cybersecurity Agency with eGA Expertise » E-Riigi Akadeemia', 27 December 2025, https://ega.ee/moldova-establishes-national-cybersecurity-agency/.

154 'BRIM - Building Resilience in Moldova', *EU NEIGHBOURS East*, 10 December 2025, https://euneighbourseast.eu/projects/eu-project-page/.

155 Victoria Tataru, *Empowering Citizens: Combating Disinformation through Media Literacy and Critical Thinking - IJC*, 22 October 2025, https://cji.md/en/empowering-citizens-combating-disinformation-through-media-literacy-and-critical-thinking/.

fully rely on the framework of the Audiovisual Media Services Code, raising questions about legal consistency.[156]

Platform enforcement has also been uneven. While Meta removed disinformation flagged by fact-checkers, Telegram has been less responsive, allowing tools such as the STOP EU/СТОП ЕС chatbot to continue operating.[157]

Overall, Moldova has made measurable progress in strengthening institutional capacity and legislative safeguards, particularly with external support. However, persistent structural vulnerabilities, including platform governance gaps, resource constraints, and the politicisation of information, continue to limit the effectiveness of its counter-FIMI strategy.

2.2.4. **Romania**

Historical context and contemporary geopolitics

Historically, Romanian public opinion has been strongly oriented towards the West. Due to past experiences with Soviet domination, most Romanians hold unfavourable views of Russia and broadly support Euro-Atlantic integration.[158] In 2024, opinion polling indicated that 83% of Romanians supported EU membership and 88% supported NATO membership.[159]

For many years, this strong pro-Western consensus contributed to the perception that Romania was relatively insulated from Russian influence operations. However, the rise of far-right political movements has introduced new vulnerabilities. Parties such as SOS and AUR have promoted narratives that align with or echo pro-Russian positions, although the latter often frames its positions more ambiguously. At the same time, Romania's firm anchoring in Western institutions has increased its strategic relevance. The country is set to host NATO's largest military base in Europe and plays an active role in training Ukrainian pilots to operate F-16 fighter jets supplied by European NATO members.[160] Despite these developments, Romania was long considered a secondary target for Russian disinformation, largely because overt pro-Russian narratives have limited traction in a society where Russia is widely perceived as a threat.

Targets and tactics

The perception of low external vulnerability shaped Romania's regulatory landscape. For years, the legislative framework addressing disinformation, primarily overseen by the National Audiovisual Council for broadcast media and the National Council for Combating Discrimination for hate speech, focused predominantly on domestic actors. As a result,

156 Anastasia Pociumban, 'Moldova's Response to Hybrid Attacks', 2. ; Matveyenko, *Assessing the Impact of Disinformation on Minority Communities in Moldova*, 4.

157 Filip Bryjka, *Russian Interference Nearly Overwhelmed Moldovan Presidential Election-Referendum Vote*.

158 *Foreign Information Manipulation and Interference Threats and Answers in Romania in the Context of the War in Ukraine* (Global Focus | International Republican Institute, 2024), https://www.global-focus.eu/2024/10/foreign-information-manipulation-and-interference-threats-and-answers-in-romania-in-the-context-of-the-war-in-ukraine/.

159 Patrik Szicherle, *Pubic Attitudesin Romania: Staying in the West with Some Doubt* (Globsec, 2024), 9, https://www.globsec.org/sites/default/files/2024-10/Public%20Attitudes%20in%20Romania.pdf.

160 Madalin Necsutu, 'Romania To Host Largest NATO Military Base in Europe', *Balkan Insight*, 21 March 2024, https://balkaninsight.com/2024/03/21/romania-to-host-largest-nato-military-base-in-europe/. ; *Final Dutch F-16 Jets Delivered to European Training Centre in Romania* (2024), https://defence-industry.eu/final-dutch-f-16-jets-delivered-to-european-training-centre-in-romania/.

legislation specifically addressing foreign information manipulation remained underdeveloped when Russia's invasion of Ukraine heightened pressure across the region.[161]

Romania has been exposed to influence from a range of actors, including evangelical networks promoting illiberal values and political spillover from Hungary's governing Fidesz party affecting minority politics in Romania. Nevertheless, Russia remains the most significant external concern. Given Romania's broadly negative public perception of Russia, disinformation campaigns rarely attempt to portray Moscow favourably. Instead, they focus on undermining trust in the European Union, fostering anti-Ukrainian sentiment within segments of the far right, and exploiting socio-economic anxieties related to inflation, security, and regional instability.[162]

A prominent example of foreign interference occurred during Romania's presidential elections in November 2024. Pre-election polls suggested that the ultranationalist candidate Călin Georgescu would receive approximately 5% of the vote. Instead, he secured nearly 23% in the first round.[163] Subsequent investigations revealed that this surge was supported by a coordinated foreign influence operation involving thousands of automated or semi-automated TikTok accounts and networks linked to Russian actors. These accounts amplified a "Romania first" narrative and promoted messaging aligned with Kremlin interests, including calls to end the war in Ukraine.[164]

Countermeasures and impact

Romanian authorities have formally identified disinformation as a national security concern in the National Defence Strategy 2020-2024. However, practical implementation of countermeasures has been limited. The Presidential Administration has announced plans to develop a comprehensive strategy to address disinformation, yet the document has not been published.

Media investigations suggest that only two concrete measures have been introduced by the government. The first is an online platform that uses artificial intelligence to aggregate and read news from the Agerpres news agency, presented as a tool to promote quality journalism and reduce exposure to disinformation. The second is the InfoRadar platform, which allows citizens to report false information related to the Romanian armed forces. However, InfoRadar has been operational since 2020 and therefore predates the recent escalation in FIMI targeting Romania.[165]

Institutionally, responsibility for countering disinformation rests primarily with the Romanian Authority for Management and Regulation in Communications (ANCOM) and the National Audiovisual Council (CNA). ANCOM serves as Romania's coordinator for the EU Digital

---

161 *Foreign Information Manipulation and Interference Threats and Answers in Romania in the Context of the War in Ukraine*.

162 Ciprian Cucu, *The Disinformation Landscape in Romania* (EU Disinfo Lab, 2025), 4–5, https://www.disinfo.eu/publications/disinformation-landscape-in-romania/.

163 Sarah Shamim, 'Who Is Calin Georgescu, Romanian Right-Wing Candidate Leading the Election?', *Al Jazeera*, n.d., accessed 22 January 2026, https://www.aljazeera.com/news/2024/11/25/who-is-calin-georgescu-romanian-right-wing-candidate-leading-the-election.

164 Andra-Lucia Martinescu et al., *Networks of Influence: Decoding Foreign Meddling in Romania's Elections* (The Foreign Policy Centre, n.d.), 11, https://fpc.org.uk/wp-content/uploads/2024/12/Networks-of-Influence-Decoding-foreign-meddling-in-Romanias-elections-2024.pdf.

165 Iulia Stanoiu, 'Romania's Anti-Disinformation Plan Fails: Secrets and Controversies', 2 May 2025, https://context.ro/serviciile-de-informatii-administratia-prezidentiala-si-guvernul-au-scris-si-tin-la-secret-planul-national-anti-dezinformare-care-a-esuat/.

Services Act (DSA), which aims to enhance transparency and accountability among large online platforms. In 2025, the EU formally integrated the Code of Conduct on Disinformation into the DSA framework, introducing provisions to reduce advertising revenues for disinformation actors and increase transparency in political advertising.[166]

However, ANCOM's credibility has been questioned following the 2023 appointment of its president, Valeriu Zgonea, who had previously been convicted of conflict-of-interest charges.[167] Preliminary assessments indicate that platform compliance with DSA obligations in Romania remains moderate.[168] Even though National Audiovisual Council has expanded its mandate to include certain online audiovisual content and has requested the removal of several social media posts, civil society organisations have criticised inconsistent enforcement. For example, the removal of a video by media personality Marius Tucă triggered concerns regarding freedom of expression, particularly given the CNA's comparatively lenient approach to disinformation during the COVID-19 pandemic.[169]

Although Romania's Constitutional Court annulled the 2024 presidential election results and barred Georgescu from the subsequent rerun, broader legislative or governance reforms addressing FIMI have been limited.[170] Romania has aligned with EU-wide bans on Russian state-affiliated outlets such as RT and Sputnik and has drafted legislation targeting deepfake-related disinformation, though this proposal has faced criticism.[171] In fact, much of the current legislation, does not require institutions to carry out activities to combat disinformation and a formal document on strategic communication is missing.

Beyond state institutions, civil society actors play a central role. National and transnational fact-checking networks contribute to debunking false narratives and strengthening media literacy.[172] The Centre for Independent Journalism, for instance, provides teacher training, classroom resources, and research on youth exposure to disinformation. It has trained over 4,500 teachers and reached approximately 100,000 students.[173] In collaboration with UNICEF, the Centre offers mentoring programmes and scholarships for journalists, focusing on responsible reporting strategies that avoid amplifying false narratives. Additionally, media literacy modules have been introduced in cooperation with ten Romanian universities since 2022.[174]

166 'The 2022 Code of Practice on Disinformation | Shaping Europe's Digital Future', accessed 9 December 2025, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

167 Madalina Botan and Andreea Stancea, *Evaluating the Implementation of the EU Code of Practice on Disinformation in Romania* (National University of Political Studies and Public Administration, 2023), 6, https://edmo.eu/wp-content/uploads/2023/09/Evaluating-the-Revised-EU-Code-of-Practice-on-Disinformation-in-Romania_v2.pdf. *Erratum: President Valeriu Zgonea was previously sentenced in 2020, but got acquitted of the charges in 2022.*

168 Madalina Botan and Andreea Stancea, *Evaluating the Implementation of the EU Code of Practice on Disinformation in Romania*, 31.

169 Ciprian Cucu and Susanna Dragomir, *Disinformation Landscape in Romania* (EU DisinfoLab, 2025), 18, https://www.disinfo.eu/wp-content/uploads/2025/11/20251103_Disinfo-landscape-in-Romania-V2.pdf; Redacția ApTI, 'CNA Nu Trebuie Să Cenzureze Abuziv Dreptul Constituțional al Cetățenilor La Libertatea de Opinie | Asociația Pentru Tehnologie Și Internet', 28 March 2025, https://apti.ro/cna-nu-trebuie-sa-cenzureze-abuziv-dreptul-constitu%C8%9Bional-al%20cetatenilor-la-libertatea-de-opinie.

170 Sarah Rainsford and Laura Gozzi, 'Georgescu Barred from Romanian Vote in Final Court Ruling', 11 March 2025, https://www.bbc.com/news/articles/cj679nk6endo.

171 *Foreign Information Manipulation and Interference Threats and Answers in Romania in the Context of the War in Ukraine*.

172 'Bulgarian-Romanian Observatory of Digital Media – Funky Citizens', accessed 3 September 2025, https://funky.ong/en/brod/.

173 'About Us - CIJ', accessed 9 December 2025, https://cji.ro/en/about-us/.

174 'Media Literacy: A Shield against the Infodemic', accessed 9 December 2025, https://www.unicef.org/romania/press-releases/media-literacy-shield-against-infodemic.

Romania also hosts a national hub of the European Digital Media Observatory, covering both Romania and Bulgaria.[175] This independent Observatory collaborates with researchers and fact-checkers specialised in disinformation, social media platforms, and media literacy to analyse disinformation trends and develop countermeasures.[176] Despite these initiatives, Romania lacks a comprehensive whole-of-society approach to countering FIMI. Analysts argue that persistent mistrust in political institutions and governance deficits create structural vulnerabilities.[177] Among segments of the Romanian diaspora, feelings of marginalisation and perceived neglect by both Romanian and host-country authorities may increase susceptibility to disinformation narratives.[178] Domestic trust levels are also low. Surveys from 2021 indicate that Romanians express greater confidence in supranational institutions such as the EU and in executive bodies like the military than in political parties, parliament, the presidency, or the media.[179] Media consumption patterns further compound these vulnerabilities. High reliance on social media and messaging applications as primary news sources increases exposure to manipulated content.[180] Interestingly, while Romanians frequently consume news via social media, surveys show comparatively lower trust in information obtained through these channels than through traditional media.[181]

A key policy implication is therefore the need to strengthen the quality, independence, and credibility of traditional media.

A key policy implication is therefore the need to strengthen the quality, independence, and credibility of traditional media.

Many outlets face challenges including political alignment, commercial pressures, limited professionalisation, and concentrated ownership structures.[182] Addressing these structural weaknesses, alongside improving governance and transparency, could significantly enhance Romania's resilience against FIMI.[183]

2.2.5. **Reflections**

The assessments of Ukraine, Poland, Moldova, and Romania demonstrate that FIMI activity presents a dynamic threat that exploits historical grievances, societal vulnerabilities, and institutional gaps. While Russia remains, the dominant actor shaping these environments, the forms and effects of FIMI vary markedly depending on geopolitical orientation, levels of societal trust, and the media ecosystem. The cases demonstrate that countering FIMI requires more than technical fixes. Resilience emerges from agile multilevel coordination, credible communication, and sustained investment in democratic institutions.

175 *"One 'Thank You' Note Can Keep You Motivated for Months": BROD Fact Checkers and Their Take on Disinformation Dynamics in Bulgaria and Romania – EDMO*, 6 November 2025, https://edmo.eu/edmo-news/one-thank-you-note-can-keep-you-motivated-for-months-brod-fact-checkers-and-their-take-on-disinformation-dynamics-in-bulgaria-and-romania/.

176 *Our Vision And Mission – EDMO*, n.d., accessed 9 December 2025, https://edmo.eu/about-us/edmoeu/our-vision-and-mission/.

177 *Foreign Information Manipulation and Interference Threats and Answers in Romania in the Context of the War in Ukraine*.

178 Alina Bârgăoanu, 'In Conversation with Alina Bargaoanu | Romania's Experience with Disinformation - Foreign Policy Research Institute', 11 July 2025, https://www.fpri.org/article/2025/11/in-conversation-with-alina-bargaoanu-romanias-experience-with-disinformation/.

179 Flavia Durach, *Disinformation, Societal Resilience and Covid-19* (ASPEN Institute Romania, 2021), 8, https://aspeninstitute.ro/wp-content/uploads/2022/03/DISINFORMATION-SOCIETAL-RESILIENCE-AND-COVID19_Report.pdf.

180 Alina Bârgăoanu, 'In Conversation with Alina Bargaoanu | Romania's Experience with Disinformation - Foreign Policy Research Institute'.

181 Flavia Durach et al., 'Countering Disinformation: A Delicate Balance between International Action and National Particularities', *Media and Communication* 13 (2025): 2–3, 8.

182 Madalina Botan, 'The Romanian Media System: Dynamics, Challenges, and Implications for Democracy', *Media and Communication* 12 (2024): 2.

183 Dessislava Boshnakova and Desislava Dankova, 'The Media in Eastern Europe', *The Media Systems in Europe* 163 (2023).

2.3. The Western Balkans: Internal vulnerabilities and growing local resilience

The Western Balkans constitutes a distinct geopolitical frontier between East and West. Over the past decades, the region has undergone a complex transition: from the legacy of the Yugoslav wars, through fragile post-conflict reconstruction, toward aspirations of European integration. However, slow and uneven institutional development has resulted in many countries remaining in a state of structural vulnerability, limiting their resilience against external pressures and making them susceptible to foreign information operations. Recent assessments highlight the urgency of developing comprehensive hybrid threat strategies that strengthen media freedom, reinforce digital and cyber defences, and safeguard information integrity.[184]

Russia's engagement in the Western Balkans combines historical, symbolic, and strategic dimensions. Although currently not a core priority of Russian foreign policy, the region occupies an important place in Moscow's political imagination, reinforced by a "heavily mythologised" narrative of Slavic brotherhood and shared Orthodox heritage.[185] Through its FIMI activity, Russia seeks to project great-power status, often acting as a spoiler to undermine Western-backed stabilisation efforts.[186] These dynamics create a common backdrop against which individual case studies, including Albania, North Macedonia, and Bosnia and Herzegovina, reveal both country-specific vulnerabilities and shared regional patterns of interference and resistance. Studying this region therefore increases awareness of the difficulty of countermeasures in a context of non-transparent media ownership, ethnic tensions, and corruption.

2.3.1. Albania

Historical context and contemporary geopolitics

Within the Western Balkans, Albania occupies a strategically important location. As a NATO member since 2009, it constitutes the Adriatic gateway into the region and serves as a critical entry point for the Western security architecture.[187] In line with this orientation, Albania presents itself as a regional stronghold against Russian influence and remains a vocal supporter of Ukraine, both at political and societal levels.[188]

Albania's geopolitical importance is further reinforced by its EU accession ambitions, which have gained renewed momentum amid increased Western engagement in the region. At the

184 Andrei Richter, *Resilience to Foreign Information Manipulation and Interference (FIMI) - Case Studies in Eastern Europe, the Western Balkans and Türkiye* (European Audiovisual Observatory and Council of Europe, 2025).

185 Wouter Zweers et al., *Little Substance, Considerable Impact*, n.d., 9.

186 Giorgio Fruscione and Paolo Magri, *Europe and Russia on the Balkan Front* (ISPI, n.d.), 129, https://www.ispionline.it/wp-content/uploads/2023/03/ISPI-Report-2023_Europe-and-Russia-on-the-Balkan-Front.pdf.

187 *The Vulnerability of Albanian Politics to Foreign Interference* (National Democratic Institute, 2024), 11, https://www.ndi.org/sites/default/files/2025-04/The-Vulnerability-of-Albanian-Politcs-to-Foreign-Interference-%281%29.pdf.

188 Tanjug, 'Albania pitches itself as bastion against Russian influence', B92.net, accessed 31 October 2025, https://www.b92.net/o/eng/news/region; Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference* (Center Science and Innovation for Development, 2024), 35, https://scidevcenter.org/wp-content/uploads/2024/10/FIMI-Analytical-Report-Albania_SCiDEV.pdf.

same time, this positioning places Albania at the intersection of competing external interests. Actors such as Russia, China, Iran and Türkiye consider Albania a strategically relevant yet challenging target for influence.

Its relatively strong pro-Western stance and continued support for Ukraine complicate direct Russian influence, yet Albania's domestic vulnerabilities (low information literacy, economic challenges, and public mistrust in institutions) create structural openings for FIMI operations.[189] Albania's alignment with NATO and the EU thus simultaneously strengthens its geopolitical position and increases its exposure to influence operations aimed at shifting public opinion and foreign policy orientation.

Targets and tactics

Unlike in some neighbouring states, Russia does not maintain a direct media presence in Albania through outlets such as RT or Sputnik. Consequently, Russian FIMI efforts rely largely on indirect and informal channels. Content originating from Russian state-affiliated sources is often republished or circulated through social media platforms such as Facebook rather than broadcast directly.[190]

This indirect dissemination exploits structural weaknesses in Albana's media ecosystem, including high levels of self-censorship, financial fragility among media outlets, and concentrated ownership structures dominated by a limited number of family-owned companies.[191] Such conditions lower the threshold for foreign narratives to enter the domestic information environment.

Russian-aligned narratives typically aim to undermine public confidence in Albania's Euro-Atlantic trajectory. Disinformation campaigns frequently portray NATO membership and EU accession as threats to Albanian sovereignty and economic development.[192] Both institutions are framed as "expansionist" and dominated by the United States, with membership depicted as reducing Albania to a subordinate or "vassal" state.[193] More recently, messaging has targeted Albania's electoral processes and institutions, casting doubt on their independence and legitimacy.[194]

Countermeasures and impact

Albania's response to FIMI has developed gradually and unevenly. A central structural challenge concerns the absence of a clear legal definition of foreign information manipulation and interference. While Albania's legislative framework addresses related domains, such

189 *The Vulnerability of Albanian Politics to Foreign Interference*, 5.

190 'Si Depërtojnë Në Median Shqiptare Narrativat Kundër NATO-s Dhe BE-Së?', Analiza, *Reporter.Al*, 15 October 2024, https://www.reporter.al/2024/10/15/si-depertojne-ne-median-shqiptare-narrativat-kunder-nato-s-dhe-be-se/; Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference*, 25–26.

191 Blerjana Bino et al., *Media Freedom in Albania* (Center Science and Innovation for Development, 2024), 14, https://scidevcenter.org/wp-content/uploads/2024/07/ENG_Media-Freedom-Shadow-Report_ALBANIA.pdf; 'Media Concentration', Media Ownership Monitor, accessed 21 November 2025, https://albania.mom-gmr.org/en/findings/media-concentration/.

192 Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference*, 25.

193 Emiljano Kaziaj and Viola Keta, *Shperndarja e Narrativave-Dezinformuese Kunder Natos Dhe Be* (BIRN Albania), 2024), 102, https://www.reporter.al/wp-content/uploads/2024/10/Shperndarja-e-narrativave-dezinformuese-kunder-natos-dhe-be-3_compressed.pdf.

194 'Berisha: Reforma Soros Në Drejtësi i Ka Prerë Kolonën Vertebrale Shtetit Shqiptar', A2CNN, 25 August 2022, https://a2news.com/berisha-reforma-soros-ne-drejtesi-i-ka-prere-kolonen-vertebrale-shtetit-shqiptar.

as data protection, cybersecurity standards, and critical infrastructure protection, these measures tend to focus narrowly on technical cyber threats rather than broader information operations.[195] Both the National Cybersecurity Strategy 2020-2025 and the Cyber Defence Strategy 2024-2028 acknowledge the risks posed by cyber and hybrid threats. However, although the latter recognises foreign information manipulation as a concern, it lacks a secured budget and does not outline concrete countermeasures.[196]

At the parliamentary level, Albania has sought to address certain aspects of FIMI, particularly regarding electoral interference. In April 2024, the Assembly of Albania (i.e. the Albanian parliament) voted in favour of the establishment of a special parliamentary commission on countering disinformation and foreign interference in the public sphere. This commission aims to improve coordination and raise the visibility of FIMI as a national security issue.[197] However, its legitimacy has been questioned, as only the ruling Socialist Party supported its creation, and the opposition did not participate. Despite this limitation, the commission has encouraged engagement with civil society, academia, and research institutes.[198]

In July 2025, parliamentarians adopted a national anti-disinformation strategy, providing a framework for legal reform, procedural safeguards, and interagency coordination.[199] Subsequently, in autumn 2025, the Assembly established a bipartisan special committee on electoral reform aimed at strengthening safeguards against foreign interference in electoral processes.[200]

Institutional responsibility for countering FIMI remains fragmented across several bodies, including the Ministries of Interior, Foreign Affairs, Defence, and the State Information Service.[201] This fragmentation has hampered coordination but has recently been addressed through the National Cyber Security Authority. This entity serves as a central coordinating body and acts as Albania's liaison to the European Centre of Excellence for Countering Hybrid Threats.[202] Albania successfully became the official 36th member of this centre in 2024.[203] International cooperation has also intensified. Albania has strengthened partnerships with the EU, NATO and particularly the United States, which has provided cybersecurity expertise and capacity-building support. Under the EU's rapid response mechanism, activated in response

195 Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference*, 10.

196 Blerjana Bino, *Analytical Report: Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference* (SCiDEV, 2024), 9–10, https://scidevcenter.org/wp-content/uploads/2024/10/FIMI-Analytical-Report-Albania_SCiDEV.pdf.

197 'Parliament Votes Establishment of Commission against Foreign Influence, Disinformation', Albanian Daily News, 4 November 2024, https://albaniandailynews.com/news/parliament-votes-establishment-of-commission-against-foreign-influence-disinformation.

198 Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference* (SCiDEV, 2024), 12.

199 Fjori Sinoruka, 'Albanian MPs Adopt National Anti-Disinformation Strategy Amidst Opposition', *Balkan Insight*, 4 July 2025, https://balkaninsight.com/2025/07/04/albanian-mps-adopt-national-anti-disinformation-strategy-amidst-opposition/.

200 'Special Parliamentary Committee on Electoral Reform to Be Established in September – Balla: Time to Depoliticize Electoral Commissions', *RTSH*, 26 June 2025, https://rtsh.al/rti/en/special-parliamentary-committee-on-electoral-reform-to-be-established-in-september-balla-time-to-depoliticize-electoral-commissions/.

201 Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference*, 13–14.

202 'Home', AKSK, accessed 31 October 2025, https://aksk.gov.al/en/home-2/.

203 Orkidea Xhaferaj, 'SCiDEV Welcomes Albania's Membership in the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)', *Scidev*, n.d., accessed 21 January 2026, https://scidevcenter.org/2024/09/14/scidev-welcomes-albanias-membership-in-the-european-centre-of-excellence-for-countering-hybrid-threats-hybrid-coe/.

to heightened cyber risks following Russia's invasion of Ukraine, Albania has invested in cyber-security infrastructure and training.[204]

At the societal level, growing attention is being paid to media literacy and civic awareness initiatives, particularly targeting rural populations, older citizens, and individuals with limited digital literacy.[205] Civil society engagement is increasingly recognised as essential. Fakotje.al, Albania's first independent fact-checking outlet established in 2018, has emerged as a key actor. By verifying statements and promises from public officials and analysing socio-economic claims, Faktoje contributes to transparency and public awareness.[206] In doing so, Faktoje reinforces transparency and accountability, and helps citizens distinguish between verified reporting and disinformation. Albania has recently also started investing more into public-private partnerships to counter online threats, for example by collaborating with private cybersecurity companies and using specialised tools to analyse online threats more efficiently.[207]

Concentrated media ownership, financial instability and limited professional protections within independent journalism, and low institutional trust constrain the effectiveness of countermeasures.

Despite these developments, structural weaknesses persist. Concentrated media ownership, financial instability and limited professional protections within independent journalism, and low institutional trust constrain the effectiveness of countermeasures.[208] Independent journalism is impeded, for instance, through criminal defamation provisions punishable by fines. In other countries, such provisions have been used to stifle investigative or critical reporting. At the same time, Albania does not grant journalists special protection against violence while exercising their profession.[209] Furthermore, journalists have limited opportunities to organise themselves and to promote the interests of independent journalism.[210]

Apart from these structural challenges, institutional frameworks remain only partially operational. The Cybersecurity Operational Centre, established within Albania's Armed Forces in 2024, has yet to become fully operational, and cyber security action plans require further harmonisation with EU standards.[211] Although Albania's ranking in the National Cyber Security Index has improved, placing 15th out of 112 countries, vulnerabilities remain. While overt propaganda may have limited traction, subtler forms of narrative manipulation and indirect influence are likely to persist.[212]

---

204 Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference*, 17–18; 'Western Balkans: High Representative Borrell Announces New Support to Albania, Montenegro and North Macedonia to Counter Cybersecurity Threats | EEAS', accessed 21 November 2025, https://www.eeas.europa.eu/eeas/western-balkans-high-representative-borrell-announces-new-support-albania-montenegro-and-north_en?s=230.

205 Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference*, 41–42; Lazarino Pjetri, 'Mungesa e Aftësive Digjitale Mban Peng Revolucionin e Shërbimeve Qeveritare', Reporter.Al, 22 December 2023, https://www.reporter.al/2023/12/22/mungesa-e-aftesive-digjitale-mban-peng-revolucionin-e-sherbimeve-qeveritare/.

206 'Njihuni Me Ne', *Faktoje.Al*, n.d., accessed 19 January 2026, https://faktoje.al/kush-jemi/.

207 'Threats, Trends and Impact of Ransomware Attacks in Albania', paper presented at International workshop on conducting criminal investigations of ransomware attacks, The Hague, 3 November 2022, https://rm.coe.int/session-i-edmond-koloshi-albania/1680a8cbe4; Blerjana Bino, *Resilience and Gaps in Albania's Responses to Foreign Information Manipulation and Interference*, 39.

208 Gjergj Erebara, 'Besimi Tek Institucionet Politike Pëson Sërish Rënie Në Shqipëri', Lajme, *Reporter.Al*, 21 May 2024, https://www.reporter.al/2024/05/21/besimi-tek-institucionet-politike-peson-serish-renie-ne-shqiperi/.

209 'Commission Staff Working Document: Albania 2024 Report', European Commission, 20 October 2024, 37, https://enlargement.ec.europa.eu/document/download/a8eec3f9-b2ec-4cb1-8748-9058854dbc68_en?filename=Albania%20Report%202024.pdf.

210 'Commission Staff Working Document: Albania 2024 Report', 38.

211 'Commission Staff Working Document: Albania 2024 Report', 71.

212 'Cybersecurity, AKSK: Albania Has Marked an Extraordinary Achievement, 15th in the World - Telegraph', Telegrafi, 25 September 2025, https://telegrafi.com/en/aksk-cyber-security-albania-has-marked-an-extraordinary-achievement-of-15th-in-the-world/.

2.3.2. **North Macedonia**

Historical context and contemporary geopolitics

North Macedonia occupies a unique position in the Western Balkans. Its political trajectory has long been tied to international factors, including its 2020 accession to NATO, ongoing negotiations about EU membership, and historically sensitive issues surrounding identity and ethnic divisions. These identity dynamics often transcend national borders and involve diasporic communities, rendering the country particularly susceptible to influence operations that exploit ethnic identity and related political sensitivities.[213]

This complex interplay of ethnic plurality, identity politics, and historically fragile media freedom has created a number of structural vulnerabilities. These are compounded by a fragmented and underfunded media landscape, low levels of institutional trust, and persistent social division that can be exploited by adversarial actors.

Targets and tactics

Foreign influence operations, especially those linked to Russia, play a major role in North Macedonia's hybrid threat landscape. Rather than operating in isolation, Russian efforts operate through a complex network of channels and proxies, combining state-sponsored media, regional spill-over, and collaboration with domestic political actors.

A key tactic involves the dissemination of pro-Russian narratives through state-affiliated media, content sharing, and social medial presence. For instance, content originating from Russian state media or pro-Russian Balkan outlets is frequently translated into Macedonian, used as sources by domestic media outlets, or republished by North Macedonian TV channels, creating a pipeline through which Kremlin-aligned messaging enters the Macedonian information space.[214] This 'recycling' of foreign content by domestic sources can partly be attributed to Macedonia's fragmented and underfunded media landscape. Many small outlets lack the resources for original reporting.[215] Such dependence significantly lowers the threshold for foreign influence to infiltrate the domestic information space. Moreover, the Russian embassy in Skopje maintains active social media accounts, serving as a direct conduit for pro-Russian narratives targeting Macedonian audiences.[216]

These Russian-led information operations also rely heavily on cooperation with domestic proxies. Local pro-Russian politicians, media outlets, or political parties sometimes act as amplifiers of Kremlin narratives. For instance, the far left Levica party has frequently echoed Kremlin narratives and is a vocal critic of providing aid to Ukraine.[217] This synergy between

---

213 Samuel Cranny-Evans, 'Hybrid Theory: The Development of Armoured Alternative Propulsion', Global Defense Technology, 28–29, https://defence.nridigital.com/global_defence_technology_feb24/hybrid_propulsion_engines_armoured_vehicles#nav-area.

214 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis* (Metamorphosis Foundation for Internet and Society, 2024), https://metamorphosis.org.mk/en/izdanija_arhiva/stability-under-threat-fimi-in-north-macedonia/.; https://euronews.al/en/study-reveals-russian-influence-through-propaganda-in-north-macedonia/

215 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*.

216 Goran Lefkov, 'The Russian Embassy in Skopje – Main Diplomatic Internet Spammer in North Macedonia', *Truthmeter*, 17 March 2023, https://truthmeter.mk/the-russian-embassy-in-skopje-main-diplomatic-internet-spammer-in-north-macedonia/.

217 Igor Petrovski et al., 'From Levica through Rodina to GROM and MAAK: Who Are Moscow's Megaphones in the Country', *Truthmeter*, 8 April 2024, https://truthmeter.mk/from-levica-through-rodina-to-grom-and-maak-who-are-moscows-megaphones-in-the-country/.

external and internal actors allows information operations to acquire a layer of 'local relevance', being presented as domestic opinions or critique rather than foreign propaganda. This makes it harder for citizens to recognise foreign interference.[218]

Countermeasures and impact

Until recently, North Macedonia's institutional response to external information operations was limited. For many years, the dominant political environment and state control over the media left little room for independent and transparent media oversight.[219] Information operations only became a topic of more open discussion following the change in government lead by the Social Democratic Union of Macedonia in 2017.[220]

In 2021, the Macedonian government developed a Strategy for Building Resilience and Tackling Hybrid Threats, which provided a concrete follow-up to the 2019 Plan for Resolute Action against the Spreading of Disinformation.[221] However, both initiatives have been criticised as being largely symbolic. [222] The adoption of the 2021-2025 strategy was delayed, and by the time of finalisation right before the elections, major political parties had already distanced themselves from it.[223] Notably, there is still no binding legal framework explicitly targeting disinformation or foreign interference.[224] Proposed laws and action groups have either stalled or been abandoned after criticism from independent media organisations or civil society.

Relatively more successful were the "Recommendations for Joint Action for Building Societal Resilience Towards Malign Influences of Disinformation", a civil society initiative that proposed a list of recommendations for countering FIMI in cooperation with dedicated research institutes and activist networks.[225] These recommendations now form the basis of North Macedonia's national framework to counter disinformation.[226]

When it comes to outreach, most officials do not raise the issue of disinformation and foreign interference in public or restrict themselves to broad statements about supporting information integrity.[227] Consequently, there are few official plans or initiatives for countering disinformation campaigns that are being implemented. While a draft law on fighting disinformation was presented in 2019, based on recommendations by the European Commission, the plan was not implemented. Another initiative, a proposed Action group to fight disinformation, comprised of various ministry-level representatives and the office of the prime minister, was

218 https://bisi.org.uk/reports/domestic-actors-fuel-russian-disinformation-in-the-western-balkans

219 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 4.

220 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 4.

221 'The National Security Strategy of the Republic of North Macedonia 2024-2029', n.d., 18.

222 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 5.

223 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 6.

224 Metodi Hadzi-Janev and Marijan Stoilkovsik, *Foreign Information Manipulation and Interference in the Republic of North Macedonia* (Skopje, 2025), 20, https://iks.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf.

225 'Recommendations For Joint Action For Building Societal Resilience Towards Malign Influences Of Disinformation', Metamorphosis, 27 June 2023, https://metamorphosis.org.mk/en/izdanija_arhiva/recommendations-for-joint-action-for-building-societal-resilience-towards-malign-influences-of-disinformation/.

226 'Commission Sstaff Working Document: North Macedonia 2024 Report', European Commission, 30 October 2024, 90, https://enlargement.ec.europa.eu/document/download/5f0c9185-ce46-46fc-bf44-82318ab47e88_en?filename=North%20Macedonia%20Report%202024.pdf.

227 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 14.

announced without prior stakeholder consultations. This faced heavy criticism by several respected NGOs in North Macedonia and was never implemented as a result.[228]

As such, much of the burden of countering information operations has fallen on grassroots initiatives and civil society actors. For instance, the Metamorphosis Foundation, supported by foreign donors like the Netherlands, debunks false narratives, maps disinformation flows, and serves as a hub for other anti-disinformation networks.[229] These efforts are supported by Truthmeter.mk, North Macedonia's only internationally certified fact-checking organisation.[230] YouThink, funded by USAID, provides another initiative, aiming to integrate media literacy into formal education curricula.[231]

Much of the burden of countering information operations has fallen on grassroots initiatives and civil society actors.

In addition, the launch of regional initiatives like the Western Balkans Quad in March 2023 holds promise. Through this initiative, North Macedonia alongside Albania, Kosovo, and Montenegro committed to fully aligning with the EU's Common Foreign and Security Policy, suggesting growing political will to resist external manipulation and deepen cooperation with Western partners.[232] North Macedonia aligned with several EU declarations or restrictive measures regarding cyber-attacks in 2023 and 2024 and strengthened its institutional collaboration with its Western allies. For instance, North Macedonia joined the European Centre of Excellence for Countering Hybrid Threats in October 2023 that is based in Helsinki and has started to implement a strategy to increase resilience against hybrid threats. Likewise, North Macedonia established a council under the Prime Minister to coordinate activities related to hybrid threats with NATO.[233]

Nevertheless, watchdogs report that FIMI continues to negatively impact North Macedonian society, shaping public opinion, eroding trust in democratic institutions, and reinforcing societal divisions. The continued absence of coordinated well-resourced institutional mechanisms therefore remains a serious structural vulnerability.[234]

2.3.3. **Bosnia Herzegovina**

Historical context and contemporary geopolitics

Bosnia and Herzegovina (BiH) exemplifies many of the structural vulnerabilities characteristic of the Western Balkans: a fragmented political architecture, entrenched ethnic divisions, and a legacy of conflict that continues to shape social and political dynamics. These factors render BiH particularly susceptible to external influence, both through economic leverage, but

228 Nenad Georgievski, *The Government Has an Action Plan to Fight Fake News and Disinformation*, 25 July 2019, https://meta.mk/en/the-government-has-an-action-plan-to-fight-fake-news-and-disinformation/; Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 14.

229 Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 15.

230 Vishinska, *Geopolitical Perspective Of Disinformation Flows In The Western Balkans - Metamorphosis* (Metamorphosis Foundation for Internet and Society, 2023), 62–63, https://metamorphosis.org.mk/en/izdanija_arhiva/geopolitical-perspective-of-disinformation-flows-in-the-western-balkans/.

231 'YouThink: Media Literacy in North Macedonia', USAID, n.d., https://www.irex.org/sites/default/files/YouThink%20Media%20Literacy%20in%20N.%20Macedonia%20Fact%20Sheet%202022.pdf.

232 'Four Western Balkan Countries Launched "100% Alignment with CFSP" Platform', *European Western Balkans*, 29 March 2023, https://europeanwesternbalkans.com/2023/03/29/four-western-balkan-countries-launched-100-alignment-with-cfsp-platform/.

233 'Commission Staff Working Document: North Macedonia 2024 Report', 90.

234 'Building a Resilient and Trusted Information Ecosystem Requires Collective Action - Metamorphosis', *Metamorphosis - Foundation for Internet and Society*, 25 June 2025, https://metamorphosis.org.mk/en/aktivnosti_arhiva/building-a-resilient-and-trusted-information-ecosystem-requires-collective-action/.

especially through information manipulation.[235] Although Russia's direct economic footprint in BiH has historically been limited compared to Western of Chinese investors, Moscow nevertheless retains significant soft-power influence. This influence operates through cultural, historical, religious, and political-ideological ties, particularly among Bosnian Serb communities and within Republika Srpska, one of the country's two entities.[236] In this context, information manipulation constitutes a primary channel through which external actors seek to shape domestic dynamics.

Targets and tactics

While Bosnia and Herzegovina may not rank among Russia's current top priorities in the region, especially compared to Serbia, its potential destabilisation can cause ripple effects across the region. As seen in neighbouring countries, Russia often acts as a spoiler to stabilisation efforts, particularly those associated with European integration or reforms in favour of multi-ethnic governance reforms.

Information operations are central to this approach. Despite Bosnia aligning with EU sanctions that prohibit the broadcasting of Russian state-sponsored channels, Russian-aligned narratives continue to circulate through indirect channels.[237] Local and regional outlets often republish content originating from Russian state media or Serbian media with close ties to the Kremlin. For instance, media outlets in Republika Srpska are known to cooperate with Russian news agencies, and broadcast Russian-aligned narratives. Much of the propagation of Russian narratives flows through offices of RT Balkan and Sputnik in Serbia, which hosts the only regional office in the region, and whose reporting spills over into neighbouring countries.[238] Political leaders such as Milorad Dodik have used such local media outlets to spread secessionist rhetoric and challenge state-level institutions.[239] In parallel, online platforms and social media serve as conduits for disinformation and hate speech, further expanding the reach of polarising narratives.[240]

The narratives pushed typically blend ethnic nationalism, historical grievances around the Srebrenica genocide, anti-Western sentiments, distrust toward state institutions, and conspiracy theories on global issues such as climate change. Temporary upticks in such information campaigns are often observed around election periods.[241] Anti-Western narratives frequently mirror common Russian propaganda and disinformation framing, including statements on alleged Ukrainian plans to deploy nuclear weapons against Russia,

---

235 Chris J. Dolan, 'Hybrid Warfare in the Western Balkans: How Structural Vulnerability Attracts Maligned Powers and Hostile Influence', *SEEU Review* 17, no. 1 (2022): 10, https://reference-global.com/2/v2/download/pdf/10.2478/seeur-2022-0018.

236 Branislav Stanicek and Anna Caprile, 'Russia and the Western Balkans: Geopolitical Confrontation, Economic Influence and Political Interference', European Parliamentary Research Service, 4 January 2023, 3, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/747096/EPRS_BRI%282023%29747096_EN.pdf.

237 'What Do European Commission 2024 Reports Say on Tackling Disinformation in Western Balkans?', In-Depth Stories, *Antidisinfo*, 3 November 2024, https://antidisinfo.net/what-do-european-commission-annual-reports-note-on-tackling-disinformation-in-western-balkans/.

238 Zweers et al., *Little Substance, Considerable Impact*, 39.

239 Thomas Brey, *Russian Media in the Balkans* (Friedrich Naumann Foundation, 2022), 20, https://www.freiheit.org/germany/russian-media-balkans.

240 *Antidisinfo*, 'What Do European Commission 2024 Reports Say on Tackling Disinformation in Western Balkans?'

241 Marija Cosic and Emir Zulejhic, *Disinformation Report: Bosnia and Herzegovina in 2024 - SEE Check* (2025), https://seecheck.org/index.php/2025/05/06/disinformation-report-bosnia-and-herzegovina-in-2024/.

and how President Putin should be considered a "liberator" in contrast to the West and its sinister motives.[242]

Countermeasures and impact

Bosnia and Herzegovina has struggled to build a coherent and effective national framework to counter hybrid threats, including FIMI. There is no overarching national strategy addressing foreign information manipulation.[243] Instead, regulatory responsibility lies with agencies such as the Communications Regulatory Agency, which enforces the Code on Audiovisual Media Services and Radio Services. Article 7, for instance, prohibits broadcasters from transmitting misleading content without factual validation and allows for financial penalties in cases of violation.[244]

In practice, enforcement has been weak. Fines are perceived as too low to be an effective deterrent.[245] Media outlets often continue to broadcast content that echoes external propaganda, and regulatory oversight lacks the resources or political will to act effectively. As a result, much of the burden for exposing and countering disinformation falls on civil society.

Apart from local fact checkers, Bosnia and Herzegovina has also benefited from international capacity-building projects.

One prominent example is the organisation Raskrinkavanje ("Deconstruction"), founded in 2017 by the citizen association Zašto ne ("Why not"). The organisation is part of a regional network of fact checking organisations that monitor media, debunk false claims, and raise public awareness.[246] In addition to Zašto ne, the Balkan Investigative Reporting Network (BIRN) publishes reports and analysis on foreign disinformation operations and implementing capacity-building initiatives to strengthen journalistic standards, raise public awareness, and train journalists in factchecking.[247]

Apart from local fact checkers, Bosnia and Herzegovina has also benefited from international capacity-building projects. The Social Media 4 Peace project (2021-2023) convened representatives of social media companies and national authorities to strengthen the resilience of civil society against online threats, especially hate speech and incitements of violence.[248] The project concluded with a report outlining the magnitude of online threats and capability gaps, as well as several recommendations to national governments and social media

242 Raskrinkavanje.ba (BiH), *Disinformation Report: Bosnia and Herzegovina in 2023 - SEE Check* (2024), https://seecheck.org/index.php/2024/09/12/disinformation-report-bosnia-and-herzegovina-in-2023/.

243 Directorate-General for Neighbourhood and Enlargement Negotiations, *Bosnia and Herzegovina 2024 Report* (European Commission, 2024), https://enlargement.ec.europa.eu/bosnia-and-herzegovina-report-2024_en; Cosic and Zulejhic, *Disinformation Report*.

244 Cosic and Zulejhic, *Disinformation Report*.

245 Tijana Cvjetićanin et al., *Disinformation in the Online Sphere. The Case of BiH* (Citizens' Association 'Why Not', 2019), 69–75, https://web.archive.org/web/20240122001905/https://zastone.ba/app/uploads/2019/05/Disinformation_in_the_online_sphere_The_case_of_BiH_ENG.pdf.

246 S. E. E. Check, 'About Us - SEE Check', 7 November 2021, https://seecheck.org/index.php/about/.

247 Aleksandra Vrbica, 'Media Integrity and Disinformation Watch - MIDWatch', Balkan Investigative Reporting Network, accessed 19 January 2026, https://birn.eu.com/programmes/media-integrity-and-disinformation-watch-midwatch/.

248 'SocialMedia4Peace: Pilot Bosnia and Herzegovina Counters Online', 20 April 2023, https://www.unesco.org/en/articles/socialmedia4peace-pilot-bosnia-and-herzegovina-counters-online-disinformation-and-hate-speech.

companies. For instance, one of the recommendations called for a transparent content moderation process and the provision of restorative mechanisms for victims of incitement to hatred. [249]

Subsequent initiatives, such as "Building Trust in Media in South-East Europe", have focused on strengthening Bosnia's media environment, such as strengthening journalistic ethics, accountability, and gender equality, while promoting media and information literacy, particularly among youth.[250] Similarly, the "Combatting Disinformation in the Western Balkans" project (2022-2024) brought together participants and different societal stakeholders to foster an informed dialogue about various aspects of FIMI. The project concluded with recommendations for improved government-civil society cooperation, greater transparency in media ownership, and the establishment of local cybercrime units. [251] Nevertheless, the overall impact of such initiatives remains limited. The safety of journalists continues to be affected by the legacy of wartime violence and a climate of impunity.[252] Although severe physical attacks are now rare, threats and harassment, particularly from high-level political figures remain common and journalists frequently face intimidation and online abuse.[253]

While Bosnia's media regulation framework formally aligns with EU standards, implementation varies considerably. The country's media landscape is highly fragmented, comprising dozens of television channels, over a hundred radio stations, and hundreds of news websites with often opaque ownership structures.[254] Consequently, blogs and lesser-known platforms frequently serve as vehicles for disinformation. Economic precarity further exacerbates vulnerability: many outlets depend on local municipal funding or foreign grants, which may discourage critical reporting on politically sensitive issues.[255]

Recent legal developments have raised additional concerns. In Republika Srpska, defamation has been re-criminalised, with fines of up to €3,000 and potential imprisonment for non-payment. Such provisions risk enabling strategic lawsuits against public participation (SLAPPs) and may deter investigative journalism. In response, initiatives such as the Council of Europe's "Protecting Freedom of Expression and of the Media in Bosnia and Herzegovina

249 *Social Media 4 Peace. Local Lessons for Global Practices* (UNESCO, 2023), 58, https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000386777&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_cd019da9-3cf9-4be3-b350-97c09dd1669e%3F_%3D386777eng.pdf&updateUrl=updateUrl9362&ark=/ark:/48223/pf0000386777/PDF/386777eng.pdf.multi&fullScreen=true&locale=en#%5B%7B%22num%22%3A230%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2Cnull%2C800%2Cnull%5D.

250 'Building Trust in Media in South-East Europe: Support to Journalism As', accessed 8 December 2025, https://www.unesco.org/en/articles/building-trust-media-south-east-europe-support-journalism-public-good.

251 'CDWB | Combatting Disinformation in the Western Balkans | European Partnership for Democracy', accessed 8 December 2025, https://epd.eu/what-we-do/programmes/cdwb-combatting-disinformation-in-the-western-balkans/.

252 *Bosnia and Herzegovina: Media Freedom in Survival Mode* (Media Freedom Rapid Response (MFRR), 2023), 12, https://www.mfrr.eu/wp-content/uploads/2024/01/bosnia-and-herzegovina-media-freedom-in-survival-mode-1.pdf.

253 *Bosnia and Herzegovina: Media Freedom in Survival Mode*, 11; 'Mapping Media Freedom: Bosnia and Herzegovina: Milorad Dodik Verbally Attacks N1 Journalist Snežana Mitrović (2023-11-17)', Mapping Media Freedom, accessed 8 December 2025, https://www.mapmf.org/alert/30866.

254 *Bosnia and Herzegovina: Media Freedom in Survival Mode*, 16; 'Bosnia-Herzegovina | RSF', 30 September 2024, https://rsf.org/en/country/bosnia-herzegovina.

255 *Bosnia and Herzegovina: Media Freedom in Survival Mode*, 17.

(PROFREX)" project aims to equip judges and civil society actors with tools to address unlawful defamation practices.[256]

Overall, persistent structural vulnerabilities such as media fragmentation, institutional weakness, ethno-religious divisions, and economic fragility continue to create fertile ground for foreign information manipulation. Russia and its proxies are likely to continue exploiting these vulnerabilities as part of broader efforts to destabilise the region, thereby obstructing Bosnia's European integration trajectory.

2.3.4. **Reflections**

In this region in particular Russian FIMI campaigns capitalise on existing polarised narratives and sentiments within society. This naturally complicates efforts countering FIMI because society is more susceptible to fabricated content and governments face more challenges to allocate resources against it. Consequently, much of the fight against FIMI rests on the shoulders of local fact-checking organisations such as "Raskrinkavanje", in Bosnia and Herzegovina or North Macedonia.[257]

[256] 'Journalists, Lawyers and Activists Join Forces to Fight SLAPP in Bosnia and Herzegovina - Freedom of Expression - Www.Coe.Int', Council of Europe, *Freedom of Expression*, n.d., accessed 19 January 2026, https://www.coe.int/en/web/freedom-expression/-/journalists-lawyers-and-activists-join-forces-to-fight-slapp-in-bosnia-and-herzegovina.

[257] Matej Trojachanec and Goran Rizaov, *Stability Under Threat – FIMI in North Macedonia - Metamorphosis*, 14.

3. Lessons Learned and the Way Forward

Responses to FIMI are far from uniform, despite adversarial narratives frequently originating from common sources. Some states have developed highly coordinated, whole-of-society approaches grounded in strategic communication, media literacy, and civil society mobilisation. Meanwhile, others still grapple with fragmented institutions, weak regulatory capacity, or low trust in governance.

Across the ten cases, countering FIMI emerges as a balancing act.

Across the ten cases, countering FIMI emerges as a balancing act: protecting democratic openness while limiting malign interference, responding rapidly to campaigns while investing in long-term resilience, and coordinating nationally while relying on EU and NATO support. These case studies collectively underline that safeguarding the information space requires not only technical tools and legal frameworks, but also sustained political will, credible institutions, and societal cohesion.

3.1. Insights from the cases: Comparative analysis

A comparative assessment of the ten case studies reveals clear variation in how European states respond to FIMI. While exposure to hostile influence differs across regions, resilience is not determined solely by threat intensity. Rather, responses vary systematically along three analytical pillars: 1) Escalation and coordination levels within government, 2) Societal actors involved in counter-FIMI efforts, and 3) Domains through which countermeasures are delivered. Taken together, these dimensions illustrate distinct response models across the Baltic-Nordic region, Ukraine and its borderland, and the Western Balkans.

3.1.1. Escalation and coordination levels

A first point of comparison concerns the degree to which counter-FIMI efforts are institutionalised within government structures and how consistently they are activated.

High-threat, high-capacity states. Estonia, Lithuania, Finland, and Ukraine exhibit the highest levels of institutionalisation. In these states, FIMI is explicitly recognised as a national security threat and embedded in strategic documents and operational practice. Countering foreign interference is treated as a continuous governmental task rather than an ad hoc reaction to specific incidents. These countries have established permanent monitoring structures, interagency coordination mechanisms, and predefined escalation pathways. Estonia and Lithuania

maintain systematic oversight of their information spaces, supported by intelligence assessments and regulatory authorities capable of taking timely action. Finland operates a coordinated national network under the Prime Minister's Office. Ukraine, operating under wartime conditions, has integrated information defence into national security and military command structures, combining strategic communications, cyber defence, and intelligence capabilities.

Medium-threat, medium-capacity states. Poland and Moldova represent a second tier. Both have established institutional structures and legal tools to address FIMI, but activation patterns are more episodic. Government involvement intensifies during high-risk periods, particularly national elections or geopolitical crises. In Poland, institutional mobilisation often coincides with electoral cycles or EU-level escalations, such as activation of the Rapid Alert System. Moldova similarly increases institutional engagement during major interference campaigns, frequently with support from international partners such as the EU Partnership Mission. Although counter-FIMI institutions exist in both countries, legislative and operational focus tends to centre on electoral integrity, illicit campaign financing, and political advertising transparency rather than comprehensive information defence.

Fragmented or low-capacity response environments. In Romania and much of the Western Balkans, governmental involvement remains comparatively limited or fragmented. Institutional responses are frequently reactive and triggered by major public incidents rather than embedded in continuous monitoring frameworks. Coordination is often dispersed across regulatory authorities, electoral bodies, or individual ministries, with limited central oversight. Comprehensive national strategies or clearly defined escalation structures are often absent. Structural constraints, such as political divisions, limited resources, or weak media regulation, further impede consistent governmental engagement.

3.1.2. Societal actors

A second differentiating factor concerns the extent to which governments can rely on societal actors in countering FIMI.

Whole-of-society models. In Estonia, Lithuania, Finland, and Ukraine, strategies to counter FIMI follow a whole-of-society model. Governmental responsibility is firmly institutionalised, but individual citizens, NGOs, independent media, and private-sector actors play complementary roles. Volunteer cyber units, fact-checking networks, investigative journalists, and media literacy initiatives operate alongside state institutions. In Estonia and Lithuania, for example, citizens contribute professional expertise to national resilience efforts, particularly in IT and cybersecurity.

State-led models with external support. In Moldova and Albania, counter-FIMI efforts are more strongly state-driven, often supported by international partners. Capacity-building initiatives focus on technical skills, cybersecurity alignment with EU standards, and institutional coordination. While NGOs and fact-checking organisations are active, collaboration between civil society and government is less institutionalised than in the Baltic-Nordic region. In Moldova in particular, internal political divisions may constrain broader citizen mobilisation.

Civil society-dominant environments. In North Macedonia, Bosnia and Herzegovina, and to a certain extent Romania, much of the operational burden of countering disinformation rests on civil society organisations. Fact-checking initiatives and investigative journalism networks play a primary corrective role. Governments in these contexts often lack either the political

will, institutional capacity, or public trust necessary to assume a leading role. As a result, resilience is decentralised, and corrective efforts may not be systematically integrated into national policy frameworks.

3.1.3. Target audiences

Differences also emerge regarding the intended audiences of counter-FIMI strategies. In Baltic and Nordic states, countermeasures are typically framed as national security priorities and directed toward the entire population. Media literacy initiatives, strategic communication, and crisis messaging aim at broad societal resilience. In contract, in several Western Balkan countries, corrective messaging is often targeted at specific communities already engaged in media literacy networks. Limited institutional capacity and internal political divisions reduce the scope of nationwide campaigns.

Limited institutional capacity and internal political divisions reduce the scope of nationwide campaigns.

3.1.4. Domains of countermeasures

A final point of comparison concerns the domains through which counter-FIMI measures are delivered. Highly resilient states operate across multiple domains simultaneously: regulatory and legal instruments (incl. Sanctions, media suspensions, and electoral transparency laws), strategic communication (incl. Proactive narrative framing), societal resilience measures (notably media literacy and civic education), and operational monitoring and rapid response mechanisms.

Ukraine represents the most advanced case in narrative mobilisation, actively shaping counter-narratives in conjunction with military and diplomatic strategy. By contrast, states relying predominantly on single-domain approaches, particularly where countermeasures consist primarily of factchecking without broader regulatory or strategic support, remain more vulnerable to sustained or adaptive FIMI campaigns.

3.1.5. Conclusions

The comparative analysis reveals several patterns across the case studies. First, perceived threat intensity strongly correlates with the degree of institutionalisation. States that interpret FIMI as a systemic national security threat, particularly Estonia, Lithuania, Finland, and Ukraine, have embedded countermeasures within permanent coordination mechanisms, strategic documents, and daily administrative practice. In these contexts, countering FIMI is not treated as a peripheral media issue but as an integral component of national defence and democratic protection.

Second, resilience appears closely linked to the configuration of actors involved. Countries that have developed whole-of-society approaches benefit from layered protection mechanisms in which government agencies, civil society organisations, independent media, private-sector actors, and engaged citizens operate in complementary roles. This integration reduces reliance on any single institution and enhances the ability to respond rapidly and adaptively. By contrast, where responsibility rests predominantly on either under-resourced state institutions or isolated civil society initiatives, responses tend to remain reactive and fragmented.

Third, the breadth of policy domains employed significantly shapes outcomes. The most resilient states combine regulatory and legal tools, operational monitoring capabilities, strategic communication, and long-term societal resilience measures such as media literacy education. This multi-domain policy blend increases both deterrence and adaptability. Where countermeasures focus narrowly on fact-checking or electoral safeguards without accompanying strategic communication or institutional coordination, vulnerability to sustained or evolving campaigns remains higher.

Finally, structural domestic factors consistently mediate effectiveness. Media fragmentation, opaque ownership structures, political polarisation, limited public trust, and resource constraints weaken the implementation of counter-FIMI strategies regardless of formal commitments. Conversely, high levels of institutional trust, professionalised media environments, and sustained civic education strengthen resilience even under sustained external pressure. Taken together, the evidence suggests that effective resistance to FIMI is less a product of isolated interventions than of broader democratic robustness and institutional coherence.

Effective resistance to FIMI is less a product of isolated interventions than of broader democratic robustness and institutional coherence.

3.2. Lessons learned across the Regions

Across the Baltic-Nordic states, Ukraine's border region, and the Western Balkans, the case studies demonstrate that FIMI constitutes a dynamic and evolving security challenge. While the geopolitical contexts and institutional landscapes differ, common patterns emerge in how states experience, prioritise, and respond to FIMI. These lessons illuminate both enduring vulnerabilities and promising pathways for building resilience.

3.2.1. Whole-of-society approaches underpin effective responses

One of the clearest lessons across the ten cases is that whole-of-society strategies are essential to effectively countering FIMI. Countries that have integrated governmental leadership with active civil society participation, empowered independent media, and sustained investments in media literacy show stronger resilience. Estonia, Finland, and Lithuania exemplify this multi-actor approach: institutional bodies coordinate strategically with non-governmental organisations, fact-checking networks, volunteer cyber units, and educational programmes to create reinforcing layers of defence. Conversely, where state action is isolated from societal actors, as in parts of the Western Balkans, responses tend to be more reactive and less effective.

Institutional coordination structures that bring together ministries, regulatory bodies, and civil society actors are crucial for synchronised detection and response. In Estonia, for example, cross-sectoral committees meet regularly to assess threats and coordinate messaging across ministries. In Poland, multi-institutional bodies review FIMI incidents and evaluate legal safeguards. In Moldova, EU-supported missions have helped bolster inter-agency collaboration. These arrangements allow for strategic rather than ad hoc reactions to influence operations and help reduce fragmentation in national responses.

3.2.2. Strategic communication and rapid response mechanisms matter

The capacity to detect and respond swiftly to influence operations constitutes a second key lesson. Rapid response and crisis management mechanisms (such as Estonia's strategic communication frameworks, Lithuania's National Crisis Management Centre, and Poland's early warning systems at National Research and Academic Network) enable states to anticipate and counter manipulative campaigns in real time. These systems facilitate fast debunking of false narratives, rapid engagement with platforms and regulators, and coordinated messaging across government and society. The European Union's Rapid Alert System and FIMI Information Sharing and Analysis Centre further augment these capacities by ensuring early warning and joint response mechanisms among member states, particularly around elections and periods of heightened political sensitivity.

In contrast, states without strong rapid response mechanisms often struggle to contain the spread of misleading narratives before they entrench. In North Macedonia and Bosnia and Herzegovina, for example, the absence of well-resourced institutional response units has meant that much of the burden of alerting the public about disinformation has fallen to grassroots organisations, with limited impact on the broader information environment.

Legal frameworks must be backed by clearly defined mandates, sufficient resources, and enforcement mechanisms.

3.2.3. Legal and regulatory frameworks require enforcement capacity

Legal instruments and regulatory frameworks form an important basis for counter-FIMI efforts, yet their effectiveness depends on implementation capacity and the broader institutional environment. EU policies such as the DSA, transparency requirements for political advertising, and the EU Code of Practice on Disinformation create a normative baseline for member states to regulate platform accountability and address harmful content. These frameworks aim to increase transparency, reduce monetisation of disinformation, and enhance oversight of online ecosystems.

Nevertheless, case studies reveal that the mere presence of legal instruments does not guarantee impact. Poland's application of provisions on political advertising transparency and Romania's incorporation of the Code of Practice into the DSA illustrate efforts to use hard law tools, but enforcement remains uneven. In Bosnia and Herzegovina, regulatory fines under the Communications Regulatory Agency are perceived as insufficient deterrents, and implementation capacity is limited by political constraints and resource shortages. Similarly, Albania's cybersecurity and hybrid threat strategies acknowledge information manipulation as a risk but lack detailed operational plans and dedicated budgets.

These experiences suggest that legal frameworks must be backed by clearly defined mandates, sufficient resources, and enforcement mechanisms that respect fundamental rights while deterring harmful behaviour. Ambiguities in legal definitions, such as what constitutes foreign interference and how offences can be reliably attributed, undermine prosecutorial capacity, as seen in several Eastern European cases.

3.2.4. Media literacy and public trust are key to societal resilience

High levels of media literacy and institutional trust significantly mitigate the impact of FIMI operations. Estonia's mandatory media literacy curriculum and Finland's emphasis on education and public awareness have contributed to an informed populace capable of critically evaluating misleading narratives. Estonia's performance in European media literacy indices and Finland's long-standing integration of critical thinking in education underscore how investment in citizen capacities reduces susceptibility to influence operations.

Conversely, low institutional trust and fragmented media landscapes create fertile ground for FIMI actors. In Romania and the Western Balkan countries, public scepticism towards state institutions and political actors undermines confidence in credible sources and amplifies the appeal of alternative, often manipulated narratives. High reliance on social media as a primary news source, coupled with fragmented traditional media landscapes further exposes populations to unverified content.

Strengthening media literacy therefore becomes a strategic imperative.

Strengthening media literacy therefore becomes a strategic imperative. Initiatives such as North Macedonia's YouThink programme and Bosnia's youth-focused media literacy projects illustrate emerging efforts to build long-term resilience, but these require stable institutional support and integration into formal education systems to increase their reach.

3.2.5. Civil society and independent media reinforce resilience

Independent media and civil society organisations play indispensable roles in exposing, analysing, and debunking disinformation. Factchecking networks such as Lithuania's Debunk.org, Finland's Faktabaari, North Macedonia's Truthmeter.mk, and Bosnia's Raskrinkavanje fill critical gaps left by weaker institutional infrastructures. These actors monitor information flows, provide contextual analysis, and bring transparency to narratives that might otherwise be left unchallenged.

Their impact is amplified when supported by national and international partners. The European Digital Media Observatory network, for example, fosters cooperation among fact-checkers and researchers across borders, enhancing collective knowledge and threat mapping. However, civil society organisations often operate with limited resources and face legal, political, and economic pressures that constrain their effectiveness. Strengthening protective environments for independent journalism, such as eliminating criminal defamation provisions that can be misused against critical reporting, remains a priority in several countries.

3.3. Concluding Remarks: Strategic Alignment with EU and NATO

FIMI cuts across many different domains, ranging from online platforms and cyber infrastructure to societal resilience, media ecosystems, national security, and international cooperation. No single actor or level of governance can effectively address all facets of FIMI, calling for a multi-level, multi-actor strategy to ensure comprehensive coverage of the threat space: including prevention, detection, mitigation, and resilience-building. If one line of defence fails, a platform failing to moderate harmful content for instance, others can step in, such as civil society, regulation, communication, or international cooperation.

A multi-level strategy is not simply desirable, but essential.

Involving multiple stakeholders, like governments, civil society, media, supranational institutions or international alliances, contributes to balancing effectiveness with democratic values, such as transparency, pluralism, and freedom of expression. Precisely because FIMI tactics evolve rapidly, a multi-level structure allows for flexibility and adaptability, enabling actors to respond dynamically across technological, regulatory, societal, and diplomatic domains. Stakeholders across countries stressed the importance of coordination, shared situational awareness, societal resilience, and preparedness, going beyond mere reactive measures during crisis situations. As such, a multi-level strategy is not simply desirable, but essential. Without it, responses risk being fragmented, reactive, or ineffective – undermining long-term resilience in the process. Findings from the Strategic Capability Game reinforced these points: when faced with dynamic FIMI challenges, participants consistently struggled in areas where coordination structures were unclear or role boundaries differed across institutions and countries, demonstrating that multi-level alignment is essential in practice.

3.3.1. National responses and the role of the EU and NATO

National responses translate high-level principles into concrete, context-sensitive policies and actions, rendering them indispensable. The national governance level is usually the first line of contact with citizens, media, civil society, and public institutions. Here, governments can establish dedicated coordination bodies or observatories to monitor and document FIMI activities, coordinate fact-checking efforts, issue early warnings, and liaise with supranational networks. Considering a legalistic and rights-conscious tradition, such a body should operate under transparent, democratic, and human-rights compliant mandates. In general, institutional culture shapes these national functions.

National governments can also spearhead media- and digital-literacy initiatives that build long-term resilience. Embedding critical thinking and media literacy in school curricula from primary education onwards and expanding awareness initiatives in adult education help societal resilience endure beyond immediate crises. Nation-wide public-awareness campaigns, especially around election periods or major events, can help citizens better recognise manipulation techniques, understand the role of platforms, and verify information independently. In parallel, supporting a robust domestic media ecosystem, including independent journalism, local media outlets, fact-checking organisations, and public-interest media, helps preserve pluralism and reduces vulnerability to foreign manipulation. Beyond regulatory safeguards like transparency in media ownership and editorial independence, sustainable funding and institutional support for media and civil-society actors working on information integrity is key.

Across regions, media literacy, education, and strengthened civil society ecosystems are consistently identified as foundational long-term countermeasures enhancing capacity, recovery, continuity, upscaling, and response speed.

Crucially, national strategies should incorporate a carefully calibrated approach to attribution, deterrence, and accountability. Where credible evidence exists, public attribution of interference, reputational measures, enforcement of takedown orders or sanctions can be used to impose costs on FIMI perpetrators. This involves trust in government communication as a structural condition for effective national responses. Routine and transparent communication as part of everyday resilience. This is where more Western country case studies experience more constraints by legal, ethical or cultural hesitations to engage directly in shaping public narratives. This suggests that strategic communication requires credible and gradual efforts during non-crisis periods rather than rapid improvisation during emergency situations. Nevertheless, these measures must be evidence-based, transparent, and proportionate. This is especially needed in democratic contexts with strong protections for free speech as indiscriminate censorship or heavy-handed content removal can instead undermine public trust, media pluralism, and democratic legitimacy. Instead, governments should develop targeted actions rooted in evidence and combine enforcement with transparent public communication, appeal mechanisms, and clear criteria. These elements are essential in safeguarding civil liberties.

Routine and transparent communication as part of everyday resilience.

3.3.2. **The European Union**

However, national response should not stand in isolation; they need to draw on supranational frameworks. At the EU-level, several frameworks and instruments already exist to contribute to such a multi-level approach to FIMI countermeasures. The Digital Services Act (DSA), in force since 2022, establishes binding obligations for very large online platforms and other intermediaries to moderate harmful content, improve transparency, and coordinate with authorities. Complementing the DSA, the EU Code of Practice on Disinformation remains an important, voluntary soft-governance mechanism, encouraging platforms to adopt best practices in transparency, moderation, and content management.

Beyond regulation, the EU supports cross-border factchecking and early-warning infrastructure through networks and initiatives that facilitate shared databases, exposure tracking, and coordinated responses. On top of this, the EU plays a role in strategic communication and external action: via foreign policy tools and public information campaigns it can counter foreign influence operations, particularly those targeting the EU's neighbourhood or partner countries.

The EU's approach to FIMI often involves norm-setting and standardisation, establishing common frameworks, terminologies, reporting obligations, and oversight mechanisms that help ensure consistent approaches among member states. As a result, this kind of supranational coordination delivers economies of scale, shared resources, and a harmonised baseline, while preserving room for national policies of individual member states. Put differently, in addition to a regulatory role, the EU also has an enabling role for national responses by strengthening and standardising them while providing economies of scale and shared resources. To support this, there is a need for better feedback loops between national authorities and EU bodies and shared public engagement campaigns on information integrity. Additionally, going beyond guiding regulation such as the DSA, the EU could set a minimum standard of FIMI countermeasures to be in place for (candidate) member states.

3.3.3. **The North Atlantic Treaty Organisation**

While much of FIMI falls under the information security, public communication, and societal resilience domains, and has so far been predominantly addressed by civilian actors, the role of NATO is also relevant, especially in the context of hybrid threats. In this regard, NATO plays a critical supporting and coordinating role, presenting an enabling layer that strengthens collective resilience.

NATO's "Approach to Counter Information Threats", formalised in 2024, recognises that disinformation, foreign interference and manipulative messaging matter to collective security and alliance cohesion.[11] Considering that, in recent years, such threats have grown significantly in scale and sophistication, NATO adopted a common approach among its Allies and partners to address them. The backbone of this approach is its evolving Information Environment Assessment capability, which combines expert analysts, technical tools, and structured processes to map and assess the information environment.

Importantly, its approach is not limited to military actors but involves whole-of-society engagement: NATO cooperates with Allied and partner governments, other international organisations (e.g. OECD, UN, EU, and the G7 Rapid Response Mechanism), academia, media organisations, social-media platforms, civil society, as well as industry stakeholders. Through the creation of such a broad network, NATO contributes to faster identification of malign actors or hostile narratives, share awareness, coordinated responses, and burden-sharing among Allies. This is of particular value for smaller or resource-constrained states.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl