D1.2 – The current state of detection and response to FIMI

Authors

Prof. Robert Kupiecki (University of Warsaw)

Prof. Agnieszka Cianciara (Institute of Political Studies of the Polish Academy of Sciences)

Prof. Agnieszka Legucka (University of Warsaw)

Amb. Tomasz Chłoń (Polish Center for Technology Development)

Dr. Filip Bryjka (Institute of Political Studies of the Polish Academy of Sciences)

Dr. Katarzyna Golik (Institute of Political Studies of the Polish Academy of Sciences)

Dr. Piotr Sosnowski (University of Warsaw)

Sara Nowacka (PhD candidate at Institute of Political Studies of the Polish Academy of Sciences)

Paweł Kasprzyk (Institute of Political Studies of the Polish Academy of Sciences)

Kamila Szymańska (University of Warsaw)

Table of contents

Abbreviations and acronyms

Abbr.	Meaning	Description
ABCDE	Actor, Behaviour, Content, Distribution, Effect	A framework used to analyse FIMI incidents.
AI	Artificial Intelligence	Multiple technologies allowing generation, classification, and execution of human-like creative tasks.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst	The general intelligence and security service for the Netherlands.
CAWI	Computer Assisted Web Interview	A research method.
CCCS	Canadian Centre for Cyber Security	Part of the Communications Security Establishment Canada; offers expert advice, guidance, services, and support for cyber security for Canadians.
CNMF	Cyber National Mission Force	The U.S. military's joint cyber force charged with defending the nation in cyberspace through full-spectrum operations to deter, disrupt, and, if necessary, defeat adversary cyber and malign influence actors. Supports U.S. Cyber Command.
DISARM	Disinformation Analysis and Risk Management	An open-source framework designed for describing and understanding the behavioural parts of FIMI/disinformation. It sets out best practices for fighting disinformation through sharing data and analysis and informs effective action. The framework has been developed in line with global cybersecurity best practices.
DNP	Dutch National Police (*Korps Nationale Politie*)	The police force for the Netherlands.
DSC	Digital Service Coordinators	Officials supported by Resilience Councils, responsible for overseeing compliance of digital services providers with regulations and coordinating enforcement actions against FIMI.
DSA	Digital Services Act	EU legislation that sets rules for digital services and platforms to ensure a safer and more accountable online environment.

EEAS	European External Action Service	The diplomatic service and combined foreign and defence ministry of the European Union.
EU	European Union	A political and economic union of 27 European states.
FBI	Federal Bureau of Investigation	The primary federal domestic counter-intelligence and security agency for the U.S.
FIMI	Foreign Information Manipulation and Interference	Acts of manipulating or interfering with information by foreign entities aimed at undermining democratic processes and national security.
FIMI RC	Resilience Council against FIMI	A council focused on addressing and mitigating FIMI threats.
FIMI RC Pl	Resilience Council against FIMI Poland	The Polish branch of the Resilience Council focused on combating FIMI threats.
GEC	Global Engagement Center of the U.S. Department of State	A bureau within the U.S. Department of State responsible for directing, leading, coordinating and integrating U.S. Federal Government efforts to recognise, understand, expose, and counter foreign state and non-state hostile disinformation. Closed its activities in December 2024.
G-7	The Group of Seven	A group of top global economies founded in 1975, which includes Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. It deals with global development, trade, climate, security, and foreign policy issues; the European Union holds observer status.
MFA	Ministry of Foreign Affairs	The government department responsible for a country's foreign relations and diplomacy.
MITRE ATT&CK	MITRE ATT&CK for Enterprise	A knowledgebase of cyber adversary behaviour and taxonomy for adversarial actions across their lifecycle.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst	The military intelligence and security service for the Netherlands.
NASK	Naukowa i Akademicka Sieć Komputerowa	A Polish research and development organisation that operates the national research and education network.

NATO	North Atlantic Treaty Organisation	A political-military defensive alliance grouping 32 member states from Europe and North America.
NGO	Non-governmental Organisation	An independent organisation that operates without government control, typically focused on humanitarian or social issues.
OpenCTI	Open Cyber Threat Intelligence Platform	A platform meant for processing and sharing knowledge for cyber threat intelligence purposes. Developed by the French national cybersecurity agency (ANSSI) along with the CERT-EU (Computer Emergency Response Team of the European Union).
RRM	Rapid Reaction Mechanism	An initiative to strengthen coordination across the G7 in identifying, preventing, and responding to threats, including FIMI.
RT	Russia Today	A Russian (dis)information TV and media outlet.
SAUFEX	Secure Automated Unified Framework for Exchange	A project financed by the European Union under HORIZON EUROPE and endorsed by various international bodies, aiming to advance the state-of-the-art in combating FIMI.
STIX	Structured Threat Information Expression	A data format used to encode and exchange cyber threat intelligence (CTI). It can also be used to share insights on FIMI incidents.
TTPs	Tactics, techniques, and procedures	A common terminology that describes an actor's behaviour, including its general goals (tactic), the methods used to achieve those tactical goals (technique), and the specific actions employed within a technique (procedure).

Introduction

This report constitutes a deliverable within the **SAUFEX** project.[1] It contains research results offering inferences, observations, and lessons-learned in seeking an answer to the following question: how are European Union (EU) Member States countering Foreign Information Manipulation and Interference (FIMI)?

FIMI as the problem indicated in the above research question has been recognised by EU Member States as a threat to their internal cohesion, stability, and wider democratic order. The 2022 *EU Strengthened Code of Practice on Disinformation*, recalling earlier topical statements issued by EU institutions, stipulates that: "The exposure of citizens to large-scale disinformation, including misleading or outright false information, is a major challenge for Europe. Our open democratic societies depend on public debates that allow well-informed citizens to express their will through free and fair political processes." However, a clear understanding of the threat and the need to take preventive action goes hand in hand with a belief in the need to protect "the fundamental right to freedom of expression, freedom of information, and privacy, and of the delicate balance that must be struck between protecting fundamental rights and taking effective action to limit the spread and impact of otherwise lawful content".[2]

Understanding the threat and the need to combat it while preserving the core values of the community is therefore an essential focal point of our research, for which the starting point is indicated above: how are EU Member States countering FIMI?

Importantly, the adopted approach is empirical, not normative. Accordingly, the focus of this report is not on what should be done but on what is being done in the EU Member States to counter FIMI. Thus, this project seeks to conduct a mapping exercise of where EU Member States currently stand in terms of strategy, policy, institutional capacity, regulation, and societal resilience. In turn, this mapping will allow for the formulation of tentative conclusions as to whether and to what extent a common model for countering FIMI is *de facto* emerging across EU Member States. In this way, our research can contribute to improving European policies to combat FIMI, including by expanding access to knowledge of Member States' FIMI preventive and countermeasures. The resulting understanding of challenges, obstacles, and good practices can contribute to better coordination of efforts at the national and EU level.

Existing research focuses on operational and normative aspects of countering FIMI, and disinformation more broadly, whereas a comprehensive empirical analysis of strategic, institutional, and regulatory capabilities is still largely missing, particularly when conducted in a broad comparative perspective.

For instance, when discussing strategies to counter disinformation and their effectiveness, various authors highlight greater emphasis on engaging (responsive) rather than disengaging (alternative) strategies[3]. Whereas the former focuses on fact-checking, debunking, turning the tables, or disrupting the disinformation network and blocking the opponent's messages, the latter relies on prevention campaigns such as educational programmes, media support

[1] Project SAUFEX (Secure Automated Unified Framework for Exchange) is financed by the European Union under the HORIZON EUROPE program. Grant Agreement no: 101132494

[2] *Strengthened Code of Practice on Disinformation*, European Commission, 2022, https://op.europa.eu/en/publication-detail/-/publication/c1c55f26-063e-11ed-acce-01aa75ed71a1/language-en [last access December 17, 2024].

[3] Matejova, M., Drmola, J., & Spáč, P. (June 10, 2024): Measuring the Effectiveness of Counter Disinformation Strategies in the Czech Security Forces, *European Security*, DOI: 10.1080/09662839.2024.2362153.

initiatives, and legal solutions like laws that revolve around speech and censorship. However, it is important to note that the above measures should be understood in operational (tactics, techniques and procedures), rather than strategic terms.

In a similar vein, a counter-disinformation literature review conducted by the Global Engagement Center (GEC) of the U.S. Department of State in July 2023[4] revealed that research on addressing preventive and defensive action is more prevalent than research dedicated to punitive or offensive measures. The reviewed literature has a predominantly normative orientation, outlining what measures policymakers *should* consider. Accordingly, in terms of defensive measures, policymakers *should* invest in resilience activities, such as fact-checking and media literacy; use a "whole-of-society" approach to detection and monitoring; and emphasize pre-bunking, positive and factual messaging, and amplification. Regarding offensive measures, policymakers *should* establish standard norms, common definitions, and a formal global code of conduct; pursue timely, targeted, and well-coordinated sanctions; and coordinate with likeminded governments on cyber operations as a response to disinformation[5].

In contrast, this report does not aim to provide an exhaustive list of the most effective measures to counter FIMI. **It contends that it is difficult to construct a scientifically rigorous measurement of the effectiveness of individual counter-FIMI tactics**. Reliance on experts' opinions, which is a tool typically used in think-tank analyses on how to counter disinformation effectively[6], has clear limitations related to normativity, subjectivity, and other biases. Thus, the programme's research team has attached greater importance to understanding the existing capabilities, coordination mechanisms, and cooperation systems implemented across the national contexts of EU member states.

The authors of this report are convinced that there is no one-size-fits-all approach; rather, effectiveness should be discussed at the systemic level with sensitivity to political, social, and security specificities. As a result, it is not the objective of this report to recommend a desirable pre-defined model to be followed by all EU member states but to highlight both similarities and specificities, areas of convergence and divergence, and patterns of diffusion of best practices.

Conceptual approach

The empirical focus of this report does not mean, however, that it completely abstracts from policy-oriented and actionable conceptualisations of measures aimed at countering FIMI. In fact, various tools oriented towards policy practice have inspired our four-dimension research framework outlined below. In this regard, the U.S. Framework to Counter Foreign State Information Manipulation is notable due to its consistent structured approach. This mechanism covers five Key Action Areas[7]: 1) national strategies and policies; 2) governance structures and institutions; 3) human and technical capacity, including digital security tools; 4) civil society, independent media, and academia; and 5) multilateral engagement via international organisations.

[4] U.S. Department of State, *Counter-Disinformation Literature Review*, July 2023, https://www.state.gov/counter-disinformation-literature-review/ [last access: October 31, 2024].
[5] Ibidem.
[6] Carnegie Endowment for International Peace, Countering Disinformation Effectively: An Evidence-Based Policy Guide, January 2024, https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en [last access: October 31, 2024].
[7] U.S. Department of State, *The Framework to Counter Foreign State Information Manipulation*, January 18, 2024, https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/ [last access: October 31, 2024].

The objective of the present report is to adopt a comprehensive and systemic approach to the empirical analysis of EU Member States' capabilities in countering FIMI. Accordingly, the research framework features four dimensions investigated at the member state level:

1) **Strategy and policy**
2) **Regulatory framework**
3) **Institutional capacity**
4) **Societal resilience**

The framework serves to conduct a mapping exercise rather than a systematic and rigorous comparison across all 27 EU member states. This is because these countries differ not only in their approaches to combating FIMI and their acuity of recognising the problem, but also in the sophistication of their systemic solutions. In this sense, it is easier to categorise these countries into separate groups based on their developed measures and policies for combatting FIMI rather than compare them directly given that the level of development of systemic solutions varies significantly.

Both deductive and inductive approaches were used to define specific analytical criteria for each dimension under investigation in this report.

To map national strategies and policies towards countering FIMI, we analysed national security strategies; sectoral strategies (related to disinformation, hybrid threats, communication, cybersecurity and digital affairs); and other documents that frame policy in this area, including action plans, concepts, and national frameworks. Comparative analysis of 27 EU Member States' approaches was followed by detailed analysis of seven case studies (i.e., the Netherlands, Latvia, Ireland, the Nordics, the Czech Republic and Slovakia, Poland and Romania, and France) of countries that possess national strategies dedicated to countering disinformation/FIMI or are currently in the process of creating or implementing such documents.

To analyse regulations aimed at countering FIMI in EU Member States, we mapped the level of state legal involvement in combating FIMI, categorising legislative approaches that ranged from a complete lack of dedicated regulation to comprehensive FIMI legislation. The documents selected for analysis included information security strategies and doctrines, media and digital platform regulations, and criminal codes. This was followed by a comparative legal analysis, examining each member state's approach to FIMI and highlighting their focus on public order, national security, and public health. Next, we assessed the role of media and internet regulation, with a particular focus on the EU's Digital Services Act (DSA), to understand its contribution to the prevention of FIMI and its compatibility with national laws. Finally, we analysed the effectiveness of FIMI regulations to identify best practices and gaps in implementation.

To map institutional capacities of EU member states, we examined the institutionalisation of national coordination systems, evaluating their centralised or decentralised character, location of principal coordination mechanism, and whether specialised state agencies had been established. In this area, we examined the usage of analytical frameworks and digital tools by state institutions and explored patterns of cooperation between state institutions and non-governmental organisations (NGOs). Finally, we looked at how institutional best practices are diffused vertically and horizontally and how they flow from trendsetters to followers.

The societal resilience section of this report takes a comprehensive approach to understanding the factors that enhance or undermine resilience against Foreign Information Manipulation and Interference. We examined the interplay between democratic practices, social cohesion, media

literacy, and trust in institutions as key elements shaping a society's ability to resist disinformation. This section categorises EU Member States into tiers based on their democratic strengths and vulnerabilities to FIMI. It also explores how historical and contemporary ties to autocratic states like Russia and China – whether economic, cultural, or religious – can be leveraged to spread disinformation and deepen societal divisions. Finally, this analysis highlights the crucial role of civil society organisations, NGOs, and grassroots movements, stressing their collaboration with governments and media as a cornerstone for fostering media literacy and building resilience.

Methodology overview

Research methodology used in this report includes the following techniques:

1) Desk research
2) Study visits
3) An expert survey
4) In-depth expert interviews

Desk research

Desk research was conducted in line with the four dimensions outlined above and in relation to all 27 EU Member States. To avoid duplication of efforts, the work was conducted by researchers responsible for in-depth coverage of specific states. Desk research was based on data available in the public domain and reflects the state of art as of July 1, 2024.

Study visits

The research team participated in three study visits to Vilnius (March 2024), Brussels (April 2024), and Helsinki (October 2024). A group of researchers also participated in the Rapid Alert System (RAS) conference organised by the Polish Ministry of Foreign Affairs (MFA) and the European External Action Service (EEAS), which was held in tandem with a counter FIMI wargame organised by the Helsinki Hybrid CoE in Warsaw (April 2024). Relevant data used for the purpose of this report was obtained during visits to the Lithuanian National Crisis Centre, the EEAS, the Hybrid Fusion Cell, NATO, and the Hybrid CoE, among others.

Expert survey

The survey conducted by the research team collected information from experts through the Computer Assisted Web Interview (CAWI) method. The anonymous survey was sent electronically to approximately 150 experts from all the EU member states, with 32 complete responses received – a 20% response rate. This relatively low response rate was unsurprising given the high level of sensitivity around the topic. The team received at least one response from 18 member states. Whereas not all member states were represented within the sample, various geographical regions of the European Union – as well as both large and small member states – were adequately covered.

Number of responses	EU Member States represented among respondents
4	Poland, Spain
3	Lithuania
2	Bulgaria, Germany, Italy, Malta, Portugal, Slovakia
1	Belgium, Czechia, Finland, France, Greece, Hungary, Ireland, Latvia, the Netherlands
0	Austria, Croatia, Cyprus, Denmark, Estonia, Luxemburg, Romania, Slovenia, Sweden

We obtained a balanced response rate in terms of gender: 17 respondents (53%) identified as male, 14 respondents (44%) identified as female, and one respondent (3%) preferred not to identify.

In terms of sectoral affiliation, the majority of respondents (53%) represented academia and think tanks. The team also recorded a sizeable representation of public administration (19%) and non-governmental organisations (16%). Individual respondents came from the business, military, and media sectors. A relative majority (41%) of respondents declared between two and five years of professional experience in the field of countering FIMI. Only two respondents declared more than 10 years of professional experience in the field. Female experts had, on average, less years of professional experience in the field than male experts.

The low response rate to our survey also indicates a relative lack of trust among potential respondents, a closing of knowledge within national silos, and a relatively low culture of sharing information regarding this sensitive area of research. This finding may provide some indication for the European Union in its practices as an institution of trust to support improvements in the culture of knowledge sharing.

The survey's content reflected the four-dimensional conceptual approach outlined above with two categories of questions. The first type of question asked respondents to provide information related to the type of policy documents, state institutions, regulatory acts, and non-governmental initiatives aimed at countering FIMI. The second type of question focused on the respondent's personal assessment of a given mechanism or tool.

Due to the relatively low response rate, the research team did not analyse survey results separately, nor did we attempt to generate conclusions relying solely on that basis. Despite this, the survey still proved to be a valuable data source insofar as it allowed the team to triangulate results obtained from desk research and in-depth expert interviews.

In-depth expert interviews

We conducted 22 in-depth interviews, which were held predominantly online, with experts from 14 EU Member States. Each expert was matched with the interviewer who was in charge of the desk research for that particular member state. Interviews were semi-structured and based on a common pool of questions that were adapted to the specificity of the member state and the respondent's expertise. Interviews were not recorded, and anonymity was granted to respondents. The interviews aimed to close gaps and triangulate data obtained during the desk research stage.

Number of interviews	EU Member States represented among interviewees
3	France
2	Czechia, Hungary, Lithuania, Poland, Romania, Spain
1	Bulgaria, Estonia, Germany, Italy, Latvia, Portugal, Slovenia
0	Austria, Belgium, Croatia, Cyprus, Denmark, Finland, Greece, Ireland, Luxembourg, Malta, the Netherlands, Slovakia, Sweden

In contrast to the balanced gender representation among survey respondents, the experts interviewed were mostly men (73%). This was not due to any biased respondent selection but rather due to the fact that those who agreed to be interviewed were predominantly men.

In terms of sectoral affiliation, the largest cohort represented by interviewees was academia and think tanks (38%). Similarly to the survey, the team also recorded a sizeable representation of public administration (21%) and non-governmental organisations (25%). Two respondents reported two affiliations.

Similarly to the survey, the questions asked during the in-depth interviews reflect the four-dimensional conceptual approach outlined above. In particular, the team sought additional information about the push factors that led to the establishment of institutions or coordination systems, specific regulatory solutions, and modes of cooperation - both nationally (with non-government stakeholders) and internationally (both bilaterally and multilaterally). We also asked respondents to assess particular institutional and regulatory solutions and modes of cooperation and asked them to explain the criteria used in their evaluations. Finally, we asked the experts to share their assessments of the prospects for the counter-FIMI field and the community's development.

Part I – THE EU'S ROLE IN COUNTERING FIMI

This section of the report analyses the evolution of the Foreign Information Manipulation and Interference concept, including the impact of new technologies enabling foreign actors to spread misleading information[8]. It examines the EU's toolbox for countering FIMI as well as its broader approach to tackling disinformation. The section evaluates efforts to standardise FIMI detection through the use of unified terminology that creates a shared understanding of the threat and promotes collaboration across society. Additionally, it explores the development of a common framework to optimise knowledge generation, sharing, and activation, grounded in open-source and collaborative standards. Finally, the section examines the EU's toolbox of joint responses (FIMI Toolbox), which aims to provide effective and proportional counter-FIMI measures and responses.

From disinformation to FIMI - evolution of the concept

FIMI is a growing political and security challenge that needs a common framework for effective prevention and response. The concept of FIMI, which is relatively new, encompasses the threats derivative to the actions of hostile actors and permits the European External Action Service (EEAS) to maintain situational awareness of developments in the information space. Without limiting its ongoing monitoring and analysis processes to specific actors, the EEAS can endeavour to set out best practices for fighting disinformation through the sharing of data, analysis, and best practices that inform effective action. However, this can only be realistically achieved if the large variety of actors engaged in countering FIMI speak a common language[9].

Between 2015 and 2021, in the context of information manipulation, the EU used the term **disinformation** to describe "verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public, and may cause public harm"[10]. The category of **foreign information manipulation and interference (FIMI)** was first introduced into the official language of the EU in 2021 to describe a concept broader than disinformation. It is defined as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory."[11]

Accordingly, FIMI is not synonymous with misinformation or disinformation. Unlike in the case of misinformation, it is spread intentionally to deceive the public; furthermore, in contrast

[8] Kupiecki, R., Bryjka, F., Chłoń, T., *International Disinformation. A Handbook for Analysis and Response*, Brill, Leiden/Boston, 2025, DOI: 10.1163/9789004715769.

[9] To help operationalise the concept, the EEAS recommends a Kill Chain taxonomy of FIMI TTPs developed by Disinformation Analysis and Risk Management (DISARM). See:
European Union External Action Service (EEAS). *1st EEAS Report on Foreign Information Manipulation and Interference Threats – Towards a framework for networked defence*, pp. 29–30, February 23, 2023, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en [last access: April 7, 2024].

[10] European Commission, 2018, "Tackling online disinformation: A European Approach. COM(2018) 236 Final," https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEXper cent3A52018DC0236, [last access: November 30, 2024].

[11] European External Action Service (EEAS), October 2021, *Tackling Disinformation, Foreign Information Manipulation and Interference. Stratcom Activity Report*. https://www.eeas.europa.eu /eeas/2021- stratcom-activity-report-strategic-communication-task-forces-andinformation-analysis_en [last access: December 11, 2024].

to disinformation, FIMI does not refer solely to false or misleading information. This latter aspect of the concept is a welcome evolution given the fact that malicious actors have long understood that the best influence operations are not limited to false information alone. As has been noted by the EU DisinfoLab: *not all disinformation is FIMI, and FIMI is not only disinformation*[12]. The main aspects of FIMI as a concept that have evolved beyond disinformation are:

- a refocusing of interest on behaviour and operating methods (while counter-disinformation activities often look at the content and tackling of narratives);

- increased use of terms and processes from cyber-threat intelligence, which have enabled the toolbox of countermeasures to expand beyond the current focus on strategic communication and debunking of misleading or false narratives;[13] and

- a holistic approach that includes mobilising whole-of-society resources, favouring the adoption of a common terminology.

In one aspect, FIMI can be perceived as a seemingly narrower concept than disinformation due to its focus on foreign actors' behaviour alone, disregarding activities that originate domestically (if they are not sponsored or inspired by foreign actors). In other ways, it can be seen as a more encompassing term as it does not limit itself to false or misleading information. Instead, FIMI focuses on the manipulative behaviour exhibited in the process of delivering information, such as an artificial amplification of a narrative through fake social media accounts that influences a public debate[14].

The concept of FIMI is increasingly used across the EU and its member states. The origins of development of the concept can be traced to 2019 when the issue of foreign digital interference and the potential benefits of standardising the description of observed incidents came to the attention of the EEAS[15]. The concept was further developed in two other EU official documents key to the evolution of the concept: the December 2020 *European Democracy Action Plan*[16] and the 2022 *Strategic Compass*[17], which called for the development of a FIMI-dedicated

[12] Hénin, N., *FIMI: towards a European redefinition of foreign interference,* EU Disinfo Lab, April 2023, https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [last access: April 07, 2024].

[13] The EEAS FIMI framework builds on experience in cybersecurity, in which forensic analysis focuses on threat actor behaviour throughout the entire timeline of its attempted attack (i.e., the "Kill Chain" model). This has helped it to better understand systemic vulnerabilities and how to spot and close their exploitation. At the heart of the Kill Chain perspective on FIMI is the systematic and granular data collection on Tactics, Techniques, and Procedures (TTPs), which are patterns of behaviour used by threat actors to manipulate the information environment with the intent to deceive. This method allows us to ask what a threat actor was doing before they were able to deploy a message, where in the attack chain they are currently, and what their next step(s) may be. Ibidem, p. 9; European Union External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats – Towards a framework for networked defence*, February 23, 2023, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en [last access: April 7, 2024].

[14] Ibidem, p. 25.

[15] Hénin, N., *FIMI: towards… op.cit.,* p. 4.

[16] European Commission, *Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0091 [last access: March 24, 2024].

[17] European Union External Action Service (EEAS), *A Strategic Compass for Security and Defence*, March 24, 2022, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf [last access: April 14, 2024], p. 12, 40.

toolbox for the EU. This doctrinal evolution concluded with the first EEAS report on *Foreign Information Manipulation and Interference Threats* of February 2023[18].

According to the definition provided by the EEAS, FIMI operators "can be state or non-state actors, including their proxies inside and outside of their own territory"[19]. Therefore, this analytical framework is applicable to all regions and actors as well as foreign and domestic analyses for its actor-agnostic design. Hence, it may be used by all stakeholders regardless of their respective focus[20]. Member states can adapt the framework according to their own analytical limitations and institutional division of competencies concerning either domestic or foreign actors.

The approach offered by the EEAS focuses on behaviour (modus operandi) rather than content (narrative) or the actor involved. Importantly, the focus on behaviour enables expanding the toolbox of countermeasures beyond strategic communication and debunking of misleading or false narratives. It helps to alleviate some of the institutional difficulties in engaging with content that is highly political by nature, such as allowing the EEAS to avoid accusations of censorship or authoritative decision-making on what is true or false.

EU Member States have not yet established uniform criteria to qualify information incidents as FIMI. Similarities in approach can, however, be observed among some of the leading nations. For example, the Swedish government considers a FIMI incident to: 1) have a foreign origin; 2) contain content that misleads the recipient; 3) have the intent to inflict harm; and 4) carry potential security risks[21], while the French agency VIGINUM considers similar criteria for digital interference: 1) involvement of foreign actors; 2) inauthenticity of behaviour; 3) misleading content; and 4) a specific target[22]. The experts surveyed for this project indicated that the main factors that make a FIMI incident relevant for further analysis or reaction are:

- An attack on the fundamental interests of the state (87,5%)
- Manifestly inaccurate or misleading content (71,8%)
- Inauthentic distribution of content (65,6%)
- Automated distribution of content (46,8%)[23]

Measuring the impact of FIMI operations presents a significant challenge. To overcome this, organisations detecting and analysing FIMI can use Ben Nimmo's Breakout Scale, a comparative model for measuring influence operations based on data that is observable, replicable, verifiable, and available from the moment it was published[24]. The Breakout Scale divides FIMI operations into six categories based on whether they remain on one platform or travel across multiple platforms (including traditional media and policy debates) and whether they remain in one community or spread through many communities. However, the model does

[18] European Union External Action Service (EEAS), *1st EEAS Report…op.cit.*
[19] Ibidem, p. 4.
[20] States remain central FIMI threat actors. Moreover, the EEAS admits that its mandate and strategic priorities have limited its focus on influence operations conducted by two state actors: Russia and China.
Ibidem, p. 8.
[21] Based on the Swedish presentation at the RAS PoCs conference in Warsaw, April 9-12, 2024.
[22] Based on the French presentation at the RAS PoCs conference in Warsaw, April 9-12, 2024.
[23] Results from the survey conducted for the purpose of this report.
[24] B. Nimmo, *The Breakout Scale: measuring the impact of influence operations*, Brookings, 2020, https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations [last access: December 3, 2024].

not offer practical solutions for how to react to FIMI operations depending on their scale and impact.

Below, we describe the Breakout Scale's categories and suggest our related risk assessment and applicable countermeasures:

Category I – Operation is conducted only within one community on a single platform, and the messaging does not spread beyond the community. The operation may reinforce that community's (*information bubble*) existing beliefs, but it has very limited potential to reach new audiences and convert users in other communities, or to spread more broadly.

Risk assessment – very low; *reaction* – monitoring.

Category II – Operation conducted either in one community across multiple platforms or across multiple communities on one platform, but it does not spread beyond them.

Risk assessment – low; *reaction* – monitoring.

Category III – Operation conducted across multiple social media platforms that reaches multiple communities; it does not spread into the mainstream media.

Risk assessment – medium; *reaction* –fact-checking and debunking by NGOs and sectoral state institutions using their own channels on social media.

Category IV – Operation that spreads beyond social media and is amplified by mainstream media.

Risk assessment – high; *reaction* – official statement, debunking, and counter-narrative using own channels and mainstream media.

Category V – Operation that is amplified by high-profile individuals such as celebrities and political candidates.

Risk assessment – high; *reaction* – official statement, debunking, counter-narrative, naming and shaming, assigning legal responsibility if the law has been violated, and cooperation with other celebrities and influencers to promote a fact-based counter-narrative.

Category VI – Operation that triggers a policy response or some other form of concrete action, or an operation that includes a call for violence.

Risk assessment – very high; *reaction* – blocking domains, origin account, and other accounts used to spread content calling for violence; holding organisers legally responsible.

The impact of new technologies and the evolution of FIMI

The EU FIMI conceptual framework is not limited to fake news, propaganda, or disinformation but focuses on interference in the political processes of states subjected to hostile information influence. It encompasses the problem of information manipulation more broadly by considering the evolving FIMI Toolbox. This includes tactics, techniques and procedures (TTPs) used by Russia, China, and Belarus, among others, including in the cyber domain (e.g., attacks on voter registries, deep fakes, or hack-and-leak operations involving the stealing and publishing of confidential information or correspondence). To counter FIMI, EU members have adopted new strategies and policies; created dedicated structures in public administration; improved regulatory frameworks; and cooperated with civil society organisations, online

platforms, and the media[25]. In doing this, they are forced to constantly adapt to the changing TTPs used by threat actors.

FIMI operations are characterised by increasing levels of automation due to technological advances. Using bot farms, or computer programs that mimic human online behaviour, attackers can spread manipulated content on a massive scale and increase the reach of malicious activity.

Another common method of carrying out FIMI operations is to impersonate politicians or institutions by cloning their websites and official social media accounts. These operations are carried out with the help of sophisticated infrastructure and cloaking software, making it difficult to detect the attacker and attribute responsibility. The use of artificial intelligence (AI) is also playing a growing role in FIMI operations, enabling malign actors to create fake-but-authentic social media personas *en masse* or fake speech by a real person (deep fake)[26].

One example of this was found by the U.S. Federal Bureau of Investigation (FBI) and Cyber National Mission Force (CNMF), in partnership with the Netherlands General Intelligence and Security Service (AIVD), Netherlands Military Intelligence and Security Service (MIVD), the Netherlands Police (DNP), and the Canadian Centre for Cyber Security (CCCS). In a joint cybersecurity advisory released in 2024, they noted that Russian state-sponsored actors (i.e., Russia Today affiliates) used the AI enhanced software package Meliorator to create fictitious online personas representing several nationalities, which then posted content on X (formerly Twitter)[27]. Using this tool, which was employed for foreign malign influence activity benefiting the Russian government, RT affiliates disseminated disinformation to and about several countries, including the United States, Poland, Germany, the Netherlands, Spain, Ukraine, and Israel[28].

Because of the increasing role of new technologies in FIMI, cooperation with the private sector plays a key role in countering its impact. In **September 2018, the European Union adopted its first Code of Practice** governing EU countries' cooperation with the private sector (including major online platforms such as Facebook, Google, Twitter, Mozilla, and Microsoft) on obligations for online platforms and the advertising industry to improve the transparency of political advertising, take down fake accounts, and reduce incentives for spreading disinformation[29]. In **2022, the code was updated** and signed by 34 private entities.

The *Strengthened Code of Practice on Disinformation* brings together a diverse range of stakeholders, empowering them to contribute to wide-ranging improvements by agreeing to precise commitments relevant to their field. It sets broad commitments and measures to counter online disinformation for its voluntary signatories, which range from the fact-checking and

[25] For more see: Chłoń, T., & Kupiecki, R., *Towards FIMI Resilience Council in Poland. A Research and Progress Report*, https://saufex.eu/research [last access: December 20, 2024].

[26] Mazzucchi, N., AI-*based technologies in hybrid conflict: The future of influence operations*, Hybrid CoE Paper, no. 14, June 2022, https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf [last access: July 9, 2024], p. 6.

[27] Although the tool was only identified on X, the authoring organisations' analysis of Meliorator indicated that the developers intended to expand its functionality to other social media platforms. The authoring organisations' analysis also indicated the tool is capable of the following: creating authentic appearing social media personas *en masse*; deploying content similar to typical social media users; mirroring disinformation of other bot personas; perpetuating the use of pre-existing false narratives to amplify malign foreign influence; and formulating messages, to include the topic and framing, based on the specific archetype of the bot.

[28] Joint Cybesecuriry Advisory, *State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity*, https://www.ic3.gov/CSA/2024/240709.pdf [last access: July 9, 2024].

[29] European Commission, *2018 EU Code of Practice on Disinformation*, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation [last access: July 9, 2024].

advertising industries to researchers and civil society representatives. These measures include de-monetising the dissemination of disinformation, increasing the transparency of political advertising, and providing researchers with better access to data. Disinformation and foreign interference are also addressed within the hybrid threats framework[30].

One important breakthrough in the fight against disinformation was achieved with the adoption of the 2022 **Digital Services Act (DSA)[31].** This landmark EU regulation entered into effect in February 2024, introducing binding obligations for very large online platforms and search engines to counter illegal online content. It also established transparency and oversight measures and rules for content moderation. These rules aim to safeguard the fundamental rights of online users and establish accountability to mitigate systemic risks such as disinformation or election manipulation. The DSA therefore provides a uniform legal framework across the EU to counter risks related to disinformation and foreign interference[32]. Once fully implemented by the EU Member States, the DSA will be the world's first regulation that enforces transparency and public oversight for very large online platforms and search engines – a model that the EU hopes will serve as inspiration for similar legislation in other parts of the world.

The EU has also established measures to protect media freedom and ensure the independent functioning of public service media. In March 2024, it adopted its new Media Freedom Act that obliges member states to protect journalists and media independence against political or economic interference[33]. The act also establishes responsibilities for the media on transparency of ownership and state advertising funds. Other EU policies and action plans that aim to respond to and build resilience against foreign information manipulation include the 2024 Artificial Intelligence Act[34], which focuses on regulating the risks of AI, and the Defence of Democracy package. This package, which was adopted ahead of the European Parliament elections in June 2024, aims to enhance transparency and accountability through legislative and non-legislative measures to tackle the threat of covert foreign influence in democratic processes. It also encourages citizens and civil society organisations to participate in building civic resilience[35].

The increasing use of AI in information operations has given malign actors the ability to gain influence over the conduct and outcome of elections in democratic states. New technologies are used with harmful intent to design and execute influence operations that target both mass audiences and specific communities. This technology provides a notable advantage for attackers as it enable the distribution of manipulated content on a mass scale without the perpetrator suffering meaningful consequences for such activity. This threat is likely to increase in the

---

[30] European Commission, *Strengthened code of practice on disinformation*, 2022, https://op.europa.eu/en/publication-detail/-/publication/c1c55f26-063e-11ed-acce-01aa75ed71a1/language-en [last access December 17, 2024].

[31] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng [last access December 17, 2024].

[32] European Commission, *Questions and answers on the Digital Services Act.* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 [last access: February 23, 2024]. European Commission, *The Digital Services Act package,* https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [last access: February 16, 2024].

[33] European Commission, *European Media Freedom Act,* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en [last accessed: March 15, 2024].

[34] European Parliament, *Artificial Intelligence Act*, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf [last access: March 13, 2024].

[35] European Commission, *Defence of Democracy – Commission proposes to shed light on covert foreign influence. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453* [last access: December 12, 2024].

future as AI-based technology continues to evolve to the point where it will be capable of planning entire campaigns, including determining effective narratives and target groups.

The EU's approach to countering FIMI

The Strategic Compass adopted by the EU Council on March 21, 2022, less than one month after the Russian invasion of Ukraine, proposed a plan to increase the resilience of states and societies to foreign information manipulation and interference by developing a counter FIMI Toolbox. In recent years, the European Union has established several instruments that enable institutions and member states to address FIMI while providing careful consideration for fundamental rights and freedoms.

The FIMI Toolbox outlines different areas and instruments that together constitute a robust and comprehensive framework for tackling FIMI. The toolbox includes short, medium, and long-term measures – from prevention to reaction – and offers a dynamic system that accounts for the constant evolution of threats. The envisaged instruments of the EU FIMI toolbox have been grouped into four dimensions:

Situational awareness – A thorough understanding of the threat is key to early detection and mounting an appropriate response. Documenting the threat sufficiently and systematically is (1) the first line of defence against FIMI. Being informed is necessary to (2) raise awareness about the threat among various audiences, including decision makers, the media, and society; (3) repair the weaknesses that aggressors exploit (e.g., by introducing media literacy programmes or putting pressure on internet platforms to prevent manipulation operations); and (4) punish the aggressors by limiting their capabilities to operate (e.g., imposing sanctions or blocking domains)[36].

Resilience building – Examples of this include strategic communication, cooperation within the EU's Rapid Alert System (RAS), or efforts to inform and raise public and institutional awareness.

Disruption and regulation – These aim to further trust, transparency, and safety in the information environment through efforts like the Digital Services Act. These are permanent instruments that shape the environment in which responses to FIMI are taken.

Joint efforts related to EU external action, including a Common Foreign and Security Policy (CFSP) and diplomatic responses – This dimension makes use of instruments in the area of foreign and security policy, such as international cooperation, the G7 Rapid Response Mechanism, or sanctions like those imposed on Kremlin-controlled media outlets like RT and Sputnik[37].

[36] Kalenský, J., *The structure and the effect of the disinformation ecosystem*, Information Security Summit IS2, https://is2.cz/en/articles/speakers-2020/jakub-kalensky-en [last access: September 9, 2024].

[37] European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, January 2024, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en, p. 14 [last access: September 17, 2024].

Table 1: Counter Foreign Information Manipulation and Interference Toolbox

Situational Awareness	Resilience Building	Disruption & Regulation	EU External Action
Common Framework & Methodology	Strategic Communication	Digital Service Act	Restrictive Measures
Monitoring & Detection	Policy Responses and Strategy	Code of Practice on Disinformation	Political Attribution
OSINT Investigations	Internal Organisational Structures	European Media Freedom Act	International Norms and Principles
Information Sharing & Analysis	Rapid Alert System	Transparency	Diplomatic Responses
Impact Assessment	Awareness Raising and Exposure	Addressing AI and Emerging Technologies	G7 Rapid Response Mechanism and others
	Capacity Building	Other Legislation and Regulations	International and Multilateral Cooperation
	Digital, Media, and Information Literacy	Engaging with the Private Sector	
	Strengthening Independent Media		
	Empowering Civil Society		
	Fact-Checking		

Source: European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, January 2024.

Russia's illegal annexation of Crimea in 2014 and its disinformation campaigns in member states compelled EU institutions to build up special mechanisms and tools to better detect and deter FIMI operations. In March 2015, the European Council asked the High Representative for Foreign Affairs and Security Policy to develop an action plan for strategic communications to counter Russia's disinformation campaigns. As a result, a taskforce responsible for monitoring, analysing, and responding to Russian propaganda and disinformation, **East StratCom, was established within the European External Action Service (EEAS)**. In 2017, two further StratCom task force units were created: one for the Southern Neighbourhood (South StratCom Task Force) and one for the Western Balkans (Western Balkans Task Force). A Sub-Saharan Africa StratCom task force was also added in 2024.

These teams are part of the **approximately 40 Strategic Communications, Task Forces, and Information Analysis Division (SG.STRAT.2) at the EEAS**[38], which support EU institutions

[38] Russia's full-scale invasion of Ukraine intensified the activities of EU institutions in countering disinformation. East StratCom, for example, was strengthened both financially and in its staffing. It now has 13 full-time employees who can outsource research tasks and analyse how Russia adapts its disinformation techniques and methods to changing situations. East StratCom monitors information messages published in more than 20 languages. Within the EEAS, similar tasks to East StratCom are carried out by analogous teams (with six full-time staff each) responsible for the Western Balkans region and the Middle East and North Africa region. They focus on counter-radicalisation and combating propaganda from terrorist organisations as well as disinformation from Russia, China, Iran, and Turkey. Additionally, there is a Horizontal Threat Team that deals with Chinese disinformation (four staff members), a team that supports EU missions and operations, a team that analyses

with policy planning and analysis, strategy, and strategic communication tools. It also provides support (e.g., analysis and instructions to combat disinformation) for EU delegations, missions, and operations under the Common Security and Defence Policy (CSDP). The unit has also developed cooperation with partner countries, the G7, NATO, civil society organisations, and the private sector (e.g., on data acquisition using modern software and technology). The aim of these activities is to build public awareness and strengthen resilience to disinformation[39].

In mid-2024, SG.STRAT.2 underwent a reorganisation, which according to EEAS analysts, aimed to "adapt the structures to the already existing tasks they have been performing so far"[40]. The new structure was announced in May 2024 and now consists of four divisions: 1) Foresight; 2) Global StratComms, which includes inter-institutional communication, public and cultural diplomacy, social media, and preparation of speeches for the EU High Representative for Foreign and Security Policy; 3) FIMI, which includes a Data Team; and 4) Geographical Taskforces (i.e., Eastern Europe, the Western Balkans, MENA, Asia-Pacific, and Sub-Saharan Africa).

To increase situational awareness of hostile information manipulation, the EU established a **Rapid Alert System (RAS)** on disinformation in March 2019. The exchange of information under this operational mechanism takes place through national points of contact (PoCs) established by the EU Member States. PoCs in the RAS come mainly from the StratCom units within member states' Ministries of Foreign Affairs (MFA), Ministries of Interior (MOI), and Ministries of Defence (MOD). This system was used in 2020 during the COVID-19 pandemic when the information space was flooded with a wave of Russian and Chinese disinformation aimed at undermining confidence in Western vaccines, EU institutions, and vaccination strategies. Despite the use of RAS to exchange information between EU institutions and the member states, private sector representatives, and G7 and NATO members, it did not stop the wave of conspiracy theories spread by, among others, anti-vaccine circles or pro-Russia and pro-China news channels, including troll factories.

RAS as a platform for the exchange of information between PoCs has some limitations and drawbacks that affect its functioning. One shortcoming of the platform is that PoCs can only receive incident information when they are logged into the system. In a situation where a PoC is carrying out other tasks that prevent them from accessing the system, they have no other means of being promptly informed about the alert, which can delay their ability to employ an appropriate reaction[41]. Therefore, according to some EU member state PoCs, an alternative (informal) system of warning is needed[42].

In the opinion of RAS users, not all incidents are sufficiently important to be put into the system. The characteristics of incidents qualifying for introduction into the system are mostly those that:

(i) may lead to the triggering of socio-political actions (e.g., protests, demonstrations, or riots).

---

quantitative data on disinformation techniques, tactics, and procedures (TTPs) used by disinformation actors (three analysts), and two political action teams that focus on building resilience. As a result of French advocacy, a team responsible for Sub-Saharan Africa, which is now seen as the focus of Russian disinformation operations, has also been created. This information is based on interviews with EEAS staff conducted on June 21, 2023, in Warsaw.

[39] Strategic Communication Task Forces and Information Analysis Division, *2021 StratCom activity report*, March 24, 2022, https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis-division_en [last access: July 29, 2024].

[40] Based on interviews during a study visit to Brussels on April 22-25, 2024.

[41] Based on a discussion held during the RAS PoCs conference in Warsaw on April 9-12, 2024.

[42] Based on a discussion held during the RAS PoCs conference in Warsaw on April 9-12, 2024.

(ii) may be part of a larger operation carried out on the territory of several EU countries.
(iii) are carried out in combination with cyber-attacks (e.g., on state electoral commissions).

Users of the system also note the potential utility of sharing technical reports of their investigations with other member states. This would help in detecting operations carried out in other EU countries, as well as in attributing activities to an attacker[43]. Until now, member states have not been willing to share such detailed reports.

One exception to this that could represent a turning point in member states sharing technical reports was the publications of the French VIGINUM, entitled Portal Kombat, which exposed the activity of a network of 193 "information portals" with similar characteristics that disseminated pro-Russian content targeting several Western countries (including France, Germany, Austria, Switzerland, Poland, the United Kingdom, and the United States)[44]. Its publication contributed to the removal of the network of Telegram accounts linked to these websites that were aimed at distorting Western public perception around the Russian invasion of Ukraine.

While RAS is a platform of state-to-state information exchange, the **Foreign Information Manipulation and Interference Information Sharing and Analysis Centre (FIMI-ISAC)** is a group of like-minded organisations that protect societies, institutions, and the critical information infrastructures of democracy from external manipulation and harm. Through collaboration, the FIMI-ISAC enables its members to detect, analyse, and counter FIMI more rapidly and effectively while upholding the fundamental value of freedom of expression. The FIMI-ISAC does not act independently to counter FIMI. Instead, it enhances collaboration to empower its members to do so more effectively[45].

Standardisation of FIMI detection and response

Like in the case of other hybrid threats, countering FIMI is primarily the responsibility of EU Member States. However, the effectiveness of these activities depends on the cooperation of various countries and organisations. Institutions responsible for countering FIMI in EU countries are housed under different governmental structures (e.g., foreign affairs, interior, or defence ministries), which allows them varied mandates, organisational structures, and scopes of tasks. Each state also uses different methodologies for analysing FIMI incidents, which complicates information-sharing and methodological standardisation.

Since 2015, the EU has been working to address this challenge by developing its own capabilities to monitor, identify, and analyse disinformation, as well as to enable the exchange of information between member states and like-minded partners. Delivering on the commitments made under the Strategic Compass, and in line with the objectives of the European Democracy Action Plan, the EU has focused on responding to the following primary needs:

1. A unified terminology to establish a common understanding of the threat that helps to facilitate whole-of-society collaboration.

[43] Based on a discussion held during the RAS PoCs conference in Warsaw on April 9-12, 2024.
[44] *Portal Kombat. A structured and coordinated pro-Russian propaganda network. Technical report*, VIGINUM, February 2024, https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf [last access: September 23, 2024].
[45] *FIMI-ISAC Collective Findings I: Elections*, October 2024, https://fimi-isac.org/wp-content/uploads/2024/10/FIMI-ISAC-Collective-Findings-I-Elections.pdf [last access: September 23, 2024].

2. A common framework to optimise knowledge generation, exchange, and activation based on open-source and collaborative standards.
3. An EU Toolbox of joint responses (FIMI Toolbox) to inform effective and proportional counter-FIMI measures[46].

Since the adoption of the Strategic Compass in March 2022, the EU has worked to standardise the detection of and response to FIMI based on the DISARM-STIX[47] method, which is used by, among others, the Data Analysis Team in the Strategic Communications, Task Forces, and Information Analysis Division (SG.STRAT.2) of the EEAS. This method allows for the analysis of TTPs used, as well as information on the infrastructure used to carry out influence operations (e.g., domains, servers or inauthentic accounts) to be entered into a common database.

DISARM is an open-source framework for fighting disinformation that was launched in 2019. It has been successfully used by global agencies and country teams to defend democracy, support pandemic-related communication, and address disinformation campaigns worldwide. DISARM is backed by the non-profit Alliance 4 Europe and is made to help people who work with communication in any sector better understand disinformation incidents and figure out what actions can be taken to defend against them or make them less effective. The DISARM foundation's Kill Chain taxonomy is currently the most suitable for the community-led conversation on best practices as it fulfils all the above criteria. The framework is structured hierarchically by phases, tactics, and techniques and represents the state-of-the-art understanding of FIMI operations.

According to EEAS Data Team Analyst, "the DISARM is the most tangible asset to express and define the many different modes of information manipulation techniques known. It enables categorisation, directs research and analysis, unlocks forecasting abilities and is foundational to enable a collaboration between different groups of analysts (whole-of-society approach). Without this repository, systematic exchange of findings would not be possible and discussions would remain superficial or prone to misunderstandings. However, it needs way more systemic field testing to streamline TTPs names, descriptions and indicators. Its complexity will remain, because the problem it tries to capture is complex. Credible, technical certification should be improved as there is currently no authority with sufficient practical experience or technical knowledge offering courses".[48] To train analysts to disarm takes more time and also it is quite time consuming to label all related TTPs.

Building on the idea of a standardised and community-driven framework we have recognised several existing concepts and models that systematically allow its users to benefit from knowledge creation and sharing/mobilisation to ultimately increase cyber resilience. These models are:

- **DISARM-STIX** to represent information about times when people spread false information on purpose. It uses the Structured Threat Information eXpression (STIX) format, which is a widely adopted standard for representing and sharing cybersecurity-

[46] *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, European External Action Service, Brussels, January 2024, ttps://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en [last access: September 23, 2024], p. 12.
[47] Newman, H., *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'*, Hybrid CoE Research Report 7, November 2022, https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf [last access: September 23, 2024].
[48] Based on a interview conducted with EEAS Data Team Analyst on June 4, 2025.

related information. DISARM-STIX aims to enable analysts and responders to share information more effectively, improve situational awareness, and coordinate their actions in response to disinformation campaigns.

- **OpenCTI** is a platform that helps organisations manage their cyber threat intelligence. OpenCTI allows users to organise and visualise technical and non-technical information about cyber threats and links each piece of information to its primary source.

In 2022, the EEAS recognised the need for a common data format for threat information sharing and collaboration. Thus, it began encoding FIMI incidents in the Structured Threat Information Expression (STIX™) format, an open-source structured language used to describe cyber threat information so it can be shared stored, and analysed consistently. STIX helps people manage cybersecurity processes and automate them. Decomposing FIMI incidents into fundamental building blocks via STIX objects enables FIMI defenders to specialise in monitoring and maintaining a continuously updated list of narratives or developing new capabilities to spot highly relevant TTPs. Creating custom extensions for idiosyncratic FIMI threat indicators not yet covered by the standard is encouraged by its creators, but a consensus is needed among FIMI defenders on which objects to use, develop, and how to use them.

STIX enables data exchange and innovation. It eliminates friction and facilitates cooperation. It has been field tested in communities way larger than the FIMI 'defender community' and proved its worth. Current projects like DAD-CDM[49] consider well the possibilities for expanding its applicaiton to FIMI research. Adherence to the data standard has adaptation costs for organisations but offsets these costs in reality as organisations do not need to translate a variety of different standards into their own but can rely on interoperability out of the box, build tools on top of this standard and scale their operations. The existence of STIX saved the community years of inefficiency but requires further adoption by the community.[50]

STIX Object	**Description**
Incident	Holds basic information about an incident (name, description, start date, objective, etc.)
Observable	A URL or file that has been observed in an incident
Channels (extension)	Any online or offline communication channel (a website, social media profile or page, TV station, etc.). Channels publish observables
Identity	Individuals, organisations, or locations including countries. Usually encoding the targets of incidents
Threat Actor	Holds information about a threat actor
Event (extension)	Describes a real-life event like an election, show, anniversary, etc. to provide the context in which incidents can take place
Vulnerability	Describes a vulnerability that was exploited to make an incident work
Language (extension)	Which language(s) was (were) used in an incident
Attack Pattern	Describes manipulative techniques (TTP) used to conduct an attack
Course of Action	Describes countermeasures to incidents

[49] See: Deibler D., *Strengthening Digital Resilience*, DAD-CDM, April 23, 2025, https://dad-cdm.org/strengthening-digital-resilience/ [last access: 05.06.2025].
[50] Based on a interview conducted with EEAS Data Team Analyst on June 4, 2025.

Narrative (extension)	Describes narratives used in incidents. Narratives can be nested and represented as meta-and subnarratives

The ABCDE Framework can be used as a guide to map out FIMI incidents; diagnose disinformation problems, structure analysis, and design countermeasures. The framework breaks down disinformation into smaller operative factors:

A. **Actors** (what kinds of actors are involved? This question can help establish, for example, whether the case involves a foreign state actor);
B. **Behaviour** (what activities are exhibited? This inquiry can help establish, for instance, evidence of coordination and inauthenticity_;
C. **Content** (what kinds of content are being created and distributed? This line of questioning can help establish, for example, whether the information being deployed is deceptive);
D. **Degree** (what is the overall impact of the case and whom does it affect? This question can help establish the actual harms and severity of the case);
E. **Effect** (What is the overall impact of the case and whom does it affect? This question can help establish the actual harms and severity of the case).

It has been used to facilitate coordination among EU institutions, member states, digital platforms, and other stakeholders in terms of thinking about and communicating the issue by establishing a common language. The ABCDE framework has several advantages for EU policymakers. It can be used to analyse data from a variety of sources, including governments, researchers, NGOs, industry actors, and journalists. The framework supports delivery of structured report based on available data and evidence assuring clear and coherent manner. When assessing information from multiple sources, this framework can provide a means of assessing the likelihood of each proposition, supporting more transparent and accurate assessments. It is used to support the efforts of EU institutions, member states, digital platforms, and other stakeholders to speak the same language when thinking about and communicating about the problem. Implementation of the framework to wider number of stakeholders (including governments, industry actors, researchers and NGOs) would felicitate information exchange and a coherent dialogue. Common language and method of making assessments of FIMI incidents should help stakeholders to design countermeasures. The five components could also provide a template for requesting and receiving information and data from various stakeholders. For example, under the actor component, an EU institution may wish to request information from a digital platform about which state actors have been identified and with what degree of confidence.[51]

According to EEAS Data Team Analyst the ABCDE is a good mnemonic to outline the scope of a FIMI incident analysis. It serves great in trainings for new analysts and considers FIMI holistically, not just the content, not just the information manipulation, but all relevant aspects combined. ABCDE does not prescribe a certain type of analysis but ensures holistic consideration of multiple factors to assess an incident's impact and paves the way for more structured discussion on the problem and findings. However, it is often mistaken as a directive for how to conduct analysis, for which it was not created and is too under complex to deliver on. Open CTI has the advantage that it works on common standards out of the box, provides space for all elements of ABCDE to be encoded, is interoperable with standards data pipelines

[51] J. Pamment, *The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework Report*, Carnegie Endowment for International Peace, 2020, ttps://www.jstor.org/stable/resrep26180.6 [last access: 03.06.2025], p. 5-8.

and input/output systems and unlocks the possibilities for inferences. Replicating a tool like this would take years to build and likely not result in interoperability with partners. It is a good balance between customization and standardisation, while providing good security. However, the tool appears too complex for non-technical users, but its mainstream adoption by the technical OSINT and cyber community shows that it does fulfil analyst needs well. A simplified version could enhance adoption for the FIMI community. [52]

The EEAS's conceptual work has led it to propose a common analytical framework and methodological standards, which, although not mandatory for EU countries, are widely considered best practices. It is up to individual member states to decide on their possible implementation. Further standardisation of working methods by EU governments' analysts, as well as NGOs involved in combating FIMI, would greatly enhance the situational awareness of member states and improve the exchange of information among them.

However, the results of our survey indicate that there is still low uptake of EU standards by member states. The most popular framework for analysing TTPs by state institutions is DISARM, which 28.1 % of respondents indicated they utilize. Open CTI, a tool for collecting and exchanging data on analysed FIMI incidents, is used by 21.8 % of respondents, while 15.6% indicated that they use the STIX format. The lowest rate of positive responses was registered for the ABCDE framework (only 6.25%), which de facto includes the comprehensive use of DISARM and STIX through Open CTI. Nearly a fifth (18.75%) of respondents indicated that they use other analytical tools.

The results look different in the case of NGOs involved in the detection and analysis of FIMI. In this case, the rate of use of the ABCDE and DISARM frameworks were considerably high (both at 22.4%), indicating the integral use of both. However, the STIX format and Open CTI software were utilized less than by state institutions (12.5% in both cases), which may indicate insufficient involvement of NGOs in information sharing.

	State institutions	NGOs
ABCDE	6.25%	22.4%
DISARM	28.1%	22.4%
STIX	15.6%	12.5%
Open CTI	21.8%	12.5%
Other	18.75%	18.75%

Source: Results of the survey conducted for purpose of this report.

The standardisation of FIMI analysis methods would also facilitate technical attribution of FIMI incidents. This, in turn, should improve decision-making at the political level regarding coordinated responses. The ability to attribute responsibility for an attack is also an essential element of deterrence, as it imposes costs on the aggressor, ranging from image and credibility damage to political and financial (if sanctions are imposed) harm.

The 2nd EEAS report on FIMI proposed a "FIMI Response Framework" with the "aim of linking analysis and insights even more effectively to timely responses, highlighting the importance of cooperation between all the stakeholders that hold key instruments to respond to the intentional manipulation of the information environment"[53]. The framework is a guide to how defenders can prevent, prepare for, respond to, and recover from FIMI attacks while continuously

[52] Based on a interview conducted with EEAS Data Team Analyst on June 4, 2025.
[53] *2nd EEAS Report*…op.cit., p. 5.

improving their security to safeguard against future attacks. The framework is composed of three main elements:

1) **Cross-domain analysis** – Integration of FIMI analysis with other data sources of analysis like OSINT, ABCDE, DISARM, and STIX frameworks, among others.

2) **Adapted countermeasures** – The pre-identification of responses based on an attack pattern (identified TTPs) and activation time. This includes:
    a. **Pre-incident (preventive counters)**
        i. Creation of common analytical frameworks and methodology.
        ii. Implementation of programmes of media and information literacy and support for independent media, civil society, and fact-checking initiatives.
        iii. Use of strategic communication activities to build resilience and trust.
        iv. Investment in capacity building to enable members of the defender community.
        v. Creation of policy instruments (e.g., the AI Act, the Code of Practice on Disinformation, or the Digital Services Act).
    b. **Mid-incident (reactive counters)**
        i. Ignore – Sometimes it is advisable to ignore an incident instead of reacting to it, which can be counter-productive and lead to the manipulation's further proliferation.
        ii. Contain - Inform online platforms when an inauthentic network or harmful content is detected.
            a. Pre-bunk a story before it strikes.
            b. Early exposure of a network.
            c. Rapidly inform stakeholders of your findings to activate contingency plans.
            d. Restrict amplification of manipulated content.
            e. Prompt audiences when they engage with manipulated content.
        iii. Minimise – Remove inauthentic accounts and the content they distribute.
            a. Remove content that violates pre-existing community guideline, including coordinated and inauthentic behaviour, impersonations, malicious false content, and non-transparent paid ads.
            b. Remove or transfer websites, channels, or accounts involved in FIMI activities.
            c. Issue legal notices.
        iv. Redirect – Redirect the recipient's attention to reliable information with a message at the appropriate level.
            a. Expose and debunk the incident, the manipulation techniques, and the threat actor's objectives.
            b. Provide suitable, easily accessible, and reliable information.
            c. Update and adapt misused content to redirect audiences to verified content.
            d. Use humour-based responses.
            e. Label false and misleading content with warnings or debunks by third-party organisations.
            f. Give greater visibility to reliable content.
    c. **Post-incident (adaptive counters)**
        i. Information sharing with relevant stakeholders to reinforce situational awareness.

ii. Capacity building among the defender community based on insights gained from previous incidents.
iii. Identify and limit financial incentives for FIMI activities.
iv. Activate diplomatic responses.
v. Deploy legal responses, including sanctions.
vi. Monitor and respond to evasion tactics circumventing legal responses.
vii. Reinforce and adapt response instruments based on lessons learned.

3) **Mechanisms for collective response** – Increased community collaboration and protocols to activate responses[54].

Disruption of FIMI by sanctioning threat actors

Russian media outlets were first recognised by the EU as tools of information warfare after the full-scale invasion of Ukraine in February 2022. In March of that year, the Council of the European Union imposed sanctions on Russian state broadcaster RT/Russia Today and the media outlet Sputnik, including their foreign languages affiliates[55]. For years, these outlets have been among the main tools of Russia's ecosystem of disinformation and propaganda against Ukraine and Western countries. They are under the direct or indirect control of the Russian authorities and have been used to support unjustified armed aggression against Ukraine as well as destabilise neighbouring countries. They also constitute a serious and immediate threat to public order and security in the European Union[56].

Following the imposition of sanctions on the outlets, the EU placed leading Russian propagandists, including TV presenter Vladimir Solovyov and editor-in-chief of the English-language version of RT, Margarita Simonyan, on its sanctions list. In total, more than 50 propagandists from the Kremlin and other entities involved in Russian disinformation activities have been included on the list, including media outlets like Rossiya RTR/RTR Planieta, Rossiya 24/Russia 24, Rossiya 1, TV Centre International, NTW/NTV Mir, REN TW, Pervy Kanal, and the media organisation RIA FAN.

The restrictions imposed by the EU prevent these media outlets from broadcasting material via cable and satellite, as well as transmitting (via web TV, platforms, portals, and apps) content that undermines the democratic order in European countries and aims to polarise EU societies. However, the Council indicated that this decision was temporary. The sanctions were put in place "until the aggression against Ukraine ceases and the Russian Federation and its associated media cease their disinformation and manipulative activities against the EU and its Member States"[57].

[54] European External Action Service*, 2nd EEAS Report…op.cit.*, p. 15-18.
[55] These are RT, formerly Russia Today, and its affiliates, including Russia Today English, Russia Today UK, Russia Today Germany, RT Balkans, Russia Today France, Russia Today Spanish, and RT Arabic, as well as Sputnik and its affiliates, including Sputnik Arabic. In June 2023, Oriental Review, Tsargrad, New Eastern Outlook, and Katehon were further restricted as part of the EU's eleventh sanctions package.
[56] For more extensive information about the role of RT and Sputnik in the Russian disinformation-propaganda ecosystem, see: U.S. Department of State, *GEC Special Report: Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem*, Global Engagement Center, January 2022, ttps://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf [last access: June 26, 2024].
[57] European Union, *Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*,

In June 2024, the EU adopted its fourteenth sanctions package against Russia, including new restrictions on Russian funding of political parties and other "opinion forming" organisations, including Russian state media in the EU. The new sanctions package prohibits EU entities that are "part of the opinion-forming process", including political parties, foundations, alliances, NGOs, think tanks, and media providers in the EU from accepting donations, funding, or other economic benefits or support "from Russia, directly or indirectly"[58]. The EU cites Russia's ongoing propaganda and disinformation campaigns aimed at undermining Ukraine's sovereignty and independence, as well as the war in Ukraine and undue influence on democratic processes in the EU as the cause for this particular restriction. The EU sanctions package defines "direct and indirect" actors vaguely as "Russia and its proxies"[59].

The EU has also implemented a decision it adopted on May 17, 2022, to "suspend the broadcasting activities of additional media outlets in the Union or directed at the Union", including the Kremlin-owned news services and depots RIA Novosti, Izvestia, Rossiskaja Gazeta, and Voice of Europe[60], until "Russian aggression in Ukraine is ended" and Russia "and its affiliated media outlets cease their propaganda activities" in the EU. The EU defines the sanctioned entities as "media under the permanent direct or indirect control of [Russian] leadership" which engages in propaganda activities that "support Russia's war of aggression against Ukraine" and "destroy" countries neighbouring Ukraine. The EU decision notes that the rules apply only to the "broadcasting activities" of the organisations concerned and do not impede journalists from conducting interviews and research in EU Member States.

Since 2022, the EU has suspended the "broadcasting activities and licences" of 18 Kremlin-backed disinformation stations. The EU does not define what constitutes "broadcasting activity" in the EU, but Western media have consistently reported that the EU has blocked access to websites of affected media outlets; search engines and social media sites have also blocked access to sanctioned media organisations as part of the broadcasting ban.

In practice, the EU imposes almost no costs on those using FIMI against its member states for their harmful effects. An example of this is the ability to view Russian websites (e.g., RT or Sputnik) on EU territory, despite EU sanctions on these media. For example, RT has not stopped broadcasting in Germany despite the ban and punitive measures enacted by the German media authority. Likewise, RT France has tried to challenge the EU ban, arguing that the Council had no power to impose such a ban and that it violates the EU Charter of Fundamental Rights. In particular, they argue it violates the right of defence and the right to a fair hearing (Articles 41 and 48), freedom to conduct business (Article 16), and freedom of expression (Article 11). On March 30, 2022, the President of the Court of Justice rejected RT France's application for an urgent preliminary ruling, and on July 27 of that year, the court, acting as a Grand Chamber, dismissed RT France's appeal in its entirety. In its judgment, the court explicitly referred to the European Convention on Human Rights and Article 10; it indicated that Article 11 should be given equal weight within the meaning of Article 52 of Charter 35. The court found that the restriction was proportionate and met the requirements for a restriction of fundamental rights

17 March 2014, ttps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0269, [last access: October 29, 2024].

[58] European Union, *Council Regulation (EU) 2024/1745 of 24 June 2024 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401745 (last access: June 26, 2024), p. 4.

[59] Ibidem.

[60] For more about the malign influence of Voice of Europe, see: Bryjka, F., *Unravelling Russia's Network of Influence Agents in Europe*, PISM Spotlight, No. 24, https://pism.pl/publications/unravelling-russias-network-of-influence-agents-in-europe [last access: April 5, 2024].

in its entirety[61]. These examples prove that the implementation of sanctions mainly depend on political will and the efficiency of the EU Member States's legal systems.

After Russia's full-scale invasion of Ukraine, some countries (e.g., Czechia and Poland) briefly (for about three to six months) maintained blocks on websites spreading pro-Russian propaganda and disinformation. However, national courts found insufficient legal grounds for such measures. In contrast, such measures were effectively taken by the Estonian authorities, which blocked 53 TV channels and 195 websites based on a law prohibiting the promotion of an offensive war[62].

Between 2013–2021, Lithuania and Latvia also blocked access to Russian television channels ten and five times, respectively, predominantly sanctioning violations related to the incitement of hatred or war[63]. The European Commission confirmed that television programmes calling for the aggression and "destruction" of various states constituted war propaganda, which justified the suspension of the broadcasts.[64] These examples demonstrate that national efforts to curb disinformation are highly dependent on the will and determination of the government to counter it. Otherwise, disinformation actors can often circumvent restrictions by using evolving methods, like new servers and proxies, that enable them to spread false and manipulated content.

Conclusion

The EU has significantly increased its situational awareness concerning threats stemming from foreign information manipulation and interference over the past decade, putting forward a common analytical framework and developing a set of tools to counter the problem.

However, the level of implementation of this framework is still low. Moreover, the existing regulatory framework and institutional capacities are still insufficient to effectively protect the information space from malign activity. The Digital Services Act, although groundbreaking in many aspects, will not in itself eradicate online information manipulation. Nor will digital, media, and information literacy programmes make societies immune to all incidents of information manipulation. Foreign actors will continue to find ways to bypass sanctions, and EU citizens will at times be persuaded to believe conspiracy theories. There is no one magic solution to the problem of disinformation.

Nevertheless, the level of harm to the EU's cohesion and public security requires that all tools from the FIMI toolbox be expanded upon and implemented to their full extent by member states.

---

[61]Bayer, J., *The European response to Russian disinformation in the context of the war in Ukraine*, "Hungarian Journal of Legal Studies", 2023, 64 (4), p. 594.

[62] On February 25, 2022, the Estonian Consumer Protection and Technical Supervision Agency banned the rebroadcasting of five TV channels for broadcasting a speech by the President of the Russian Federation that justified military aggression and violated the Media Services Act. The agency continued to monitor and act against channels and websites spreading harmful content. On August 4, 2022, it ordered that four websites promoting war propaganda, supporting crimes of aggression, and inciting hatred be blocked due to their threat against public order. Further measures were taken on May 4, 2023, when Estonia restricted access to 195 websites and 51 TV channels to protect its information space and enforce sanctions. Such actions have been regularly implemented, showcasing Estonia's ongoing commitment to safeguarding its information environment from disinformation.

[63] The domestic media authority based its decisions on Articles 3(4)(a)(i) and 6 of the AVMS Directive, which allow for the suspension of television programmes if they incite hatred on the basis of certain criteria. See: Sten Hansson et al., 'COVID-19 Information Disorder: Six Types of Harmful Information during the Pandemic in Europe', *Journal of Risk Research* 24, no. 3–4 (April 3, 2021): pp. 380–93, https://doi.org/10.1080/13669877.2020.1871058.

[64] J. Bayer, *The European…op.cit.*, p. 592.

Further efforts in coordination, exchange of information, and common action are also needed. To do that, the EU must dedicate far more meaningful financial and human resources than it is currently, and EU Member States need to demonstrate continuous political will in addressing the threat.

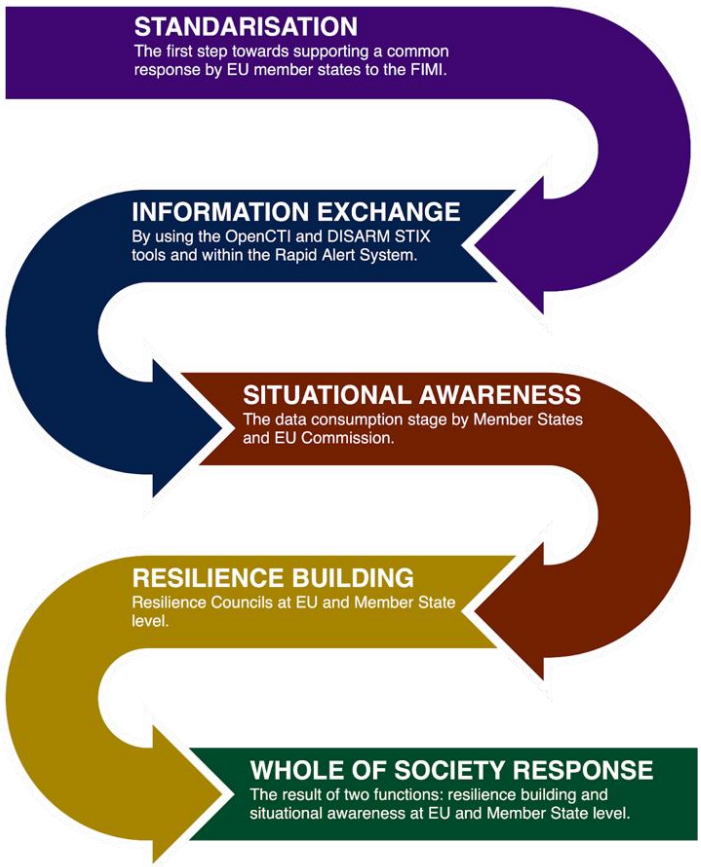
The ineffectiveness of the EU's response system to FIMI is the result of varying degrees of progress by individual EU countries in countering FIMI, different regulations at the national level, a lack of political will to be more proactive, and restrictions related to the protection of freedom of expression. The implementation of the DSA, which is expected to increase the ability of states to influence online platforms to combat and remove illegal content, is expected to help change this.

The low level of standardisation of methods for detecting and analysing FIMI incidents hinders the exchange of information between EU Member States – both by state administrations and NGOs. Member States are currently facing a lack of data that could serve as an initial contribution to the development of national FIMI incident databases and provide a basis for further analytical efforts. It impedes the integration of the data held, which, in turn, slows the response to ongoing operations. For the defenders' community to be able to effectively support their governments, as well as the EU, in terms of collective responses, there is a need for FIMI analysis to be standardised based on the ABCDE, DISARM, and STIX frameworks. Development of a common and standardised framework for FIMI analysis is crucial for a community-driven taxonomy of FIMI TTPs to enable stakeholders systematic and granular data collection on threat actors. This taxonomy needs to be agile, specific, and open source to allow for maximum stakeholder inclusion and widespread adoption. It constitutes the first step toward achieving a *whole-of-society response*.

Every tool in the FIMI Toolbox should and can be expanded upon and further developed. Therefore, it is recommended that the FIMI Toolbox be expanded to include a dataset provided by the EEAS Data Team. This dataset should contain information on state-linked and state-aligned channels that are overtly involved in FIMI operations.

The next step involves facilitating information sharing between Member States and the EEAS through the RAS, which contributes to enhanced situational awareness. Situational awareness is a prerequisite for building societal resilience. The task of strengthening resilience lies with the Resilience Councils at both the EU and national levels, as well as with organizations such as EDMO, EUvsDisinfo, and other civil society actors.

In conclusion, a *whole-of-society response* results from the **interplay of two core functions:** 1) situational awareness and 2) resilience building. These functions are implemented at two levels: the EU level and that of the Member States. **Standardizing information exchange is essential to enabling these functions—this is the primary objective of the SAUFEX project.**



Stages towards developing a whole of society response

Model for information sharing, response and building resilience to FIMI

Part II – STRATEGIES AND POLICIES

This section evaluates how EU Member States incorporate countering FIMI and disinformation in their strategic documents and policy frameworks. It analyses how these countries set out strategic objectives for countering FIMI or disinformation; whether their strategic documents point to specific solutions for responding, building institutional capacity, regulating, and increasing social resilience; or whether they merely characterise the problem. Emphasis is put on countries that have adopted dedicated strategies, sectoral strategies (e.g., cybersecurity strategies), national action plans, and road maps focused on countering FIMI or disinformation.

Review of strategic documents

Strategic documents are used to outline the general direction of a state's policy in specific areas. The most important among these is the national security strategy, which analyses the existing security environment and defines the aspirations of a state resulting from its position and potential. The national security strategy identifies the national interests and strategic objectives of the state, which it seeks to realise in the mid to long-term perspective.

National security strategies therefore act as a general orientation tool for a state's policies, facilitating the definition of specific sectoral objectives and the methods for their implementation. It is from this overarching document that sectoral strategies (e.g., cyber security, defence, military, foreign policy, education, and migration) are derived. In lieu of these, countries sometimes choose to adopt documents that are less conspicuous (e.g., national action plans or road maps) but define objectives that can be achieved in a relatively shorter time frame (i.e., two to five years).

The research conducted for this report identifies only two EU Member States that have adopted or are advanced in the process of adopting strategies specifically dedicated to countering disinformation and FIMI. Nevertheless, the majority of EU states address FIMI threats in their national security strategies (77.7%).

Moreover, a significant share of EU Member States address the topic of countering FIMI in their cybersecurity strategies (88%). The inclusion of this subject matter increased between 2017 and 2024 and was significantly influenced by global events, including Russia's hybrid aggression against Ukraine in 2014, increasing Russian interference in U.S. and European elections (since 2016), disinformation campaigns related to COVID-19, and war propaganda related to Russia's full-scale invasion of Ukraine in 2022.

Only a few member states have thus far neither updated their national security strategies (i.e., Austria, Cyprus, Greece, Italy, and Malta) nor inscribed the threat of disinformation in any other strategic documents.

It should be noted that not all member states included FIMI and disinformation in their cybersecurity strategies and address these threats in their national security strategies.

This is an important observation because cybersecurity strategies are documents that focus primarily on the technical issues of problems occurring in the cyber domain. Challenges identified in these documents may include disinformation campaigns, fake news, and deepfakes, which are viewed as attempts to manipulate and polarise public opinion with the intention of altering perceptions of reality. For example, Germany's Cyber Security Strategy (2021) emphasises the need to protect media companies' websites from cyber-attacks. This

approach indicates that the German authorities identify cyberspace and digital media as a major area of defence against disinformation. Thus, it has chosen to link the countering of these kinds of threats to the country's cyber security. This may limit defence to technical activities related to the defence of information and communication infrastructure against activities identified as part of hostile operations[65].

Table 2: Strategic and policy documents that frame national approaches to countering FIMI

	National Strategy	**Dedicated Strategy**	**Cybersecurity Strategies**	**National Action Plans or Road Maps**	**Other Relevant Documents**
Austria	Austrian Security Strategy (2013) No mention of disinformation.	-	Austrian Cybersecurity Strategy (2021)	Digital Action Plan for Austria: Goals, Guidelines and Principles (2020) Action Plan Deepfake (2022)	Digital Sovereignty for Austria (2023)
Belgium	National Security Strategy (2021)	-	Cybersecurity Strategy for 2021-2025	-	-
Bulgaria	National Security Strategy (2018)	-	National Cyber Security Strategy (2023)	-	Bulgaria-U.S. Memorandum of Understanding on Combating Disinformation
Croatia	National Security Strategy (2017) No mention of disinformation but does mention hybrid threats.	-	The National Cyber Security Strategy (2015) No mention of disinformation.	-	-
Cyprus	-	-	Cyprus Cyber Security	-	-

[65] Bundesministerium des Innern, für Bau und Heimat, *Cybersicherheitsstrategie für Deutschland*, Bundesministerium des Innern 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.html. [last access: September 20, 2024].

			Strategy (2012) No mention of disinformation.		
Czech Republic	National Security Strategy 2023	National Strategy for Countering Hybrid Interference (2021)	Cybersecurity Strategy 2021-2025	Education Policy Strategy	National Defence Strategy (2023)
Denmark	Danish Security and Defence Towards 2035	-	National Strategy for Cyber and Information Security (2022–2024)	Action Plan to Safeguard Danish Democracy and Society (2019)	National Digitalisation Strategy (2022)
Estonia	National Security Policy (2017) National Security Concept of Estonia (2023)	-	Government Cyber Security Strategy (2019-2022) No mention of disinformation.	-	National Defence Development Plan 2031
Finland	Security Strategy for Society (2017) Will be renewed by end of 2024. In March 2024, work began on a national security strategy that will be published by June 2025.	-	Finland's Cyber Security Strategy 2019 Finland's Cyber Security Strategy 2024-2035 (October 2024)	Countering Disinformation – A Guidebook for Communicators on Countering Information Influencing (2019) Media Literacy and National Education Strategy	Government's Defence Report (2021) Government Report on Changes in the Security Environment (2022) Government Programme (2023) Government Report on Finnish Foreign and Security Policy (2024)

France	National Strategic Review (2022)	-	-	-	Report on Information Manipulation (2018) Published by the Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces). Enlightenment in the Digital Age Report (2022)
Germany	National Security Strategy 2023	-	Cyber Security Strategy (2021)	-	-
Greece	-	-	National Cyber Security Strategy (Version 2.0)	-	-
Hungary	National Security Strategy (2021)	-	-	-	-
Ireland	-	In progress.	National Cyber Security Strategy (2019–2024)	-	-
Italy	-	-	National Cyber Security Strategy (2022-2026)	-	-
Latvia	National Security Concept (2023)	-	The Cybersecurity Strategy (2023-2026)	Conceptual Report on the National Strategic Communication and Security of	National Development Plan for 2021-2027

				the Information Space 2023-2027	
Lithuania	National Security Strategy (2021)	-	National Cyber Security Strategy (2018)	-	Procedure for the Coordination of Strategic Communication in the Area of National Security (2020)
Luxembourg	Luxembourg Defence Guidelines 2035	-	National Cybersecurity Strategy IV (2021-2025)	-	-
Malta	-	-	National Cybersecurity Strategy (2023-2026)	-	Malta Information Technology Agency Strategy for 2023-2026 Foreign Policy Strategy (2023)
The Netherlands	Security Strategy for the Kingdom of the Netherlands (2023-2029)	All-Government Strategy for Effectively Combating Disinformation (2022) Government-wide Strategy for Effectively Tackling Disinformation (2019)	Netherlands Cybersecurity Strategy (2022-2028)	Nationwide Response Framework Against State-Sponsored Actors	-

Poland	National Security Strategy (2020)	Drafted Information Security Doctrine (2015) Not adopted.	Cyber Security Strategy 2019-2024	Strategy of State's Digitalization 2024-2035 In progress.	-
Portugal	Strategic Concept of National Defence No mention of disinformation.	-	National Cyberspace Security Strategy 2019-2023	-	-
Romania	National Public Order and Security Strategy 2023 – 2027 National Defence Strategy 2020-2024	National Strategy for Strategic Communication and Combating Disinformation (2020) Not adopted.	National Cyber Strategy for 2022-2027	-	National Strategy in the Field of Artificial Intelligence 2024-2027 U.S.-Romania Memorandum of Understanding to Strengthen Cooperation on Countering FIMI
Slovakia	Security Strategy (2021)	Concept for Combating Hybrid Threats (2018)	National Cyber Security Strategy (2021-2025)	Action Plan for Coordination Against Hybrid Threats 2022-2024 Strategic Communication Concept of the Slovak Republic (2023)	-
Slovenia	National Security Strategy (2020)	-	Cyber Security Strategy (2016) No mention of disinformation.	-	-

Spain	National Security Strategy (2021)	-	Estrategia Nacional de Ciberseguridad (2019) No mention of disinformation.	National Procedure Against Disinformation	-
Sweden	National Security Strategy (2024)	-	National Cyber Security Strategy (2016)	Countering Information Influence Activities: A Handbook for Communicators (2018) The Psychological Defence Agency's Handbook to Recognise and Deal with Disinformation, Misleading Information, and Propaganda (2023)	Total Defence 2021-2025 Government Bill The Swedish Defence Commission Report 2024

Source: Own study.

EU Member States' strategies to counter disinformation and FIMI

Only two EU countries currently have a strategy dedicated to countering disinformation: Latvia[66] and the Netherlands[67]. In Ireland[68], work on a similar strategy is underway.

While several EU countries, particularly in Central and Eastern Europe, address the threat of disinformation and FIMI to a varying degree in their national security strategies and other strategic documents, the Nordic countries have implemented a whole-of-government approach through a series of subsequent documents that approach the problem in a systemic way.

Below is a summary of the existing or planned strategies dedicated to countering disinformation in EU Member States.

The Netherlands

Several Dutch strategic documents provide policy frameworks that contribute to countering disinformation and FIMI. Most notably, these include: The Security Strategy for the Kingdom of the Netherlands (2023-2029)[69], the Netherlands Cybersecurity Strategy (2022-2028)[70], and the Nationwide Response Framework Against State-Sponsored Actors[71]. Notably, the Netherlands is the first country in the EU to have adopted a national strategy specifically dedicated to countering disinformation and FIMI.

The first Government-wide Strategy for Effectively Tackling Disinformation was announced by the Dutch Minister of the Interior and Kingdom Relations in October 2019. The strategy was constructed around three lines of action: prevention, strengthened messaging, and, if necessary, response[72]. However, in recognition of rising disinformation and misinformation, the government published an updated Government-wide Strategy for Effectively Combating Disinformation in December 2022. The new strategy highlights the importance of establishing a set of actions to counter disinformation[73]. In addition to the three lines of action listed in the

---

[66] Cabinet of Ministers of the Republic of Latvia, *The National Concept on Strategic Communication and Security of the Information Space 2023–2027*, 2023, https://www.mk.gov.lv/en/valsts-strategiskas-komunikacijas-un-informativas-telpas-drosibas-koncepcija?utm_source=https%3A%2F%2Fwww.google.com%2F [last access: March 20, 2024].

[67] Ministry of the Interior and Kingdom Relations (of the Netherlands), *Government-wide strategy for effectively tackling disinformation,* 2022, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation [last access: November 23, 2024].

[68] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland), *National Counter Disinformation Strategy Working Group,* 2023, https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group/ [last access: September 30, 2024].

[69] Government of the Netherlands, *Security Strategy for the Kingdom of the Netherlands,* 2023 https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands [last access: April 3, 2024].

[70] Ministry of Justice and Security of the Netherlands/National Cyber Security Centre, *The Netherlands Cybersecurity Strategy 2022-2028,* 2022, https://english.ncsc.nl/publications/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028 [last access: January 31, 2023].

[71] Government of the Netherlands, *Letter to Parliament on tackling state threats and presenting a threat assessment of state actors,* 2022, https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/28/tk-aanpak-statelijke-dreigingen-en-aanbieding-dreigingsbeeld-statelijke-actoren-2 [last access: November 28, 2024].

[72] House of Representatives of the Netherlands, *Policy efforts to protect democracy against disinformation*, 2019, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019D41916&did=2019D41916 [last access: October 18, 2024].

[73] Ministry of the Interior and Kingdom Relations (of the Netherlands), *Government-wide strategy for effectively tackling disinformation,* 2023. https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation [last access: November 23, 2024], p. 5.

previous strategy, two additional actions have been added: strengthening free and open public debate (e.g., by maintaining a pluralistic media landscape and promoting the importance of investigative journalism) and reducing the impact of disinformation (e.g., by raising awareness of disinformation among state institutions).

According to the new Dutch strategy, addressing FIMI fits within the state's broader approach to addressing hybrid threats[74]. Nevertheless, many of the countermeasures envisaged to counter disinformation also serve the purpose of countering FIMI since disinformation is often a key component of FIMI. Acknowledging that disinformation is not disseminated by state actors alone, the strategy points to an increasingly assertive attitude and increased use of information operations and disinformation to serve political interests by foreign state actors. The document references FIMI as a specific risk to national security, as well as the stability and security of international organisations like the EU and NATO.

The Dutch strategy emphasises the primacy of the rule of law, freedom of speech, and freedom of the press and notes that classifying disinformation and fact-checking are not primarily government duties[75].

Recognising that public debate is increasingly conducted on large and internationally operating platforms and that disinformation has become increasingly difficult to discern, the strategy places strong emphasis on stimulating and using public alternatives to online platforms[76].

The strategy places strong emphasis on the importance of implementing and enforcing several EU legislative frameworks - most notably the EU Digital Services Act, the European Media Freedom Act, and the (voluntary) EU Code of Practice on Disinformation. It highlights the role of the government and the coordinated approach of state institutions and agencies to counter disinformation but also recognises that disinformation is a global phenomenon that requires cooperation from a broad and diverse range of stakeholders and transnational networks. It therefore envisages a role for non-state actors, including civil society organisations, researchers, academia, journalists, independent media, and online platforms as stakeholders in awareness raising efforts and other aspects of the strategy's implementation.

Finally, the strategy notes that the Netherlands is committed to developing an effective response, where possible, in collaboration with national and international partners - primarily within the EU context, albeit also within the OECD, NATO and G7 formats. The strategy dedicates considerable attention to the promotion of norms and values within internationally shared standards for tackling disinformation. The Netherlands advocates for an alternative to content control that safeguards human rights and effectively counteracts disinformation campaigns[77].

Latvia

Latvia treats countering FIMI as a part of its defence and deterrence capabilities[78], and the Latvian authorities have taken several actions to strengthen the security of the country and society. Since 2023, the National Security Concept has named disinformation campaigns and the spread of misleading narratives that have the potential to create dissent and conflict within

[74] Ibidem, p. 10.
[75] Ibidem, p. 5.
[76] Ibidem, p. 6.
[77] Ibidem, p. 9, 12.
[78] *The regulation of fact-checking and dinsinformation in the Baltic* States, *Becid* (blog), May 2024, https://becid.eu/results_and_studies/the-regulation-of-fact-checking-and-disinformation-in-the-baltic-states/ [last access: November 29, 2024].

society as key threats to the country[79]. In particular, the concept highlights Russian interference in Latvia's political processes, stating that "the current legal regulation of media activities does not address the current challenges to the security of the Latvian information space". The concept also includes a dedicated paragraph to conducting media policy discussions at the EU level, which calls for requirements for social media companies to prevent the spread of false information, primarily through the European Democracy Action Plan.

Furthermore, the National Development Plan for 2021-2027 recommends strengthening the national information space, preventing disinformation campaigns, and improving media literacy. The plan stresses that "content created in the information space, including the media, helps to sustain democracy and strengthen civic values. Access to high-quality media content in the national language and sufficient and high-quality information about what is happening in society also strengthens us as a society and a democratic country."[80]

The most important guidelines from the Latvian authorities regarding FIMI can be found in the Conceptual Report on the National Strategic Communication and Security of the Information Space 2023-2027[81]. This is a medium-term policy planning document that sets out the national vision and objectives for strengthening information space security, including the development of strategic communication capabilities.

The document defines six main lines of action to strengthen the security of the national information space and put into practice models of coordination and cooperation: 1) the implementation and development of national strategic communication capabilities; 2) measures to make the information space resilient to security threats; 3) strengthening and improving the media environment; 4) creating an engaged and resilient society; 5) partnering with organised civil society, the private sector, and academia; and 6) international cooperation[82].

The concept is complemented with an action plan, which is not publicly available. It is expected that the implementation of solutions provided in the report will strengthen society's sense of belonging to Latvia, Europe, and its values; as a result, citizens' support and trust in government policies and communication will gradually increase.

According to the Latvian government, the most effective way to combat FIMI is through clear and consistent communication by state and local authorities with their target audiences; a strong and high-quality media environment; and a skilled, educated, and engaged public capable of recognizing and resisting manipulation within the information space. Strengthening each of these elements contributes to greater national security. Latvia takes a whole-of-society approach to cyber and information security, considering the weaponisation of large data ecosystems, hard-to-analyse audio and visual content, problematic user behaviour, and evolving media consumption, as well as technological dependence on China. Latvia, like Lithuania, utilizes a

[79] Voltri, J., *Countering Russian Information Influence in the Baltic States: A Comparison of Approaches Adopted in Estonia, Latvia, And Lithuania*, 2022, https://www.kvak.ee/files/2023/01/Sojateadlane-19-2022-Johannes-Voltri-COUNTERING-RUSSIAN-INFORMATION-INFLUENCE-IN-THE-BALTIC-STATES-A-COMPARISON-OF-APPROACHES-ADOPTED-IN-ESTONIA-LATVIA-AND-LITHUANIA.pdf [last access: October 19, 2024], p. 176.

[80] *Par Latvijas Nacionālo attīstības plānu 2021.–2027. gadam (NAP2027), Latvijas Vēstnesis, 127*, 06.07.2020, https://likumi.lv/ta/id/315879-par-latvijas-nacionalo-attistibas-planu-20212027-gadam-nap2027 [last access: October 19, 2024].

[81] *Par Valdības rīcības plānu Deklarācijas par Evikas Siliņas vadītā Ministru kabineta iecerēto darbību īstenošanai, Latvijas Vēstnesis*, 16, January 23, 2024, https://likumi.lv/ta/id/349266-par-valdibas-ricibas-planu-deklaracijas-par-evikas-silinas-vadita-ministru-kabineta-iecereto-darbibu-istenosanai [last access: October 19, 2024].

[82] Ibidem.

blocking strategy. Instead of countering false information by projecting its own version of reality, the state protects its narratives by blocking those of an opponent.

Ireland

In 2020, the Irish government established the Future of the Media Commission and tasked it with developing recommendations for sustainable public funding and other support to ensure the viability and independence of the media in Ireland to meet public service objectives. The commission's report, released in July 2022, contains a total of 50 recommendations that, in effect, constitute a strategic agenda for the transformation of the Irish media sector. One of these recommendations is for the development of a national counter disinformation strategy to enhance trust and protect the safety of Irish users of global content platforms[83].

While the Irish strategy is not yet finalised, a large amount of information can be drawn from publicly available the strategy working group's reports, terms of reference, and citizen scoping paper. The multi-stakeholder working group began its work in February 2023 and operates three subgroups that inform the development of the Irish strategy on: (1) existing countermeasures, (2) the emerging regulatory environment, and (3) supporting journalism and providing public interest information. The working group has shared five guiding principles around which the strategy could be developed[84]:

1) Counter disinformation and protect freedom of speech using a rights-based approach.
2) Counter disinformation by building resilience and trust at individual and societal levels.
3) Counter disinformation through increased cooperation, collaboration, and coordination.
4) Counter disinformation through corporate accountability and regulatory enforcement.
5) Counter disinformation through evidence-based countermeasures and interventions.

The Irish national strategy for countering disinformation aims to enact coordinated efforts with relevant government ministries and agencies to counter campaigns targeting Ireland; develop effective monitoring; and build relationships between different national actors, including researchers and media platforms. The latter would also require supporting fact-checking and disinformation research and independent journalism in countering disinformation, as well as new initiatives in media literacy.

The authors of the Irish strategy put a strong emphasis on conducting public consultations as part of this process. According to the scoping document that formed the basis of a written public consultation, disinformation is a problem "because it is designed to create doubt and disruption. It distorts the nature of public discourse, undermining trust in sources of reliable information and negatively impacting people's ability to make informed decisions based on accurate information."[85]

---

[83] The Future of Media Commission, *Report of the Future of Media Commission*, July 12, 2022, https://www.gov.ie/pdf/?file=https://assets.gov.ie/229731/2f2be30d-d987-40cd-9cfe-aaa885104bc1.pdf#page=null [last access: September 15, 2024], p. 250.

[84] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland), *National Counter Disinformation Strategy Scoping Paper*, https://www.gov.ie/pdf/?file=https://assets.gov.ie/286028/37ceb147-b155-4655-af17-df6189be7928.pdf#page=n [last access: September 16, 2024], p. 10–12.

[85] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland), *National Counter Disinformation Strategy Scoping Paper*, https://www.gov.ie/pdf/?file=https://assets.gov.ie/286028/37ceb147-b155-4655-af17-df6189be7928.pdf#page=n.

The Nordics

None of the Nordic EU Member States - Finland, Sweden or Denmark - have dedicated strategies for countering disinformation or FIMI. However, all three countries have recognised them as a threat to the functioning of democratic societies and have incorporated discussions around disinformation and FIMI in other strategies and policies.

All three countries emphasise a whole-of-government and whole-of-society approach in countering FIMI and disinformation and highlight the importance of civil society in countering threats in the information space. The Danish Security and Defence Towards 2035 sees disinformation as part of a hybrid toolbox aimed at spreading instability and sowing discord in national public discourse within NATO and the EU[86]. The strategy discusses resilience against these threats as part of "societal security", which covers more policy areas than classic military preparedness. Accordingly, this document notes that societal security against hybrid threats is handled nationally through a whole-of-government approach, although the term is not further defined[87].

The 2024 National Security Strategy of Sweden recognises influence campaigns and disinformation as a threat to Swedish democracy. Disinformation and cyber threats are mentioned specifically as a hybrid tool when discussing capacity-building against hybrid threats[88]. Accordingly, managing these threats requires improved situational awareness and decision-making capacity and improved collaboration between different sectors and decision-making levels in society[89]. A similar approach was adopted in the Total Defence 2021-2025 Government Bill in Sweden, which discusses threats of disinformation to democratic society within the framework of hybrid threats and vulnerabilities brought by social and technological development[90].

Similarly, the Finnish government's Defence Report of 2021 notes that Finland's defence increasingly requires preparedness against threats beyond conventional military activity. The report refers to these threats as "broad-spectrum influencing", which includes cyber and information influences[91].

In addition, the 2024 Government Report on Finnish Foreign and Security Policy notes the security challenges that emerging technologies can pose. It specifically mentions the development of AI, cyber-attacks, information influencing, and disinformation, as well as the need to build a national knowledge-base in countering disinformation. Among other measures, it proposes developing information defence, diplomacy, and strategic communication "toolboxes", as well as developing national guidelines for targeted and coherent cyber attribution activities, considering key allies and partners[92].

---

[86] Danish Ministry of Defence, *Danish Security and Defence Towards 2035*, September 2022, https://www.fmn.dk/globalassets/fmn/dokumenter/strategi/rsa/-regeringens_security-policy-report_uk_web-.pdf, [last access: November 29, 2024], p. 20.

[87] Ibidem, p. 20, 71-74.

[88] Government Offices of Sweden/Prime Minister's Office, *National Security Strategy*, July 2024, https://www.government.se/globalassets/government/national-security-strategy.pdf, [last access: November 29, 2024], p. 6, 20, 27, 30,40.

[89] Ibidem, p. 30.

[90] Ibidem, p. 51-52.

[91] The Finnish Government/Valtioneuvosto, *Government's Defence Report/Valtioneuvoston puolustusselonteko*, September 9, 2021, http://urn.fi/URN:ISBN:978-952-383-820-8, [last access: November 29, 2024], p. 18, 23.

[92] The Finnish Government/Valtioneuvosto, *Government Report on Finnish foreign and security policy/Ulko- ja turvallisuuspoliittinen selonteko*, June 20, 2024, https://urn.fi/URN:ISBN:978-952-383-890-1 [last access: November 29, 2024], p. 18, 28.

Denmark also notes the challenge of disinformation and information influencing campaigns in its tech diplomacy and digitalisation strategies. For example, the Ministry of Foreign Affairs' Strategy for Tech Diplomacy Denmark's concept recognises that new technologies may risk undermining international peace and security through "personally targeted disinformation on social media generated by artificial intelligence or future quantum computers capable of breaking existing encryption"[93]. The strategy calls for international partnerships, regulation, and cyber-diplomatic efforts to counter threats in cyberspace, including disinformation campaigns[94]. It also advocates for stronger public-private cooperation, both domestically and internationally, and increased responsibility of tech companies in countering cyberattacks and the spread of misinformation and disinformation on digital platforms[95].

The Finnish Security Strategy for Society from 2017 outlines the comprehensive security concept that serves as the basis for the Finnish whole-of-government and whole-of-society approach to preparedness. Disinformation and information influencing are discussed in connection to cognitive resilience. The strategy highlights the importance of the media in upholding and creating societal resilience and underlines the importance of critical media literacy and basic digital proficiency in countering disinformation. It also notes that enhancing a trustworthy journalism and media environment strengthens civic participation and aids in countering disinformation. Moreover, it notes that effective, trustworthy, well-timed, and well-planned communications are important in trust-building[96].

The Comprehensive Security Concept of Finland from 2018 stresses that the primary defence against information influencing is an educated and media literate society. Media literacy and media education are part of the guiding provisions of the Finnish nationwide education strategy; they have historically been part of education programmes from early childhood education until high school/vocational training and are considered a civic skill[97].

The Swedish approach also emphasises the role of civil society and media actors in countering disinformation and FIMI. The country's Countering Information Influence Activities: A Handbook for Communicators[98] aims to increase public communicators' awareness and understanding of information influence campaigns and develop their ability to respond to them.

The more recent 2023 handbook by the Psychological Defence Agency aims to strengthen the Swedish population's ability to identify and resist foreign influence campaigns. It contains tips and tools for recognising attempts of foreign powers to influence the Swedish population.[99]

---

[93] Ibidem, p. 12.

[94] Ibidem, p. 17, 18, 21.

[95] Ibidem, p. 8, 17, see also Denmark's Ministry of Finance, *Danmarks digitaliseringsstrategi Sammen om den digitale udvikling*, May 2022, https://www.regeringen.dk/media/11324/danmarks-digitaliseringsstrategi-sammen-om-den-digitale-udvikling.pdf [last access: November 29, 2024].

[96] The Finnish Security Committee/Turvallisuuskomitea, *Security Strategy for Society/Yhteiskunnan turvallisuusstrategia - Valtioneuvoston periaatepäätös,* November 2, 2017, https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf [last access: November 29, 2024], p. 14, 23, 32, 89.

[97] Finland's Security Committee/Turvallisuuskomitea. *The Finnish comprehensive security concept/Turvallinen Suomi - Tietoja Suomen kokonaisturvallisuudesta,* October 4, 2018 https://turvallisuuskomitea.fi/turvallinen-suomi-2018-tietoa-suomen-kokonaisturvallisuudesta/ [last access: November 29, 2024], p. 8, 23, 125.

[98] Swedish Civil Contingencies Agency/Swedish Psychological Defence Agency, *Countering information influence activities – A handbook for journalists,* https://mpf.se/download/18.5ed1a83718d2a5fd639d524/1706648817558/countering-information-influence-activities-a-handbook-for-journalists.pdf, [last access: July 26, 2024].

[99] The Psychological Defence Agency, *DON'T BE FOOLED -A handbook to help you recognise and deal with disinformation, misleading information, and propaganda,* 2023,

Sweden has also made recent adjustments to its education system to enhance media literacy, including critical digital literacy and online safety education. These new initiatives aim to increase learning with digital texts, media, and tools; strengthen skills in critical evaluation of sources; and increase students' understanding of the impact of digitalisation on the individual and society[100].

Denmark, like its Nordic counterparts, has multiple other initiatives aimed at increasing young people's media literacy skills and cyber competencies and promoting online safety in the country through formal and informal education[101].

The three countries also recognise that they individually, as well as the EU and NATO, may increasingly become targets of such operations in the future. For example, Finland's 2022 government report on changes in the security environment, which was conducted in response to Russia's full-scale invasion of Ukraine in February 2022, describes new threats in the Finnish security environment, including hybrid and information influencing. It notes that Finland will "strengthen its security" in response as the country prepares to become a target of hybrid influence activities both in the short and long term. The 2023 Government Programme introduced planned measures to counter hybrid threats and strengthen cyber and information security, primarily by investing in education in the field.

Finland revised its Cyber Security Strategy in 2024 in response to the evolving operating environment and in accordance with the Government Programme; however, the strategy reflects a stronger link between the cyber and information domains compared to the two other Nordic countries[102].

The Danish National Strategy for Cyber and Information Security (2022–2024) notes that the security of the cyber and information domains are closely connected: "certain authoritarian states are actively trying to undermine the application of international law in cyberspace and increase control over the internet, while at the same time exploiting the global ICT infrastructure to conduct cyberattacks, influence campaigns, and aggressive cyber espionage"[103] The strategy highlights the importance of international cooperation and equipping citizens and businesses with the tools and skills needed to navigate the digital sphere safely[104]. It foresees several strategic initiatives, including digital literacy measures that equip

https://www.bliintelurad.se/assets/uploads/2024/04/Handbok-Dont-be-fooled-2023-EN-TA_240417.pdf [last access: September 15, 2024].

[100] The European Commission, *Media literacy and safe use of new media – Sweden,* https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/sweden/68-media-literacy-and-safe-use-of-new-media [last access: November 28, 2024]. The Government Offices of Sweden, *Nationell digitaliseringsstrategi för skolväsende/National digitization strategy for schools,* October 19, 2017, https://www.regeringen.se/contentassets/72ff9b9845854d6c8689017999228e53/nationell-digitaliseringsstrategi-for-skolvasendet.pdf [last access: November 28, 2024]; Andric, A., *Sweden – National Digitalisation Strategy for the School System 2023-2027*. The European Union Digital Skills & Jobs Platform, July 24, 2023, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/sweden-national-digitalisation-strategy-school-0 [last access: November 28, 2024].

[101] European Commission, *Denmark: Education and Training Media literacy and safe use of new media,* March 25, 2024, https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/denmark/68-media-literacy-and-safe-use-of-new-media [last access: November 28, 2024].

[102] Finland's Prime Minister's Office, *Finland's Cyber Security Strategy 2024–2035,* October 2024, https://julkaisut.valtioneuvosto.fi/handle/10024/165893 [last access: November 28 , 2024].

[103] Denmark's Agency for Digital Government, *Danish National Strategy for Cyber- and Information Security 2022–2024,* December 2021, https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/strategic-objectives/ [last access: November 29, 2024], p. 33.

[104] Ibidem, p. 5.

children, young people, and adults with skills in digital literacy as well as strengthening society's access to cyber and information security skills through higher education and the allocation of more funding for new initiatives in digital security[105].

While largely focused on the cyber domain, the Swedish Defence Commission's report underlines the importance of systematic work on information and cyber security[106]. It notes synergies between the cyber and information domains, particularly in connection to Russia's methods of cyber warfare and hybrid attacks in connection to the full-scale invasion of Ukraine, as well as the potential threat it poses to Sweden and its allies[107]. The 2016 National Cyber Security Strategy also draws a connection between the cyber domain, disinformation, and influence campaigns and highlights the importance of media and news agencies, training, and the role of international cooperation in counteracting the effects of disinformation and influence campaigns[108].

Czechia and Slovakia

The Czech Republic's approach to countering hybrid threats from Russia shifted following the 2021 identification of the perpetrators of a 2014 subversion operation against an ammunition depot in Vrbětice carried out by Russian military intelligence (GRU) officers[109]. In 2021, the country adopted its National Strategy for Countering Hybrid Interference, which defines objectives and determines instruments essential for the protection of vital, strategic, and other interests of the Czech Republic against hostile hybrid interference. The development of this document was commissioned by the 2016 National Security Audit.
The strategy is based on a systemic, holistic, comprehensive, and whole-of-society approach to assure societal and institutional resilience. It complements the existing system of security policy documents by formulating a comprehensive nationwide policy to counter hybrid interference[110].
The need to counter disinformation is also mentioned in the: 1) Security Strategy of the Czech Republic of June 28, 2023; 2) the Defence Strategy of the Czech Republic of October 4, 2023; 3) the Cybersecurity Strategy 2021-2025, which emphasises the importance of strategic communication; and 4) the Education Policy Strategy, which calls for enhancing media literacy as one of its priorities.

Slovakia is one of the most vulnerable countries in the EU to foreign hostile influence, which is evidenced by various public opinion polls showing high acceptance of Kremlin narratives as well as the use of foreign (mostly Russian) narratives by domestic political actors. While the country's first policies addressing FIMI date back to 2017, their real implementation only began after the full-scale Russian invasion of Ukraine in 2022.

Within Slovakia, there is little in terms of legislation, institutions, and public policies dedicated to combatting FIMI. There is no current effective legislation in place to counter FIMI, and the

[105] Ibidem, p.5, 23-25.
[106] Ibidem, p. 16.
[107] Ibidem, p. 29.
[108] Government Offices of Sweden/The Ministry of Justice, *A national cyber security strategy* (2016/17:213), https://www.government.se/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213, [last access: July 26, 2024], p. 7, 23-24, 26.
[109]Gniazdowski, M., & Wasiuta, M., *Russian attacks in the Czech Republic: domestic context, implications, perspectives, Center for Eastern Studies*, April 20, 2021, https://www.osw.waw.pl/en/publikacje/analyses/2021-04-20/russian-attacks-czech-republic-domestic-context-implications, [last access: June 19, 2024].
[110] This strategy was developed in accordance with the Public Strategy Development Methodology authorised by the Czech Government Resolution No. 71 dated January 28, 2019, see: *National Strategy for Countering Hybrid Interference*, Prague 2021, p. 3, https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/national-strategy---aj-final.pdf [last access: June 19, 2024].

legislative system lacks any definition of the basic terms and concepts related to it. The primary obstacle to implementing effective measures against FIMI and hybrid threats in Slovakia is the current government's denial of their necessity. This resistance stems from the adoption of pro-Russian narratives promoted by disinformation actors, alongside prevailing government views that measures aimed at addressing disinformation are censorship. Without acknowledging the issue, the government lacks motivation to develop or enforce strategies to counter these threats[111].

In 2017, the Slovak government began to develop policies against hybrid threats following the EU's adoption of its first measures within a joint framework the year before. In 2018, Slovakia adopted the Strategy for Combating Hybrid Threats[112], which defined major threats and proposed an initial institutional framework to address them. In 2021, the government approved two crucial strategic documents: 1) the Security Strategy of the Slovak Republic, which identifies disinformation and propaganda as major hybrid threats, including FIMI[113]; and 2) the Defence Strategy of the Slovak Republic, which emphasises the need to strengthen the state's resilience to FIMI and hybrid threats.

These strategic documents proved the government's readiness to focus on active strategic communication and the development of public administration capacities, as well as the strengthening of cooperation between the administration and NGOs, academia, and media to counter disinformation in a systemic way. This would include adopting interministerial and sector-specific systemic measures, including financial ones, to enable NGOs to develop their programmes and capacities.

The adaptation of the Action Plan for Coordinating the Fight Against Hybrid Threats for 2022-2024, which sets up more than 50 specific measures for countering hybrid threats and resilience building, and the realisation of the EU-funded project "Enhancing Slovakia's Resilience to Hybrid Threats by Strengthening Public Administration Capacities*"* allowed the government to create new structures and capacities for addressing hybrid threats and countering FIMI. However, the newly created institutional capacities were not sustained, and after the change of government in September 2023, most of the institutions were disbanded, weakened, or rendered ineffective. Moreover, the new government's updated strategic document on strategic communication to ensure communication between the state and the public, which replaced the 2023 concept, excludes the civic sector from any participation in this area and reduces previous cooperation among ministries to a minimum[114].

Poland and Romania

In the face of increased Russian interference, which has been actively supported by Belarus since 2020, Polish state agencies and civil society organisations have scaled up their capabilities

[111] Zahorjan, D., Haburaj, P., & Milo, D., *Recommendations to future Parliamentarians on responses to FIMI: A selection of case studies – Slovakia*, New Security Threats Institute, September 2024, p. 3.
[112] Úrad vlády Slovenskej republiky, *Návrh Koncepcie pre boj Slovenskej republiky proti hybridným hrozbám*, July 11, 2018, https://rokovania.gov.sk/RVL/Material/23100/1 [last access: November 29, a2024].
[113] The strategy indicates that to counter disinformation, "[…] the Slovak Republic will focus on establishing a coordinated national mechanism for increasing resilience to disinformation and information operations. The aim is to strengthen the structures and decision-making processes of early identification, evaluation, and response to influential and disinformation effects, as well as the implementation of systemic measures. The Slovak Republic will support the development of critical thinking, especially young people, and will use the best practices and recommendations of international organisations, as well as competent non-governmental sector, in the fight against disinformation and propaganda." See: *Security Strategy of the Slovak Republik*, 2021, p. 19, https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf [last access: September 2, 2024].
[114] Zahorjan, D., Haburaj, P., Milo, D., *Recommendations…op.cit.*, p. 3, 8.

and countermeasures. However, a coordinated response at the state level is hindered by the absence of clear guidelines and common situational awareness.

Poland drafted an Information Security Doctrine[115] in 2015, but the document was not approved, and the country still lacks a dedicated strategy for countering FIMI and disinformation. However, these threats are acknowledged in other Polish national strategies. The 2020 National Security Strategy of the Republic of Poland[116] recognises the Russian Federation as a threat actor that undertakes "multi-faceted and comprehensive actions using non-military means (including: cyber-attacks, disinformation) to destabilise the structures of Western states and societies and to create divisions among Allies." It makes clear that the digital revolution "also creates room for disinformation and manipulation of information, which requires effective strategic communication activities"[117].

The strategy calls for the building of capabilities to protect the information space, counteract disinformation, and increase public awareness of threats related to the manipulation of information through education. However, possible threats in the information space are presented superficially, and no concrete solutions in the fight against disinformation are indicated[118]. Experts expect that the next National Security Strategy of the Republic of Poland, which is currently being prepared, will address this shortcoming. The recommendations published by the National Security Bureau on July 4, 2024, include:

- The creation of a strategic communication strategy and development (at the government level) of a trans-sectoral system of integration and coordination of all relevant state institutions.
- The strengthening of instruments for rapid analysis of threat actors' activities.
- The acquisition and implementation of IT, cyber, and information tools (preferably based on AI technology) to build state-level capacity to plan and conduct cognitive actions, including recognition of adversaries' information, psychological, and cyber operation models/infrastructure and TTPs.
- The adaptation of a strategy for countering hostile cognitive activities and building the state's cognitive resilience.
- Amendments in Polish legislation to ensure effective and coordinated protection of the information space[119].

[115] *Projekt Doktryny bezpieczeństwa informacyjnego RP*, Biuro Bezpieczeństwa Narodowego, July 24, 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [last access: November 29, 2024].
[116] Biuro Bezpieczeństwa Narodowego. *The National Security Strategy of the Republic of Poland*, May 12, 2020, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf [last access: November 29, 2024], p. 6.
[117] Ibidem, p. 8.
[118] Berlińska-Wojtas, P., *Bezpieczeństwo informacyjne RP w dobie COVID-19.* Zeszyty Naukowe Zbliżenia Cywilizacyjne XVII (1)/2021, 33–50. https://dx.doi.org/10.21784/ZC.2021.003 [last access: August 28, 2024], p. 42.
[119] *Rekomendacje do Strategii Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, https://www.bbn.gov.pl/ftp/dokumenty/REKOMENDACJE_SBNRP_4_lipca_2024.pdf [last access: July 4, 2024], p. 34-35.

The Cybersecurity Strategy of the Republic of Poland for 2019–2024[120] describes, in detail, FIMI threats as well as risks associated with technological developments and new global challenges. The act also addresses threats related to disinformation and foreign influence in cyberspace by including measures to protect critical infrastructure and counter cyber-attacks, which are often linked to disinformation campaigns.

In Romania, a framework document dedicated to building capacity to counter FIMI – the National Strategy for Strategic Communication and Combating Disinformation – was developed in 2020; however, the document has not been implemented. According to experts involved in the strategy-making process, the document correlates with the policies of both the EU and NATO, and its premise is to strengthen social resilience and protect and maintain a credible and transparent information environment in Romania.

The strategy proposes an inter-institutional approach for generating a coherent public discourse in collaboration with relevant stakeholders. The document distinguishes between two paths of action: proactive, oriented towards promoting democratic values and state policy objectives through narratives and political action; and reactive, according to emerging threats. The document was never published nor subjected to public debate or consultation with civil society[121].

According to experts, the strategy is reportedly unusable due to its incompatibility with existing Romanian legislation. Thus, Romania effectively does not have a national strategy for strategic communication and countering disinformation. While some legislative initiatives have been put forward, unfortunately, none of them have come to fruition[122].

To address this strategic vacuum, the Romanian government approved the National Strategy in the Field of Artificial Intelligence 2024-2027 in July 2024. The strategy describes AI as dual-use technology, increasingly in use as part of hybrid warfare, cyber-attacks, disinformation, and influence operations. It also supports research into the ethical applications of AI tools in addressing societal challenges, including those related to disinformation[123].

France

France currently has no general strategic document dedicated to countering FIMI or disinformation. However, some recommendations, as well as elements of strategy and policy planning, can be found in various documents (i.e., reports, doctrines, and strategic reviews) published under the auspices of the President of the Republic, the Senate, the Ministry of the Armed Forces, and the Ministry of Europe and Foreign Affairs.

In 2018, a report on information manipulation was published by the Policy Planning Staff (Ministry of Europe and Foreign Affairs) and the Institute for Strategic Research (Ministry of

[120] Ministerstwo Cyfryzacji. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [last access: December 30, 2019].

[121] *Is Romania ready to combat disinformation and communicate effectively? Preparedness to identify and counter information manipulation and malign influence in the context of the war in Ukraine*, Global Focus, January 9, 2023, ttps://www.global-focus.eu/wp-content/uploads/2023/01/Is-Romania-ready-to-combat-disinformation-and-communicate-effectively-1.pdf [last access: November 16, 2024], p. 2.

[122] This data comes from an expert interview held on September 11, 2024.

[123] *Strategia națională în domeniul inteligenței artificiale 2024-2027*, 2024, https://www.mcid.gov.ro/wp-content/uploads/2024/02/Strategie-Inteligenta-Artificiala-22012024_clean_final.pdf [last access: November 16, 2024], p. 7, 85, 86, 88, 116.

the Armed Forces)[124]. The report concluded with 50 recommendations directed at: 1) government, 2) civil society, and 3) private actors. Recommendations for the government included: a) avoiding a purely top-down governmental response and opting for a horizontal collaborative approach, relying on civil society; b) creating a dedicated permanent structure within a wider institutional network; c) adopting legislative measures against fake news, reinforcing legislation that punishes online harassment, and making registration compulsory for foreign media; d) investing in international exchange; and e) promoting media literacy in schools. Recommendations for civil society included: a) enhancing fact-checking and using AI and automated language processing; b) developing normative initiatives (rankings, indexes, labels); c) adopting an international charter of journalistic ethics in a collaborative manner; and d) encouraging researchers to intervene in public debates. Finally, its recommendations for private actors included: a) requiring platforms to contribute to the funding of quality journalism and independent research and b) establishing a new contract with users that is founded on new digital rights.

In 2021, President Emmanuel Macron launched the commission *Les Lumières à l'ère numérique* (Enlightenment in the Digital Age), which was chaired by sociologist Gérard Bronner and brought together 14 experts, including historians, political scientists, lawyers, journalists, teachers, sociologists, and civil society representatives to measure and understand the dangers that digital technology poses to national cohesion and democracy. The commission issued a report in January 2022[125] with 30 recommendations, which notably included: 1) supporting and reinforcing scientific research on disinformation; 2) adapting the Open CTI platform for sharing data on disinformation between government, researchers, platforms, and journalists; 3) creating an inter-ministerial digital governance mechanism and developing a digital security culture that includes information risk and involves all state actors; 4) creating a mechanism of crisis management at the EU level to react to massive information operations; 5) creating a co-regulation regime between platforms, regulators, and civil society within the DSA framework; and 6) reviewing all education processes to systemically develop critical thinking.

In 2021, the Ministry of Armed Forces published some elements of the L2I doctrine: *La lutte informatique d'influence*[126]. L2I refers to military operations conducted in the information layer of cyberspace to detect, characterise, and counter attacks; support StratCom; and inform or deceive, independently or in combination with other operations. The Military Programming for 2019-2025 also gives appropriate means to cyber defence, which was further prioritised in the Strategic Review.

The 2022 National Strategic Review upgraded "influence" to a sixth strategic function, including it with "knowledge/appreciation/anticipation","deterrence","protection/resilience","prevention", and "intervention", guaranteeing its prioritisation and funding. The strategic review notes that:

> The aggressiveness shown by our competitors reminds us that nothing can be taken for granted: in addition to our diplomatic, economic, and strategic interests, the new battles

[124] Vilmer, J.B. Jeangène, Escorcia, A., Guillaume, M., & Herrera, J., *Information Manipulation: A Challenge for Our Democracies*, Report by the Policy Planning Staff (CAPS) of the Ministry of Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry of the Armed Forces, Paris, August 2018, ttps://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf [last access: June 16, 2024].

[125] Elysee, Les Lumières à l'ère numérique (January 2022) https://www.elysee.fr/admin/upload/default/0001/12/127ff0d2978ad3ebf10be0881ccf87573fc0ec11.pdf [last access: June 16, 2024].

[126] *La lutte informatique d'influence (L2I)*, https://www.defense.gouv.fr/comcyber/nos-operations/lutte-informatique-dinfluence-l2i [last access: June 16, 2024].

for influence are about our ability to keep the French and European model alive, and to ensure that France's involvement on the international stage is understood and accepted. Inseparable from the other strategic functions described in this review, the influence function must be embodied in a national influence strategy that will set the general framework for action by all the actors concerned, determine the intentions, and provide guidance for the national sectoral and/or geographical strategies. This strategy will aim to: defend France's long-term interests as well as universal values, the application of international law, multilateralism and the preservation of common goods; promote and showcase its commitments in all areas; respond or retaliate to manoeuvres or to attacks against our interests, particularly in the information field.[127]

Selected case studies of other EU Member States

In many EU Member States, disinformation is treated as an element of hybrid threats (e.g., Belgium[128]), cyber security, or both (e.g., the National Security Strategy of Bulgaria[129]). When using the term disinformation, some countries lack any specific conceptualisation, while others use the definition adopted by the EU in 2018 (e.g., Latvia and Estonia[130]) or propose their own conceptual frameworks. Some of these frameworks are overly general, making it impossible to operationalise them.

While it is noteworthy that Lithuania began addressing disinformation long before many other EU countries recognised it as a problem, its revised Public Information Act (2006) required clarification of the concept, defining it originally as "false information that is intentionally disseminated to the public"[131]. The Lithuanian National Security Strategy of 2021 highlighted the intensive digitalisation of all sectors and, consequently, the proliferation of cyber and information threats. These conditions have prompted the Lithuanian authorities to develop institutional capacities for conducting targeted counter disinformation activities to ensure coordinated monitoring, analysis, assessment of the operational information environment, and rapid response to information incidents[132].

In 2020, the Lithuanian government adopted a special procedure for the coordination of strategic communication in national security. It defines how the various state institutions and bodies react to:

- ***Information threats*** – such as war propaganda, incitement to war and hatred, attempts to distort historical memory, and dissemination of other unfounded and misleading information contrary to the national security interests of the Republic of Lithuania. These

[127] SGDSN, National Strategic Review 2022, p. 24. https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022 [last access: June 9, 2024].

[128] Comité stratégique du renseignement et de la sécurité, Stratégie de sécurité nationale, 1 Dec. 2021, p. 19, https://www.egmontinstitute.be/app/uploads/2022/02/NVS_Numerique_FR.pdf [last access: June 9, 2024].

[129] *Aktualizirana strategiâ za nacionalna sigurnost na Republika B"lgariâ*, 23.03.2018, https://www.me.government.bg/files/useruploads/files/akt.strategiq2020.pdf, [last access: July 20, 2024].

[130] *Defending the vote: Estonia creates a network to combat disinformation, 2016–2020*, Global Challenges Election Disinformation, https://successfulsocieties.princeton.edu/sites/g/files/toruqf5601/files/TM_Estonia_Election_FINAL%20edited_JG.pdf [last access: November 29, 2024].

[131] Lietuvos Respublikos Visuomenės Informavimo Įstatymo Pakeitimo Įstatymas, July 11, 2006, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.280580 [last access: November 29, 2024].

[132] Lietuvos Respublikos Seimas, *Dėl Nacionalinio saugumo strategijos patvirtinimo*, December 16, 2021, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/10625df0623a11ecb2fe9975f8a9e52e?jfwid= [last access: November 29, 2024].

are aimed at promoting distrust and discontent with the state and its institutions, democratic system, and national defence; increasing national and cultural divisions; weakening the sense of national identity and citizenship; and attempting to discredit Lithuania's membership in the EU and NATO.

- ***Information incidents*** – one-off information actions carried out by non-EU and/or non-NATO member states or their entities which, through biased public information, are intended to influence the decision-making process related to the national security interests of the Republic of Lithuania. These are not directly related to any other such action.
- ***Continuous information pressure*** – continuous information incidents or a set of information incidents directly related to other information incidents, which are carried out by non-EU and/or non-NATO Member States or their entities and aim to influence the decision-making process related to the national security interests of the Republic of Lithuania through public information[133].

Once an information incident has been identified, an initial assessment is carried out according to defined criteria (see Table 3). The assessment is based on an analysis of the source, content, and context of the information incident. For each criterion, one score is selected to describe the impact, and the scores are totalled. The response can then be adjusted accordingly (see Table 4).

Table 3: Criteria for assessing an information incident

Criteria for an information incident	Assessment of the information incident criterion	Scoring the information incident
1. Source of the information incident. Can be a politician, institution, media outlet, NGO, academic institution, other public opinion forming entity or group of public opinion forming entities or groups of public opinion forming entities, coming from a non-EU and/or non-NATO member state. Through the use of public information	1.1. The source of the information incident does not have the ability to influence decision-making processes related to the national security interests of the Republic of Lithuania by means of public information.	0 points
	1.2. The source of the information incident has the capability to disseminate information to groups or regions of society and may become a potential initial channel for dissemination of information by means of mass media influencing decision-making processes related to the national security interests of the Republic of Lithuania, or it may convincingly imitate such a source.	1 point
	1.3. The source of the information incident has the capability to disseminate information throughout the territory of the Republic of Lithuania and to influence decision-making processes related to the national security interests of the Republic of	2 points

[133] Lietuvos Respublikos Seimo, *Dėl Nacionalinio saugumo strategijos patvirtinimo*, August 26, 2020, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3f019ef4eb8511eab72ddb4a109da1b5?jfwid=2r1mkfzc [last access: November 29, 2024]. p. 1-2.

Criteria for an information incident	Assessment of the information incident criterion	Scoring the information incident
and other means of public opinion forming influence, this entity seeks to influence the decision-making process related to the national security interests of the Republic of Lithuania.	Lithuania by means of public information, or convincingly imitating such a source.	
	1.4. The source of the information incident has the capability to disseminate information in the EU and/or NATO Member States and other neighbouring states of the Republic of Lithuania and to influence decision-making processes related to the national security interests of the Republic of Lithuania by means of public information, or to imitate such a source in a convincing manner.	3 points
	1.5. The source of the information incident has the capability to disseminate information in the EU and/or NATO Member States and other states in the neighbourhood of the Republic of Lithuania and to influence decision-making processes related to the national security interests of the Republic of Lithuania by means of public information, and represents the official position of non-EU and/or non-NATO Member States.	4 points
2. Content of the information incident. This information is provided by the means of public information that affects decision-making processes related to the national security interests of the Republic of Lithuania.	2.1. The content of the information incident disseminated through the media does not influence decision-making processes related to the national security interests of the Republic of Lithuania through the media.	0 points
	2.2. The content of an information incident disseminated by the mass media may influence individual regions, social, or ethnic groups, influencing decision-making processes related to the national security interests of the Republic of Lithuania.	1 point
	2.3. The content of an information incident disseminated through the media may influence the public and decision-makers in the field of national security of the Republic of Lithuania by influencing decision-making processes related to the national security interests of the Republic of Lithuania through the media.	2 points

Criteria for an information incident	Assessment of the information incident criterion	Scoring the information incident
	2.4. The content of the information incident disseminated by means of mass media, by hacking into information systems, and/or changing the content of mass media unrelated to the information incident may influence the public and decision-makers in the field of national security of the Republic of Lithuania, as well as the publics of international partners/foreign countries, by influencing processes of decision-making in the area of the Republic of Lithuania's national security interests.	3 points
3. Context of the information incident. Geopolitical and/or political events and processes related to national security issues of the Republic of Lithuania during which the information incident occurred.	3.1 The context of the information incident is unfavourable to the influence of public information on decision-making processes related to the national security interests of the Republic of Lithuania.	0 points
	3.2 The context of the information incident contributes to the impact of the media on decision-making processes related to the national security interests of the Republic of Lithuania.	1 point
	3.3 The context of the information incident contributes to decision-making processes related to the national security interests of the Republic of Lithuania through the use of public information and may have consequences for threat management and crisis prevention in the near future.	2 points
	3.4 The context of the information incident contributes to the influence of the media on decision-making processes related to the national security interests of the Republic of Lithuania and has clear and dangerous consequences for threat management and crisis prevention.	3 points

Source: Lietuvos Respublikos Seimo, *Dėl Nacionalinio saugumo strategijos patvirtinimo*, August 26, 2020.[134]

[134] Lietuvos Respublikos Seimo, *Dėl Nacionalinio saugumo strategijos patvirtinimo*, August 26, 2020, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3f019ef4eb8511eab72ddb4a109da1b5?jfwid=2r1mkfzc [last access: November 29, 2024]. p. 8.

Table 4: Recommended response based on the threat level of the information incident

No.	**Information incident score**	**Threat level of the information incident**	**Recommended level of response**
1.	Between 9 and 10 points	Level 1 (*high*)	The Prime Minister of the Republic of Lithuania, members of the Government of the Republic of Lithuania.
2.	Between 6 and 8 points	Level 2 (*medium*)	Public authorities or bodies.
3.	Between 3 and 5 points	Level 3 (*low*)	A public information service provider, NGO, higher education institution, or other opinion-forming body is recommended to make a public response.
4.	0 to 2 points	Level 4 (*lowest*)	Information is provided to a public information service provider, NGO, higher education institution, or other opinion-forming body, as appropriate, but is not responded to by means of public information.

Source: Lietuvos Respublikos Seimo, *Dėl Nacionalinio saugumo strategijos patvirtinimo*, August 26, 2020.

The definition framework and response methodology adopted by Lithuania is unique compared to other EU countries' strategy documents, many of which contain terminological blunders. For instance, in relation to issues of information manipulation in the Spanish National Security Strategy (2017), "misinformation campaigns" are mistakenly listed as a threat instead of "disinformation campaigns", despite the fact that the term misinformation refers to the *unintentional* dissemination of false or manipulated information (as opposed to disinformation, which is deliberate).[135] However, this inconsistency was addressed in the Spanish National Security Strategy from 2021, which describes disinformation as one of the main threats for state security.

Germany's Cyber Security Strategy (2021) defines disinformation as "the deliberate dissemination of false or misleading information"[136]. Its strategy highlights the particular threat posed by the dissemination of disinformation through online platforms that have been victim to

[135] The document points out that "misinformation campaigns are not an isolated incident but in fact form part of a planned strategy: the so-called hybrid war, which combines everything from conventional forces to economic pressure and cyberattacks", See: Gonzales, M., *Spain's national security strategy to include risk of disinformation campaigns*, El Pais, December 1, 2017, https://english.elpais.com/elpais/2017/12/01/inenglish/1512122156_659936.html [last access: September 11, 2024].

[136] Bundesministerium des Innern, für Bau und Heimat, *Cybersicherheitsstrategie für Deutschland*, Bundesministerium des Innern 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.html. [last access: September 11, 2024]

cyber-attacks. The document indicates that disinformation activities may be part of broader hybrid operations conducted by foreign states.

In the case of Hungary's National Security Strategy, the word "disinformation" appears only once (i.e., Chapter 5, Paragraph 68). It is notable that the document's emphasis is not placed on external sources of disinformation in Europe but instead on "turning international public opinion against Hungary in an organised and systematic manner". Disinformation is therefore not seen as a threat to state security, but rather, as the authors themselves articulate, an "attempt to restrict Hungary's ability to act"[137]. Given that this is the only strategic document of Hungary in which the concept of disinformation appears and that its interpretation is at odds with the approaches of all other EU countries, it can be concluded that the Hungarian government does not view the issue of information manipulation as a security threat.

As part of the implementation of the National Cyber Security Strategy 2022-2026, Italy plans to implement a national coordination action, consistent with initiatives adopted at the EU level and in synergy with "like-minded countries", to prevent and combat online disinformation[138].

This action aims to use the characteristics of the cyber domain to counter attempts to influence the country's political, economic, and social processes[139].

According to the results of the survey conducted for this report, the existing strategic documents framing policy to counter FIMI are mostly classified by experts as inadequate (50%). Although 31.3% of respondents expressed the opposite view, only 9.3% rated the degree of adequacy as high. A quarter of respondents could not clearly indicate an answer. Similar trends can be observed when it comes to assessing the degree of implementation of the documents in practice. Over half of respondents (53.1%) considered the implementation of these strategies to be low or very low, while less than a quarter (21.8%) assessed their implementation positively.

Conclusions

Due to the relatively recent development of the FIMI framework, most existing national strategy documents use the term "disinformation" and offer no mention of FIMI. This lack of terminological standardisation leads to conceptual confusion, giving rise to the possibility of different interpretations and, consequently, varied approaches and instruments used to counter the threat.

Most EU Member States' strategies do not directly translate into comparable resilience against disinformation. Rather, it seems that in each of these countries, disinformation poses a problem, but in different ways; this, it can be argued, is greatly influenced by the factors specific to each national context. Countries approach disinformation differently as elections, along with the related disinformation content, are largely influenced by national political, economic, and sociocultural specificities. Some forms of disinformation seem to be global, but each country exhibits specific structural factors; strengths and weaknesses within its media system; practices

[137] *Hungary's National Security Strategy*, 2021, https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html [Access: 30.07.2024]; Veress, C., *The Comparison Between the Hungarian and Romanian National Security Strategies*, European Scientific Journal, ESJ, 2022/39, p. 133, 135–139.

[138] Agenzia per la Cybersicurezza Nazionale, *National Cybersecurity Strategy 2022 – 2026: Implementation Plan*, Presidenza del Consiglio dei Ministri 2022, 9, https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza [last access: June 27, 2024].

[139] Agenzia per la Cybersicurezza Nazionale, *National Cybersecurity Strategy 2022 – 2026: Implementation Plan*, Presidenza del Consiglio dei Ministri 2022, 9, https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza, [last access: June 27, 2024].

of media use; and levels of trust in media, which together play a key role in how disinformation is received, perceived, and used.

In the coming years, EU Member States will face new challenges related to the threat of FIMI and disinformation. These challenges will be driven by technological advancements as well as increased geopolitical rivalries. Therefore, EU countries should accelerate the implementation of existing strategic documents and provide strong political support by building nonpartisan consensus in this area.

To effectively protect the information space for open, democratic debate that is free of foreign interference and manipulation, EU Member States will need to dedicate significantly more attention and resources to countering the threat. The EU should assist member states in standardisation efforts and promote best practices, including on coordination with NGOs, the media, and the private sector as well as on maintaining institutional memory and crafting collective response measures.

Part III – INSTITUTIONAL CAPACITY

This section examines the institutional capacity of the European Union Member States in countering FIMI and disinformation. It seeks to analyse and assess: 1) the institutionalisation of coordination systems aimed at countering FIMI within the EU member states; 2) the extent and scope of the use of analytical frameworks and digital tools to identify and monitor FIMI; 3) the types of cooperation between state institutions and NGOs in countering FIMI; and 4) the level of international cooperation and exchange of best institutional practices. This section will focus on the most emblematic national case studies that provide the best illustrations of the patterns and processes under scrutiny.

Institutionalisation of coordination systems in the EU Member States

This section seeks to map the processes and stages of institutionalisation of coordination systems aimed at countering FIMI within EU Member States based on three key variables: a) the **centralised versus decentralised** nature of the coordination system; b) the **government versus ministerial** level of coordination; and c) the existence of a **specialised agency** dedicated to countering FIMI.

These variables combined allow for member states to be designated to one of three broad categories: 1) **Champions** (high levels of institutionalisation); 2) **Aspiring Players** (medium levels of institutionalisation); or 3) **Laggards** (low levels of institutionalisation).

States with a high level of institutionalisation, or champions, have a well-developed and centralised coordination system with a viable government level coordination mechanism and a specialised agency established. This group is thus far represented by only two countries: France and Sweden.

On the other side of the spectrum, states with a low level of institutionalisation, or laggards, possess a very rudimentary coordination mechanism, which is typically, albeit not exclusively, characterised by ministry-level coordination and no specialised agency. Examples of low levels of institutionalisation include small states and/or states with relatively limited administrative capacities, including Bulgaria, Cyprus, Hungary, Luxembourg, Malta, and Romania. Relatively low levels of institutionalisation were also observed in Belgium, Denmark, and Portugal.

States with a medium level of institutionalisation, or aspiring players, possess diverse institutional solutions. They may have either centralised or decentralised coordination systems, with either a government or ministerial level coordination mechanism. Their coordination systems are already well developed, and some of them have experimented with specialised agency solutions. Examples of medium levels of institutionalisation include larger member states like Germany, Italy, Poland, and Spain, as well as the Netherlands and the "eastern flank" states that take Russian threat actors seriously: Czechia, Estonia, Finland, and Lithuania.

It should be noted that this analysis is based on data available in the public domain as well as the subjective perceptions of experts who responded to the research team's survey and participated in interviews. It should further be noted that, due to security concerns and political sensitivities related to the fight against FIMI, not all coordination practices within member state governments are likely to be publicly disclosed.

The centralised versus decentralised nature of the coordination system

When evaluating the institutionalisation of coordination systems aimed at countering FIMI and disinformation, a decentralised system designates responsibilities within various levels of government (i.e., central, regional, local), as well as with non-governmental stakeholders. A centralised system allocates responsibilities predominantly, although not exclusively, within a central structure that features a government-level coordination mechanism and a specialised agency or administrative unit dedicated to monitoring, analysing, and responding to FIMI. This report finds that the vast majority of EU Member States have adopted decentralised coordination systems to fight disinformation and FIMI.

Centralised coordination systems were identified in only Czechia, France, and Sweden.

Decentralised coordination systems with a government-level coordination mechanism were identified in Estonia, Finland, and Lithuania.

Decentralised coordination systems with a ministry-level coordination mechanism were identified in Denmark, Germany, the Netherlands, and Poland.

Rudimentary institutional solutions, which are difficult to assign to any coordination typology at this stage of development, were identified in Bulgaria, Cyprus, Hungary, Luxembourg, Portugal, and Romania. These countries do not have robust coordination systems in place, although they do possess institutions, which are sometimes significant in number (e.g., Romania) and have formal responsibilities in the field of fighting disinformation. In these cases, a leading but not necessarily coordinative role in the field of strategic communication and countering disinformation is typically placed within the ministries of foreign affairs (e.g., Bulgaria, Portugal). Some states also house their solutions within other ministries, including the ministries of justice (e.g., Luxembourg) and the ministries of the interior (e.g., Cyprus).

In some countries, such as Belgium, it is difficult to identify any type of comprehensive institutional system of coordination; rather, according to survey respondents, the state has "various dispersed initiatives that are not coordinated by state institutions". Belgium is a peculiar case of a state with weak federal institutions that is deeply divided along regional and linguistic lines. Local communities' information ecosystems are highly connected to neighbouring countries: France for Wallonia, and the Netherlands for Flanders. This public space fragmentation around linguistic communities has prevented strong national initiatives from emerging[140].

Government versus ministerial level of coordination

A minority of EU Member States have opted for a coordination mechanism placed under the authority of the head of government and/or within their office at the central government level. This is notably the case for France and Sweden (within centralised coordination systems) but also for Finland and Lithuania (within decentralised coordination systems).

In France, the Secretariat General for Defence and National Security, under the direct authority of the Prime Minister, is responsible for countering FIMI at the policy and operational level. This structure also provides the Secretariat for the National Defence and Security Council, chaired by the President of the Republic, which is the leading body for defining France's security and defence policy. Placed at the heart of the executive, the Secretariat General oversees inter-ministerial coordination regarding FIMI. It has three main missions: 1) crisis

[140] Alaphilippe, A., *Disinformation Landscape in Belgium*, EU DisinfoLab, May 2023, https://www.disinfo.eu/wp-content/uploads/2023/05/20230509_BE_DisinfoFS.pdf [last access: June 6, 2024].

monitoring and notification of threats and risks; 2) advising and drafting of executive decisions regarding defence and national security; and 3) operations, notably in the field of vigilance and protection against foreign digital interference (via its technical service VIGINUM).

In Sweden, the Prime Minister's Office coordinates on national security issues. The Crisis Management Coordination Secretariat, under the National Security Adviser, is responsible for monitoring FIMI and bears overarching responsibility for FIMI-related issues within the Swedish Government Offices. The Ministry for Foreign Affairs (MFA) is responsible for countering foreign malign information influence activities within the framework of foreign and security policy. It also has a coordinating role regarding strategic communication aimed at preventing and combating malign information influence and disinformation about Sweden abroad. Finally, the Ministry of Defence is responsible for psychological defence and oversees the Swedish Psychological Defence Agency.

In contrast, Finland's comprehensive security model integrates a decentralised whole-of-government and whole-of-society approach, involving the authorities, businesses, NGOs, and citizens. Government-level coordination is overseen by the Prime Minister's Office, whereas the Government Situation Centre (VNTIKE), and, in particular, the Hybrid Team, manage a whole-of-government hybrid threat assessment cycle. The Preparedness Unit and the Government's Operational Centre, established during the COVID-19 pandemic, manage preparedness coordination[141].

In Lithuania, coordination at the government level is ensured by the National Crisis Management Centre, which operates at the level of the Lithuanian Government Office and was established in January 2023[142]. It employs approximately thirty experts and coordinates the work of ten institutions in responding to FIMI, according to information provided through the expert survey. However, each state institution is responsible for monitoring the information space within their own area of competence. Its experts also assess incidents based on a pre-defined set of criteria and, if needed, report them to the National Crisis Management Centre, which coordinates further communication. The head of the centre is the government's vice-chancellor who has direct access to the prime minister and is involved in coordination and operations as well as strategic decision-making.

Beyond these cases, the majority of EU Member States have allocated their coordination mechanism at the ministerial level. Ministries responsible for coordinating policies aimed at countering FIMI vary, and it is difficult to detect any dominant pattern of convergence at this stage of the institutionalisation process.

In some member states, the leading institution for coordination appears to be the Ministry of Foreign Affairs. This is the case for Poland, which appointed a Plenipotentiary for Countering International Disinformation in May 2024[143]. The plenipotentiary is supported by the Department for Strategic Communications and Countering Foreign Disinformation within the MFA. However, responsibilities related to countering FIMI are also placed within the

[141] Fjäder, C., & Schalin, J. Building resilience to hybrid threats: Best practices in the Nordics. The European Centre of Excellence for Countering Hybrid Threats (HybridCoE). [date published: May 2024] https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf, [last access: June 17, 2024].

[142] Seimas pritarė naujam krizių valdymo ir civilinės saugos modeliui, December 8, 2022, https://lrv.lt/lt/naujienos/seimas-pritare-naujam-kriziu-valdymo-ir-civilines-saugos-modeliui/?fbclid=IwAR3Ks1Idn6VDLM5UYzviZ2TQiVLbs8DvKPNAALAn2IGmrDReyzngGRdygs.

[143] *Tomasz Chłoń pełnomocnikiem Ministra spraw zagranicznych ds. przeciwdziałania dezinformacji międzynarodowej*, https://www.gov.pl/web/dyplomacja/tomasz-chlon-pelnomocnikiem-ministra-spraw-zagranicznych-ds-przeciwdzialania-dezinformacji-miedzynarodowej, [last access: May 14, 2024].

Chancellery of the Prime Minister, the National Security Bureau, the Ministry of Defence, the Cyberspace Defence Forces, the Government Security Centre, the Ministry of Digital Affairs, and various intelligence agencies. Notably, Poland had a brief episode from 2022 to 2023 when a government level coordination mechanism was managed by the Government Plenipotentiary for Security of Information Space[144]. However, this office was dissolved after the change of government in October 2023 due to high levels of politicisation. It was admittedly involved in political campaigning aimed at discrediting the opposition as agents of (domestic) disinformation.

In Germany, the Strategic Communications Plenipotentiary at the Ministry of Foreign Affairs is responsible for combating disinformation at the federal level. An important role is also played by the Inter-Ministerial Working Group on Hybrid Threats (AG Hybrid), the Federal Office for the Protection of the Constitution, and the Operational Communications Centre under the Bundeswehr's Cyber and Information Space Command. Yet, despite several sectoral institutions and cross-sectoral initiatives, the state's lack of central coordination between task forces and departments at the ministerial level remains a significant problem, according to survey respondents.

In the Netherlands, the responsibility for coordinating policy against disinformation is designated to the Minister of Interior and Kingdom Relations; however, each ministry is charged with responding effectively and appropriately when it faces disinformation within its own policy area[145]. In Denmark, coordination is spread across several ministries, with key responsibilities being placed with the Ministry of Defence and the Ministry of Justice[146].

Existence of a specialised agency dedicated to countering FIMI

France and Sweden are the only two EU Member States that have thus far established and made fully operational specialised agencies dedicated exclusively to monitoring, analysing, and responding to FIMI.

VIGINUM (Fr. *Service de vigilance et protection contre les ingérences numériques étrangères*; Eng. Vigilance and Protection Service Against Foreign Digital Interference) is a technical and operation service created in 2021 that is attached to the Secretariat General for Defence and National Security under the authority of the Prime Minister. VIGINUM oversees inter-ministerial coordination at the technical level and is a central part of the French coordination system. This inter-ministerial ecosystem features officials from VIGINUM, the Operational Committee to Combat Information Manipulation (COLMI), the Ministry of Europe and Foreign Affairs (MEAE), the Ministry of the Armed Forces, and the Ministry of the Interior[147]. At the technical level, the VDC-P network (Fr: *Veille, Détection, Caractérisation et Proposition*; Eng: Monitoring, Detection, Characterisation, and Proposal) brings together, under VIGINUM, different administrations with technical capabilities in the fight against information

[144] *Premier powołał Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP*, https://www.gov.pl/web/sluzby-specjalne/premier-powolal-pelnomocnika-rzadu-ds-bezpieczenstwa-przestrzeni-informacyjnej-rp [last access: September 9, 2022].

[145] Ministry of the Interior and Kingdom Relations (of the Netherlands), Government-wide strategy for effectively tackling disinformation, December 23, 2022, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation.

[146] Fjäder, C., Schalin, J., *Building resilience to hybrid threats: Best practices in the Nordics.* The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), May 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf, p. 13, [last access: June 5, 2024].

[147] Charles Thépaut, Deputy Director of Monitoring and Strategy at the Ministry of Europe and Foreign Affairs, Twitter, February 12, 2024, https://x.com/diplocharlie/status/1757158603897626942 [last access: June 5, 2024].

manipulation[148]. VIGINUM has grown from eight people in July 2021[149] and, as of 2024, employs approximately 70 people, most of which work in the Operations Unit as OSINT analysts, geopolitical analysts, and data lab analysts[150].

The Swedish Psychological Defence Agency was established in 2022 and answers to the Ministry of Defence. The agency leads the coordination and development of Sweden's psychological defence in collaboration with public authorities and other stakeholders. Similarly to the French VIGINUM, it is responsible for monitoring only external campaigns; democratic principles forbid the agency from monitoring domestic actors[151]. The agency was established to identify, analyse, and provide support in countering malign information influence and conduct work on preventing, detecting, and counteracting information influence operations. It also aims to strengthen citizens' ability to detect and resist malign influence campaigns and disinformation. It endeavours to achieve this by cooperating with education agencies, municipalities, regions, and civil society organisations[152].

There are also recent developments in other EU member states that point to a nascent diffusion of the use of a specialised agency solution. For instance, in June 2024, the German Federal Government created the Central Office for the Recognition of Foreign Information Manipulation (DE: *Zentralen Stelle zur Erkennung ausländischer Informationsmanipulation)*[153]. It is charged with identifying the methods used by foreign influence campaigns and determining how to detect them at an early stage; it is also tasked with improving the federal government's ability to respond to such threats. The office reports to the Ministry of the Interior and cooperates with the Chancellor's Office, the Ministry of Foreign Affairs, the Ministry of Justice, and the Federal Press Office[154]. Currently, it has 10 staff members, with a target of 20.

Another example of specialised agencies being developed by EU Member States is the Centre on Information Resilience, which was founded in 2022 as a pilot project by the Finnish National Emergence Supply Agency[155]. The project aimed to develop policies and tools to combat malicious information influence operations while acting as a national expertise hub for the authorities, businesses, and citizens. The centre was founded after a preliminary study on

---

[148] ASSEMBLÉE NATIONALE, SÉNAT: RAPPORT PUBLIC FAIT AU NOM DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, June 29, 2023, p. 48 https://www.assemblee-nationale.fr/dyn/16/dossiers/activite_dpr_2022_2023 [last access: June 5, 2024].

[149] Bernigaud, A., Defending the Vote: France Acts to Combat Foreign Disinformation, 2021 – 2022, Innovations for Successful Societies, Trustees of Princeton University, 2023, https://successfulsocieties.princeton.edu/publications/defending-vote-france-acts-combat-foreign-disinformation-2021-%E2%80%93-2022 [last access: June 5, 2024].

[150] Based on an interview with the Deputy Head of the Coordination and Strategy Unit, VIGINUM/ SGDSN conducted in Paris on April 26, 2024.

[151] Giandomenico, J., & Linderstål, H., *Disinformation Landscape in Sweden,* May 2023. https://www.disinfo.eu/wp-content/uploads/2023/05/Sweden_DisinfoFactsheet.pdf, p. 7-8.

[152] Psychological Defence Agency. *Our Mission*, March 15, 2024] https://mpf.se/psychological-defence-agency/about-us/our-mission.

[153] *Deutscher Bundestag - 71. Sitzung*, n.d., https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1022350-1022350.

[154] Deutschlandfunk.de, *Bundesregierung - Stelle gegen ausländische Desinformation inimmt Arbeit auf*, June 17, 2024, https://www.deutschlandfunk.de/stelle-gegen-auslaendische-desinformation-inimmt-arbeit-auf-100.html, [last access: June 20, 2024].

[155] Finnish National Emergency Supply Agency/Huoltovarmuuskeskus. *Finnish National Emergency Supply Agency builds capabilities to counter information influencing/ Huoltovarmuuskeskus rakentaa kykyä torjua informaatiovaikuttamista*, August 17, 2022, https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuskeskus-rakentaa-kykya-torjua-informaatiovaikuttamista#.

information security by the National Emergence Supply Agency revealed significant national deficiencies in information security[156].

Use of digital and analytical tools by state institutions

This subsection seeks to map the use of analytical frameworks, such as DISARM, and digital tools, such as Open CTI, to analyse FIMI across the EU Member States. It should be noted that this exercise is based on data available in the public domain as well as information procured from experts who responded to the survey and participated in interviews. It should further be noted that, due to security concerns and political sensitivities related to the fight against FIMI, operational and technical details of FIMI identification, analysis, and response across the member states' administrations are not necessarily disclosed in public.

An overall observation that emerged from the survey is the disconnect between state, non-governmental, and academic awareness of frameworks employed by their counterparts. Respondents affiliated with member states' public sectors demonstrated knowledge about tools used by state institutions and NGO representatives were well aware of tools used by NGOs; however, neither side demonstrated a strong awareness of the tools used by the other. Respondents affiliated with academia or think-tanks usually possessed little knowledge about tools used by both state institutions and NGOs. Notably, respondents from member states such as Greece, Slovakia, Latvia, Czechia, and Finland were not able to inform our researchers of whether state institutions in their countries use any analytical or digital tools to analyse FIMI. In contrast, respondents from Italy, Malta, and Portugal confidently asserted that such tools are not used by state institutions in their countries.

It should be deduced from the above that knowledge about the usage of tools by governmental or non-governmental actors is scattered and fragmented even at the expert level. A poignant illustration of this problem can be seen within the survey respondents from Poland. Whereas some of the Polish academia and think-tank experts could not answer whether such tools were employed, others pointed out that NGOs utilize the ABCDE framework, while a respondent from the public administration noted that state institutions use the tools DISARM, STIX, and Open CTI.

This indicates a clear need for more comprehensive knowledge sharing and cooperation across sectors and EU Member States.

The following are examples of the usage of analytical and digital tools where there is clear evidence that they are used by state institutions responsible for identifying, analysing, and responding to FIMI.

The French agency VIGINUM is transparent about its working methods related to the identification and analysis of FIMI. Analysts at the agency have used the DISARM analytical framework regularly, and in January 2024, VIGINUM published a doctrine (Version 1.0) related to the usage of STIX (Structured Threat Information Expression) 2.1 and OpenCTI [157], indicating that it is in the early stage of using this toolbox. It is worth noting that VIGINUM

[156] Finnish National Emergency Supply Agency/Huoltovarmuuskeskus, *Countering information influencing - Preliminary report/Informaatiovaikuttamisen torjunta – Esiselvitys*, December 1, 2021, https://www.huoltovarmuuskeskus.fi/files/d601de13993e8873d2d66bf379c35f13309dc42a/hvk-informaatiovaikuttamisen-torjunta-esiselvitys.pdf.

[157] VIGINUM: Capitalisation des campagnes et incidents de manipulation de l'information dans OpenCTI. Doctrine d'utilisation de VIGINUM. Version 1.0 | janvier 2024, https://github.com/VIGINUM-FR/Doctrine-OpenCTI/blob/main/SGDSN_VIGINUM_DoctrineOpenCTI.pdf [last access: June 5, 2024].

has a legal mandate[158] that rigorously defines the scope and type of data it can collect as well as what it can detect and characterise. Its mandate allows it to analyse only information operations that: are executed by a foreign state or foreign non-state actor; involve massive, purposeful, artificial, or automated distribution; feature manifestly inaccurate or misleading content; and constitute an attack on the fundamental interests of the state.

The agency can only use open source information, and it needs individualised authorisation for automated data collection for a maximum of six months; after four months from when it starts the data collection, the rough data must be deleted. Its mandate is so strict that the Scientific and Ethical Council that oversees VIGINUM suggested in its 2023 annual public report that the mandate should be expanded so that it can also monitor smaller platforms of less than five million users[159].

In Lithuania, both state institutions and NGOs use ABCDE, DISARM, Open CTI, and STIX, according to survey respondents. The National Crisis Management Centre within the Lithuanian Government Office first used Open CTI as a pilot project before the NATO summit that took place in Vilnius in July 2023[160].

Similarly, in Ireland, both state institutions and NGOs use DISARM, Open CTI, and STIX. In addition, survey respondents from the business sector reported the use of MITRE ATT&CK, noting that this is a "knowledge base used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community"[161].

Dutch state institutions solely use the DISARM analytical tool, according to survey respondents from the public administration sector. NGOs in Germany use the ABCDE and DISARM frameworks; however, according to a German respondent from the military sector, usage of digital tools and analytical frameworks by state institutions to identify and analyse FIMI constitutes classified information.

In some EU Member States, such as Belgium or Bulgaria, the use of analytical and digital tools appears to be more widespread among NGOs than state institutions. In Bulgaria, NGOs have provided trainings to public administration staff on DISARM, Open CTI, and STIX. These NGOs also use other frameworks and methodologies, according to the International Fact-Checking Network and the European Fact-Checking Standards Network. Survey respondents indicated that the Bulgarian administration also uses the RESIST Counter Disinformation Toolkit[162] developed by the government of the United Kingdom.

---

[158] Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361; Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044454057, [last access: May 14, 2024].

[159] Secrétariat général de la défense et de la sécurité nationale: RAPPORT DU COMITÉ ÉTHIQUE ET SCIENTIFIQUE SUR L'ACTIVITÉ DU SERVICE DE VIGILANCE ET DE PROTECTION CONTRE LES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES (VIGINUM) JUILLET 2021 – DÉCEMBRE 2022, https://www.sgdsn.gouv.fr/files/files/Viginum%20-%20rapport%20CES.pdf, [last access: June 5, 2024].

[160] *Informacinę erdvę NATO viršūnių susitikimo metu stebėjo pirmą kartą Lietuvoje suburta tarpinstitucinė analitikų komanda*, July 14, 2023, https://lrv.lt/lt/naujienos/informacine-erdve-nato-virsuniu-susitikimo-metu-stebejo-pirma-karta-lietuvoje-suburta-tarpinstitucine-analitiku-komanda/, [last access: August 19, 2024].

[161] ATT&CK Matrix for Enterprise, https://attack.mitre.org/, [last access: August 14, 2024].

[162] Government Communication Service, RESIST 2 Counter Disinformation Toolkit, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/, [last access: June 24, 2024].

Cooperation between state institutions and NGOs

This subsection seeks to map the types of cooperation between state administrations and the third sector on countering FIMI in European Union Member States. The authors of this report have identified three types of cooperation between public authorities and NGOs. The first type of cooperation is a **top-down model** in which the state institutions initiate cooperation with civil society stakeholders. This often translates into formalised cooperation formats established by the relevant institutions. The second type of cooperation is a **bottom-up model** initiated by NGOs. The third model is characterised by state actions that are not only **uncooperative** but also constitute active **obstruction** of NGOs' activities aimed at tackling disinformation and FIMI.

This typology has been developed based on case studies of cooperation models in the member states, including data from expert interviews, surveys, and desk research.

Top-down cooperation model

Many European Union Member States seek to use the advisory and consultative role of NGOs for resilience building, developing comprehensive strategies regarding FIMI, and improving strategic communication. The resulting types of cooperations that form are highly dependent on individual considerations within each country. Countering disinformation and foreign interference covers a whole spectrum of activities, and each country has its own approach to the complex problem of FIMI, which determine cooperation with civil society actors.

To strengthen the process of best practices exchange between the public administration and the third sector, states often aim to formalise cooperation with civil society organisations and stakeholders. This process is initiated through orders, and, subsequently, provisions in the statutory documents of state bodies and institutions, which are then translated into **formalised cooperation platforms**. One of this report's observations is the correlation between the establishment of formalised cooperation platforms with civil society organisations and higher levels of state institutionalisation of coordination systems. States that have established such platforms for regular cooperation coordinated by state institutions are Sweden (assessed as a "champion" with a high level of institutionalisation), Finland, Ireland, Italy, Spain, and Poland (assessed as "aspiring players" with medium levels of institutionalisation).

Table 5: Formalised cooperation platforms and their coordinating state institution

Member state	Formalised cooperation platform	Coordinating state institution
Finland	Security Committee	Ministry of Defence
	Knowledge Centre on Information Resilience	National Emergency Supply Agency
Spain	Forum Against Disinformation Campaigns	Department of National Security of the Cabinet of the Presidency of the Government
Sweden	Cooperative Council	Psychological Defence Agency

Member state	Formalised cooperation platform	Coordinating state institution
Poland	Consultative Council on Resilience to International Disinformation	Ministry of Foreign Affairs
Ireland	The Working Group	Department of Tourism, Culture, Arts, Gaeltacht, Sports, and Media
	Media Literacy Ireland	Media Commission
Italy	Technical Table	Communications Regulatory Authority

Source: Own study.

Although France is not included in the table, it also utilizes a top-down cooperation model between its state institutions and NGOs. While no official cooperation platform has been established to date, VIGINUM oversees communication with civil society and academia. This progress began in 2023 after initial service consolidation. In 2023, a conference uniting stakeholders was organised to map relevant actors, and as of 2024, these exchanges are slated to become increasingly focused and concrete.

Finland has established two cooperation platforms. The first is the Security Committee, an independent, permanent cooperative body for which the Ministry of Defence provides a secretariat[163]. The second platform is the Knowledge Centre on Information Resilience within the National Emergency Supply Agency, which has broadened its scope on hybrid threats and informational influence[164].

Poland established the Consultative Council on Resilience to International Disinformation (often referred to as Resilience Council) in September 2024 as an advisory body to the Ministry of Foreign Affairs, the country's leading institution for countering FIMI efforts. It is composed of a chairperson, the Plenipotentiary of the Minister of Foreign Affairs for Countering International Disinformation, his deputy, and representatives of civil society invited by the minister. Experts with knowledge or experience in a specific field may participate in the council's work as advisors. The council meets at least every two months, or more often if

[163]Fjäder, C. & Schalin, J,. *Building resilience to hybrid threats: Best practices in the Nordics.* The European Centre of Excellence for Countering Hybrid Threats (HybridCoE). [date published: May 2024] https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf, p. 18.
The Security Committee of Finland/Turvallisuuskomitea, *Operation and Responsibilities*, https://turvallisuuskomitea.fi/en/security-committee/operation/ [last access: August 2, 2024].

[164] Finnish National Emergency Supply Agency/Huoltovarmuuskeskus, *Countering information influencing - Preliminary report/Informaatiovaikuttamisen torjunta – Esiselvitys*, December 1, 2021, https://www.huoltovarmuuskeskus.fi/files/d601de13993e8873d2d66bf379c35f13309dc42a/hvk-informaatiovaikuttamisen-torjunta-esiselvitys.pdf; Finnish National Emergency Supply Agency/Huoltovarmuuskeskus, *Finnish National Emergency Supply Agency builds capabilities to counter information influencing/ Huoltovarmuuskeskus rakentaa kykyä torjua informaatiovaikuttamista,* August 17,2022] https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuskeskus-rakentaa-kykya-torjua-informaatiovaikuttamista#.

required[165]. The idea for this type of resilience council was championed by the SAUFEX consortium.[166]

The Spanish Forum against Disinformation Campaigns, gathering expertise from different civil society sectors, meets once a year to discuss potential focal areas to address in the next year based on current trends and threats. In December 2022, nine working groups were established that notably dedicated greater attention to foreign interference driven by the 2022 Russian invasion of Ukraine[167].

Italy's Technical Table (It: *Tavolo tecnico*) brings together media representatives, digital platforms, academics, and civil society stakeholders. Work is carried out in four thematic groups: telecommunications and consumers, postal services, media services and digital platforms[168], and big data.

Two patterns can be distinguished based on the type of coordinating state institution employed by states. First, cooperation is often coordinated by institutions that are part of the national security sector (e.g., MFA or MoD). This is the case for the majority of EU Member States and indicates that these countries frame FIMI mainly as a security threat. The second pattern can be observed in Ireland and Italy. In Ireland, greater emphasis is put on the media sector and promoting media literacy. In Italy, the cooperative platform is coordinated by a regulatory institution, which indicates the state is taking a more technical approach to FIMI.

Another form of top-down cooperation is **state funding for research projects regarding disinformation**, which is notably present in Austria, Croatia, and Germany. The central focus of Austria's state-funded research projects are deep fakes. The Federal Ministry of Finance is also responsible for funding research and development initiatives related to security and defence, which includes funding projects that identify and combat disinformation (e.g., the DefalsifAI project[169]). In Croatia, state financing has been provided for universities through a public call by the Ministry of Culture and Media and the Agency for Electronic Media[170]. Germany has pledged to invest in research on the impact of FIMI on democracies as a member of the G7 format. It has also supported the call for researchers to have access to data to better understand the scope, scale, and extent of information manipulation.

---

[165] *Zarządzenie nr 30 Ministra Spraw Zagranicznych w sprawie Rady Konsultacyjnej do spraw Odporności na Dezinformację Międzynarodową przy Ministrze Spraw Zagranicznych*, Warsaw September 11, 2024, https://www.gov.pl/web/dyplomacja/zarzadzenie-nr-30-ministra-spraw-zagranicznych-z-dnia-11-wrzesnia-2024-r-w-sprawie-rady-konsultacyjnej-do-spraw-odpornosci-na-dezinformacje-miedzynarodowa-przy-ministrze-spraw-zagranicznych [last access: October 29, 2024].

[166] For an extensive research report written prior to the presentation of the proposal for the creation and principles of work of the Resilience Council and the normative and organisational process of its formation in Poland, prepared within the framework of the SAUFEX project, see: Chłon, T., Kupiecki, R., *Towards FIMI Resilience Council in Poland. A Research and Progress Report*, https://saufex.eu/research [last access: November 24, 2024].

[167] Vicente, A.R., *Disinformation Landscape in Spain*, EU DisinfoLab, March 2023, https://www.disinfo.eu/wp-content/uploads/2023/03/20230224_SP_DisinfoFS.pdf [last access: October 29, 2024]; *Foro contra las campañas de desinformación en el ámbito de la seguridad nacional*, Trabajos 2023, *Catálogo de publicaciones de la Administración General del Estado*, https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf [last access: November 18, 2024], p. 159.

[168] Example of public consultations on regulations regarding removing malicious online videos: https://web.archive.org/web/20230509160315/ https://www.agcom.it/documents/10179/29559719/Delibera+22-23-CONS/1e92c9c1-53fb-4229-b92a-ca91613a42d4?version=1.0 [last access: October 29, 2024].

[169] Defalsif-AI, Austrian Presse Agentur, https://science.apa.at/project/defalsifai-en/ [last access: October 29, 2024].

[170] Read-Twice-Media-Literacy-Needs-Assessment-CROATIA-v1.pdf [last access: October 29, 2024].

Estonia, Latvia, and Lithuania are examples of small countries that have boosted their institutional capacities by cooperating with various third-sector actors in the field of combating FIMI. Because these are small countries, the community of people and organisations involved in countering disinformation is not sizeable, and experts often know one another other, which has translated into more **informal** but vibrant forms of **cooperation and information exchange**. In Lithuania, NGOs are included in the operational algorithm of intervention of the National Crisis Management Centre (NCMC), which is responsible for strategic communication and response to informational threats. The NCMC recommends NGOs respond to an incident when the threat level is low (i.e., a score of 3-5), according to its ten-point scale[171].

Bottom-up cooperation model

The bottom-up cooperation model is characterised by third-sector stakeholders initiating activities to counter FIMI while state institutions remain passive. Accordingly, no formalised mechanisms and formats exist for cooperation between the public sector and NGOs. The bottom-up model of cooperation can be identified in states with relatively low institutional capacity. These countries often face political and social challenges; as a result, NGOs complement state capacities or compensate for their absence. No formalised and permanent cooperation formats with civil society were identified in countries with low levels of institutionalisation. The states that can be classified as utilizing a bottom-up cooperation model are, *inter alia*, Belgium, Romania, and Bulgaria; in these cases, respondents assessed the level of cooperation between the public and third sector as low.

In particular, NGOs in these countries engage with the public administration by inviting officials to various events, proposing legislative change, conducting trainings for civil servants, promoting analytical and digital tools and frameworks, and sharing best practices. Often, these organisations are part of the EDMO network.

In Belgium, national-level initiatives are scarce due to the country's regional and linguistic fragmentation. However, the *Centre de Crise National* (En: National Crisis Centre) promotes research and tools developed by NGOs. The organisations mentioned include notably EDMO BELUX and DROG.

Despite initiating cooperation, NGO experts from Romania indicate passiveness from state institutions and a lack of collaborative efforts. This has translated further into a lack of effective public debate on how the state should tackle disinformation and conduct strategic communications.

In Bulgaria, protracted political instability has not been conducive to enhancing permanent cooperation and implementing NGOs' recommendations for addressing FIMI. However, Bulgarian NGOs did play a notable role in initiating bilateral cooperation between the U.S. and Bulgarian administrations on matters related to FIMI. Moreover, during organised events, NGOs have enhanced the exchange of practices between Bulgarian government representatives and representatives of institutions such as VIGINUM and the European Commission. The third sector has also promoted the use of DISARM, STIX, and OpenCTI, providing training for government staff.

[171] *955 Dėl Strateginės Komunikacijos Nacionalinio Saugumo Srityje Koordinavimo Tvarkos Aprašo Patvirtinimo*, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3f019ef4eb8511eab72ddb4a109da1b5?jfwid=2r1mkfzc [last access: November 1, 2024].

Non-cooperation (obstruction) model

There is a group of member states in which state institutions and civil society are not only completely decoupled, but the state actively limits the capacities of NGOs in investigating and countering disinformation. This pattern is discernible in Slovakia and particularly in Hungary.

Hungarian civil society organisations that receive funding from foreign sources have been classified by the government as agents of foreign influence. Furthermore, following the adoption of the Sovereignty Protection Act in November 2023[172], the Hungarian government now considers European funds as a foreign source of funding. This law is similar to the Russian Foreign Agents Act, which classifies Western soft power as a threat. Assigning the label of "foreign agent" to independent organisations aims to undermine public trust in them.

Another action being taken by the Hungarian government to limit civil society's capacities in addressing FIMI is its restriction of access to information for independent journalists and NGOs. For example, fees for accessing relevant public information have been increased and state institutions have been granted additional time to provide it[173]. Moreover, the Hungarian government has feigned cooperation with civil society in the area of FIMI by establishing a network of state-controlled GONGOs and institutions, such as the V4 News Agency, which it has branded as independent despite the fact that it is funded by government politicians[174].

International cooperation: exchange of best institutional practices

Bilateral and multilateral international cooperation on countering FIMI allows for the exchange of best institutional practices and enhances mutual capabilities. This often takes the form of creating institutions, which serve as platforms for multilateral cooperation. The authors of this report have identified two types of best practices flows: **a vertical flow (i.e., organisation to state)** and **a horizontal flow (i.e., state to state and organisation to organisation)**.

This analysis is based on open-source data and responses provided by interviewed experts. Due to security concerns and political sensitivities related to FIMI, not all details of international cooperation are public. However, EU Member States' engagement and cooperation in international organisations and with other states reflect their strategic interests, foreign policy goals, and individual considerations, as well as their perceptions of FIMI threat levels.

---

[172] Wiseman, J., & Panyi, S., *MFRR Podcast: Navigating Hungary's new Sovereignty Protection Act*, October 31, 2023, International Press Institute, https://ipi.media/ipimedia/mfrr-podcast-navigating-hungarys-new-sovereignty-protection-act/ [last access: August 2, 2024].

[173] *The Hungarian government further weakens freedom of information and transparency*, DemNet, June 11, 2019, https://demnet.hu/en/blog-en/hungarian-government-further-weakens-transparency/ [last access: September 22, 2024]; Munkacsoport, J., *Hungarian government further weakens access to information*, K-Blog, January 23, 2024, https://k.blog.hu/2024/01/23/hungarian_government_further_weakens_access_to_information?utm_medium=doboz&utm_campaign=bloghu_cimlap&utm_source=nagyvilag [last access: September 22, 2024].

[174] Sarkadi Nagy, M., *London-based V4 Agency is Orbán's propaganda machine disguised as global media product*, Atlatszo.hu, May 25, 2020, https://english.atlatszo.hu/2020/05/25/london-based-v4-agency-is-orbans-propaganda-machine-disguised-as-global-media-product/ [last access: August 1, 2024]; Walker, S., *London media agency carries Viktor Orbán's nativist message*, The Guardian, Budapest, May 5, 2019, https://www.theguardian.com/world/2019/may/05/london-based-media-agency-channels-victor-orban-nativist-message-hungary [last access: August 1, 2024]; Sarkadi Nagy, M., *"International News Agency" informing Hungarians about a declining West from London has actually never left Budapest*, Atlatszo.hu, September 8, 2022, https://english.atlatszo.hu/2022/09/08/international-news-agency-informing-hungarians-about-a-declining-west-from-london-has-actually-never-left-budapest/ [last access: August 1, 2024].

For example, Latvia's diverse modes of international cooperation include the EU, the United Nations (UN), the Council of Europe (CoE), the Organization for Security and Cooperation in Europe (OSCE), and the Organization for Economic Cooperation and Development (OECD), as well as various bilateral and regional formats. Italy, in turn, sees its engagement in countering disinformation within the G7 and the OECD as an opportunity to exert global influence in this field.

Vertical flow of best practices

The vertical flow (i.e., organisation to state***)*** of best practices is understood here as a process where solutions and mechanisms developed within international organisations such as the EU, NATO, and the OECD are transferred to individual countries.

European Union

EU institutions and member states share insights related to disinformation campaigns and coordinate responses through the Rapid Alert System (RAS). In particular, although not exclusively, the EU is viewed as a norm-setter of good practices in the Netherlands, Sweden, Finland, Austria, Poland, France, Romania, Germany, and Estonia. In France, VIGINUM has contributed significantly to expanding pan-European situational awareness by supplementing the RAS database.

The Polish MFA has engaged in international cooperation on countering disinformation through policy making at the EU level, involving the FIMI toolbox, sanctions, proactive media campaigns, and the funding of small-scale projects aimed at countering FIMI. Estonia and Germany also participate in the work of the Task Force on Eastern Strategic Communication of the European External Action Service (EEAS) through the participation of seconded experts.

NATO

Under the NATO umbrella, member states cooperate to enhance their capabilities, notably within the Centres of Excellence (COEs), which have been created and funded at the initiative of individual countries. COEs are international military organisations that train and educate leaders and specialists from NATO member and partner states. Although they are NATO-accredited, they are not part of the NATO Command Structure, nor are they subordinate to any other NATO entity.

The NATO Strategic Communication Centre of Excellence is based in Riga, Latvia and was established in 2014 by Latvia, Estonia, Germany, Italy, Lithuania, Poland, and the United Kingdom, later joined by Sweden, the Netherlands, Finland, Slovakia, Denmark, Hungary, and Spain. It functions as a multi-stakeholder platform supported by international experts with military, government, and academic backgrounds who contribute to the strategic communication capabilities of participating countries[175].

Estonia and Romania have built their counter-FIMI capabilities by actively engaging in cybersecurity cooperation within NATO and the EU. This is reflected in the establishment of the NATO Cooperative Cyber Defence Centre of Excellence and the EU Agency for Large-scale IT Systems (EU-LISA) in Tallinn[176]. Romania relies heavily on cooperation with the EU and NATO; particularly in the area of cybersecurity, Romania has followed the approaches developed by its NATO partners when it comes to countering disinformation. Sweden has also

[175]For more, see: https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5 [last access: November 18, 2024].

[176] For more, see: https://ccdcoe.org/about-us/; https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-operational-management-large-scale-it-systems-area-freedom-security-and_en [last access: November18, 2024].

noted that it sees its newly acquired NATO membership as an important platform for pursuing the issue of disinformation and has highlighted the importance of EU-NATO cooperation in countering hybrid threats[177].

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is an autonomous organisation that possesses the only multilateral framework for the EU and NATO, as well as G7 members, to work and conduct exercises together. The centre's work is planned and coordinated by the Hybrid CoE Secretariat, which is located in Helsinki, Finland. Participation in the centre's activities is open to all EU and NATO countries, and the number of participating states has grown to include 36 countries. It acts as a think tank, provides expert and advisory support, and a provides a platform for sharing experience and information on hybrid threats, including FIMI. The Helsinki centre primarily contributes to situational awareness of both international bodies by providing expertise and training in countering hybrid threats[178].

The OECD

Another relevant cooperation forum is the OECD Information Integrity Hub, which was established in 2022 as a peer-learning platform that enables countries to exchange data and best practices. The initiative is supported by France, Belgium, Finland, Greece, Italy, Lithuania, Luxembourg, the Netherlands, and a few non-EU countries (i.e., Korea, Chile, Colombia, Canada, the UK, the U.S., and Norway). The hub also functions as the Steering Group of the OECD Expert Group on Public Governance Responses to Mis- & Disinformation, which is composed of all OECD member countries[179].

Horizontal flow of best practices

The horizontal flow (i.e., state to state and organisation to organisation) of best practices is understood here as a process in which solutions and mechanisms are exchanged between individual states (i.e., bilateral cooperation) and regional formats (i.e., multilateral cooperation). Notably, the latter may include cooperation within such minilateral formats as the Weimar Triangle, the Lublin Triangle, the Baltics, or the Benelux states.

By sharing their know-how on countering FIMI, more advanced states help to strengthen the capabilities of newcomers to this policy area. The most active players in providing such assistance are the United Kingdom, which exports its strategic communication model, and France, which promotes VIGINUM's institutional and operational model of countering FIMI. The United States also has a framework for cooperation with like-minded countries (see below).

France has acted as an exporter of good practices to countries that seek guidance in building their institutional potential. The VIGINUM's Coordination and Strategy Unit oversees international relations, both bilateral and multilateral, aimed at positioning France as a key actor within the community that fights FIMI. Consultations with VIGINUM experts have been held in Bulgaria and Germany, with the latter following the French model in designing its agency to combat disinformation.

The U.S. Framework to Counter Foreign State Information Manipulation is a format for transatlantic cooperation. It serves as a tool for diplomatic engagement to deepen cooperation

[177] Government Offices of Sweden/Prime Minister's Office, *National Security Strategy*, July 2024, https://www.government.se/globalassets/government/national-security-strategy.pdf, p. 28, 29, [last access: November 20, 2024].
[178] For more, see: https://www.hybridcoe.fi/who-what-and-how/ [last access: November 18, 2024].
[179] OECD Information Integrity Hub, https://www.oecd.org/en/networks/oecd-information-integrity-hub.html [last access: October 24, 2024].

between like-minded partners. In 2024, eight EU member states (i.e., Poland, Bulgaria, Romania, Finland, Estonia, Lithuania, Czechia, and Italy) signed a memorandum of understanding to strengthen cooperation with the United States on countering foreign state information manipulation. Importantly, six of these countries are NATO "eastern flank" states.

Bulgaria is an example of a country that has sought assistance and guidance from partners (notably the U.S. and UK) on developing institutional capacity and formal legal solutions to counter FIMI. State institutions like the MFA and MoD use the British RESIST framework in their work, which has become the base model adopted by the Bulgarian administration. Bulgaria is in the initial phase of building its capacity, and the RESIST toolkit is mostly utilized as a starter model for fledgling countries.

Collaboration in tackling FIMI has intersected across organisations and formats. For example, the European Union cooperates with the G7 in the Rapid Response Mechanism (RRM), which is coordinated by Canada with NATO[180].

In the area of **EU-NATO cooperation**, NATO officials have indicated that coordination remains narrow due to political reasons and a lack of agreement regarding the exchange of classified information. The mandate of the NATO Public Diplomacy Division (NATO PDD) is primarily to carry out the Alliance's public communications around its aims and objectives. Thus, NATO as an organisation is limited in its ability to counter FIMI since most activities in this area fall within the scope of responsibility of its member states.

The exchange of views between the two organisations does not always translate itself into real action and implementation at the national level. However, potential for cooperation between NATO and the EU lies in the standardisation of detection, analysis, and response methods to FIMI and ensuring interoperability[181].

One noteworthy group of countries within the EU are the **G7** members Italy, Germany, and France. These member states host numerous very large online platforms (VLOPs) and search engines (VLOSEs)[182], which plays a significant role in their positions as norm-setters in tackling disinformation. Policy guidelines on a specific topic that are set within the G7 format often have a ripple effect on many other international organisations and institutions. For instance, in 2018, the G7 established the Rapid Response Mechanism (RRM) dedicated to strengthening coordination, analysis, and response to information threats.

This tool is part of the broader G7 Commitment to Defending Democracy from Foreign Threats[183]. Meetings of the RRM Working Groups are held with the participation of representatives of NATO, the EU, the OECD, think tanks, civil society stakeholders,

[180] *Disinformation and Foreign Interference: Speech by High Representative/Vice-President Josep Borrell at the EEAS Conference*, Brussels, January 21, 2024, https://www.eeas.europa.eu/eeas/disinformation-and-foreign-interference-speech-high-representativevice-president-josep-borrell-eeas_en [last access: October 21, 2024].
[181] SAUFEX study visit to NATO Headquarters in Brussels, [last access: April 23, 2024].
[182] Very large online platforms and search engines are those with over 45 million users in the EU. They must comply with the most stringent rules of the DSA.
[183] *Charlevoix Commitment on Defending Democracy from Foreign Threats*, Charlevoix 2018, https://publications.gc.ca/collections/collection_2018/amc-gac/FR5-144-2018-30-eng.pdf [last access: October 23, 2024].

institutions like EDMO, and companies like Google[184]. During Italy's 2024 Presidency of the G7, AI-generated disinformation became a primary topic of consideration[185].

Based on the outlined analysis above, it is evident that countries that have experienced major hybrid attacks in the past are more likely to engage in various international initiatives and cooperation formats to strengthen their security. They see membership in the EU, NATO, and the OECD, as well as bilateral formats, as platforms for pursuing thematic issues, including disinformation. "Trendsetters" in this area include the Baltic states, Finland, Poland, Sweden, and the G7 countries Italy, France, and Germany. However, states that do not feel particularly threatened by FIMI and disinformation tend to follow trends from these international forums. These "follower" countries are, inter alia, Belgium, Romania, and Bulgaria.

The main push factor that has led to increased international cooperation and the boosting of institutional capabilities regarding FIMI has been the Russian Federation's aggressive behaviour in Europe and, in particular, its full-scale invasion of Ukraine. Furthermore, hybrid attacks on the Polish-Belarussian and Lithuanian-Belarussian borders, orchestrated by the Belarussian authorities with Russian support, also provided notable policy triggers for both Poland and Lithuania. In view of the 2023 NATO summit in Vilnius and anticipated hostile actions from Russia, Lithuania made notable efforts to strengthen its FIMI-related capabilities. Some eastern flank countries - most notably Estonia - have a longer history of dealing with Russian orchestrated hybrid threats, starting with cyber-attacks on its critical infrastructure conducted as early as 2007.

Beyond Central and Eastern Europe, the French experience with foreign interference in its 2017 presidential elections, as well as a FIMI campaign directed at the French Army in Mali in 2022, proved vital for both creating an exemplary national-level coordination system and engaging in international cooperation as a best practice exporter. Other countries, which possess relatively limited administrative capacities, such as Romania, have chosen to follow a path already outlined by its NATO allies.

Conclusions

EU Member States' coordination systems aimed at countering FIMI reveal varied levels of institutionalisation. Only two member states (i.e., France and Sweden) can be classified as "champions" in this area, featuring centralised systems of coordination with a government-level coordination mechanism and established specialised agencies responsible for FIMI identification, analysis, and response.

A larger group of "aspiring players" consists of larger member states (i.e., Germany, Italy, Poland, and Spain), as well as smaller Northern and Eastern European states (i.e., Estonia, Finland, and Lithuania) that are subject to direct and repeated attacks by Russian hybrid threats, including FIMI. These states utilize decentralised coordination systems, with either government or ministerial level coordination mechanisms, and only some of them (i.e., Germany and Finland) have begun experimenting with a specialised-agency type of solution.

[184]For example: *G7 Working Group Meeting on disinformation at the Farnesina*, Jult 3, 2024, https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2024/07/riunione-alla-farnesina-del-gruppo-di-lavoro-g7-su-disinformazione/ [last access: October 24, 2024].

[185] De Agostini, L., Catena, B., & Autolitano, S., *Mitigating AI-Generated Disinformation: A Cyber Collaborative Framework for G7 Governance*, Policy Brief, Think7, May 2024, https://think7.org/wp-content/uploads/2024/05/T7it_tf1_pb01.pdf [last access: October 23, 2024].

However, many states across the EU, referred to as "laggards", continue to be characterised by low levels of institutionalisation, featuring only rudimentary decentralised coordination systems with coordination mechanisms that are either non-existent or at the sectoral level. Low levels of institutionalisation tend to correlate with states that are smaller, have limited administrative capacities, and perceive low levels of threats from FIMI.

Accordingly, there is limited evidence of the use of analytical frameworks, such as DISARM, and digital tools, like STIX and Open CTI, across EU Member States' institutions. This could be the result of limited use of these tools as well as less public access to information due to security concerns and political sensitivities. France, known as an institutionalisation "champion", is a rare example of a member state that is both an advanced and transparent user of these tools and frameworks. Based on the analysis conducted, it is evident that there is a need for more information and best practice sharing in this respect, both between member states and state institutions and civil society.

Three models of cooperation of state institutions with civil society organisations were identified in this analysis: a top-down cooperation model, a bottom-up cooperation model, and a non-cooperation model. The top-down model, with its formalised cooperative platforms (i.e., Finland, Ireland, Italy, Poland, Spain, and Sweden), correlates with a medium to high level of institutionalisation of coordination systems. Meanwhile, bottom-up (i.e., Belgium, Bulgaria, and Romania) and non-cooperation (Hungary) models correlate with low levels of institutionalisation of coordination systems.

When evaluating the international exchange of best institutional practices, a correlation was identified between active engagement in international cooperation and previous experience with major hybrid attacks, including FIMI. Two types of flows of best practices on countering FIMI were identified: a vertical flow (i.e., organisation to state) and a horizontal flow (i.e., state to state or organisation to organisation).

The vertical flow was notably identified within the EU, the OECD, and NATO. The horizontal flows were observed within EU Member States with medium to high levels of institutionalisation of coordination systems (i.e., France) or former member states (i.e., the United Kingdom) that act as trendsetters and exporters of best practices.

In addition, non-EU allies, such as the U.S., have created their own tools of multilateral engagement aimed at cooperating with EU and NATO eastern flank members. Meanwhile, states that have not experienced major hybrid attacks and/or states with relatively limited administrative capacities, and thus low levels of institutionalisation of coordination systems, tend to act as followers and importers of best practices. Horizontal flows were also identified between international organisations and formats, most notably being the EU and NATO as well as the EU and the G7.

Part IV – REGULATIONS

This section of the report examines how foreign information manipulation and interference is regulated across EU Member States. It also assesses the extent of state legal involvement in addressing FIMI, categorising legislative approaches that range from the absence of dedicated regulations to comprehensive FIMI-specific legislation. This analysis is complemented by a comparative legal review, exploring how each EU Member State addresses FIMI, with particular attention to the areas of public order, national security, and public health. It then evaluates legislation that governs the media and internet (particularly through the context of the EU Digital Services Act) as well as criminal codes to understand their effectiveness in preventing FIMI and aligning with national security and public order frameworks. Finally, this section examines and assesses the overall impact of FIMI regulations, identifying best practices and gaps in implementation.

Models of FIMI regulations

No European Union Member State currently possesses specific legislation directed at addressing FIMI. Instead, states make use of various criminal codes that are legally applicable to prevent and combat disinformation (e.g., defamation, insult, misleading a public institution or public promotion of fascism and hate speech, hooliganism). Given the EU countries' different legal cultures, research carried out as part of the SAUFEX project shows that regulations utilized in the fight against FIMI depend on the model of state intervention in the information sphere.

Through analysis of legal regulations used to combat disinformation in EU Member States, four levels of legislative interference can be distinguished. The lowest level of regulation, or the **minimal** interference model that is mainly represented by Luxembourg, is characterised by a deliberate abandonment of dedicated legislation, instead opting to wait and adopt relevant European regulations[186]. Luxembourgian law notably does not define information manipulation or external interference[187]. A similar lack of legislation can be observed in Czechia, where attempts at regulation have failed due to the lack of adequate legal frameworks, which has been confirmed by the country's court system.

The model of **moderate** interference utilizes **the existing legal framework** without creating specific legislation and can be observed in several member states. Austria, for example, has adapted its current media regulations and rectification mechanisms, while Portugal has introduced legislation under the Charter on Human Rights in the Digital Age but refrained from defining specific sanctions for the spread of disinformation. Denmark, which can also be classified as possessing a moderate interference model, has regulated the issue through a ban on political advertisements on television and a media liability regime. The Netherlands' approach is characterised by a particular focus on regulating political advertising through a voluntary code of conduct (NL: *Gedragscode Transparantie Online Politieke Advertenties*). The model observed in Austria, Belgium, and Italy is primarily based on classic instruments of criminal (e.g., defamation, incitement to hatred) and media law, supplemented by mechanisms to control online content. Finland also does possess national legislation that is specifically dedicated to combatting disinformation or FIMI, relying more on media education and existing laws.

[186] Hénin, N. & Sessa, M.G., *Disinformation Landscape in Luxembourg*, op. Cit.
[187] Belgium – Luxembourg Digital Media and Disinformation Observatory, Regulating disinformation: look-up on the legal framework in Luxembourg, op. cit.

The **significant** interference model can be used to characterise the approaches of Germany and France. Germany's NetzDG law requires social media platforms to remove illegal content within 24 hours of notification[188], while France's ARCOM has broad coordination powers and can impose fines of up to six percent of platforms' global turnover[189]. Furthermore, French regulations for the pre-election period allow for a rapid response to disinformation.

The most **intense** interference model can be observed in the Baltic States and Poland, due in large part to their geopolitical location and historical experience. Lithuania has criminalised social media manipulation with a penalty of up to five years in prison[190], and Latvia has adopted similar measures in the context of elections and deepfake technology. Poland has introduced the harshest penalties - a minimum of eight years of imprisonment for disinformation carried out on behalf of foreign intelligence.

In this context, Cyprus presents a notable case study. Its existing legislation (i.e., Article 50 of the Penal Code) criminalises the classic offence of publishing false news, focusing on intent to cause fear and public alarm, which is punishable by a fine and up to two years of imprisonment[191]. A key element in prosecuting this offence relies on the offender's awareness of the falsity of the information, as they must "knows or have reason to believe it to be false"; this makes it difficult to penalise the distribution of existing false content. A new law that was slated to be adopted in September 2024 was expected to explicitly criminalise "fake news" with a penalty of up to five years of imprisonment[192].

EU Member States' legislation

Based on analysis of the 2022 Strengthened Code of Practice on Disinformation and the European Commission Guidance on Strengthening the Code of Practice on Disinformation, **six key regulatory variables in countering disinformation can be distinguished**:

1. The existence of dedicated legislation that directly addresses disinformation, underpinning the legal framework in this area.

2. The implementation of the EU Digital Services Act (DSA), which introduces binding legal obligations for online platforms and establishes a co-regulatory framework.
3. Regulation of political advertising, which is crucial for the transparency of democratic processes and against the manipulation of public opinion.

---

[188] *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)*, https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Hasskriminalitaet/20220721_NetzDG.pdf?__blob=publicationFile&v=2, [last access: September 2, 2024].

[189] Blocman, A., *Platform regulation and DSA implementation: ARCOM and European Commission Increase Cooperation*, IRIS Legal Observations of the European Audiovisual Observatory, https://merlin.obs.coe.int/article/9903.

[190] *Anyone who, by manipulating the accounts of an online social networking service platform, significantly increased the dissemination of information aimed at acting against the Republic of Lithuania [...] shall be liable to [...] imprisonment for up to five years*.

[191] Cyprus Criminal Code, https://www.cylaw.org/nomoi/arith/CAP154.pdf, [last access: July 14, 2024], p. 27; European Regulators Group for Audiovisual Media Services (ERGA), *Notions of disinformation and related concepts (ERGA Report)*, 2021, https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf, [last access: July 14, 2024], p. 33, 69.

[192] Cyprus Mail. *Freedom of speech objection to fake news criminalisation push*, July 4, 2024, https://cyprus-mail.com/2024/07/04/freedom-of-speech-objection-to-fake-news-criminalisation-push/ [last access: July 14, 2024]; Verfassungsblog, *Prison for Fake News: A Proposal to Criminalize Fake News in Cyprus*, July 12, 2024, https://verfassungsblog.de/prison-for-fake-news/ [last access: June 14, 2024].

4. A legal framework for researchers and fact-checkers to access data, which is important for monitoring and analysing disinformation phenomena.

5. Oversight and enforcement mechanisms that ensure the effectiveness of adopted regulations.

6. Criminal legislation on disinformation, which is a deterrent and sanctioning element.

These variables form a comprehensive regulatory framework to assess the degree of development of legal instruments in individual EU Member States to counter disinformation.

Table 6: Implementing the EU Code of Conduct on Disinformation

State	Dedicated Legislation	Political Advertising Regulation	Criminal Provisions	Media Authority	DSA Coordinator	Other Key Authorities
Austria	No, but has relevant provisions in its Media Act	Yes, through the Media Act	Yes (§§ 105f StGB and others)	Komm Austria	Komm Austria	Federal Communications Senate (Appeals body)
Belgium	No	Yes, through its general media law	Yes, through its general criminal law	CSA (Fr.), VRM (Fl.)	FPS Economy (Planned)	Intelligence Services Review Committee
Bulgaria	No	Limited	No specific provisions	Council for Electronic Media (CEM)	Communications Regulation Commission (CRC)	-
Croatia	No	Yes, through its media law	Limited	Agency for Electronic Media (AEM)	HAKOM	-
Cyprus	Planned for 2024	Limited	Yes (Article 50 the Penal Code)	Cyprus Radiotelevision Authority	Cyprus Radiotelevision Authority	-
Czech Republic	No	Limited	No specific provisions	RRTV	Czech Telecommunication Office	-

State	Dedicated Legislation	Political Advertising Regulation	Criminal Provisions	Media Authority	DSA Coordinator	Other Key Authorities
Denmark	No	Yes[193]	Yes (§108 Criminal Code)	Radio and Television Board	Danish Business Authority	Media Liability Board
Estonia	No	Yes, through its general media law	Yes (§280 Criminal Code)	CPTRA	CPTRA	-
Finland	No	Yes	Yes (Criminal Code)	TRAFICOM	TRAFICOM	-
France	Yes (Law 2018-1202)	Yes, comprehensive	Yes	ARCOM	ARCOM	VIGINUM (Foreign digital interference)
Germany	Yes (NetzDG)	Yes	Yes (StGB)	The Media Authorities (DE: *die medienanstalten*)[194]	Federal Network Agency (BNetzA)	Federal Office for Information Security, Central Office for the Recognition of Foreign Information Manipulation (ZEAM)
Greece	No	Limited	Limited	NCRTV	EETT	-
Hungary	No	Limited	Yes (Criminal Code)	NMHH	NMHH	-
Ireland	Yes (Online Safety Act 2022)	Yes (Electoral Reform Act 2022)	Limited	Coimisiún na Meán	Coimisiún na Meán	Electoral Commission
Italy	No	Yes, through AGCOM guidelines[195]	Yes (Article 656)	AGCOM	AGCOM	Agenzia per la Cybersicurez

[193] Danish law interprets "political" in a broader sense than just party politics; it refers also to campaigning for the purposes of influencing legislation or executive action by local or national (including foreign) governments.

[194] The central supervisory authorities for the regulation of private broadcasting and telemedia in Germany is made up of 14 separate offices of the German States. See: https://www.die-medienanstalten.de/, [last access: June 27, 2024].

[195] Autorità per le Garanzie nelle Comunicazioni, *Comunicato stampa 16 novembre 2017*, November 16, 2017, https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-16-novembre-2017, p. 2-3. Autorità per le Garanzie nelle Comunicazioni, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018*, January 31, 2018, https://www.agcom.it/node/11720, [last access: June 27, 2024].

State	Dedicated Legislation	Political Advertising Regulation	Criminal Provisions	Media Authority	DSA Coordinator	Other Key Authorities
						za Nazionale ACN
Latvia	No	Limited	Yes (Article 231)	NEPLP	Consumer Rights Protection Centre	-
Lithuania	Yes	Yes	Yes (Article 285)	LRTK	RRT	Strategic Communication Department
Luxembourg	No	No	No	ALIA	Competition Authority	-
Malta	No	Limited	Yes (Article 82)	Broadcasting Authority	MCA	-
Netherlands	No	Yes, comprehensive	Yes (Criminal Code)	CvdM	ACM	-
Poland	No	Limited	Yes (Article 130(9))	KRRiT	UKE (Planned)	Internal Security Agency
Portugal	Yes (Law 27/2021)	Limited	No	ERC	ANACOM	-
Romania	No	Limited	Yes (Article 404)	CNA	ANCOM	-
Slovakia	Act on Cyber Security No. 69/2018Coll Act on Military Intelligence No. 500/2022 Coll. Amendment to Act No. 110/2004 Coll. on the Functioning	Limited	Limited, Article 133 of the Criminal Code No. 300/2005 Coll.	Committee on Culture and Media	Council for Media Services	-

State	Dedicated Legislation	Political Advertising Regulation	Criminal Provisions	Media Authority	DSA Coordinator	Other Key Authorities
	of the Security Council					
Slovenia	N/A	N/A	N/A	AKOS	AKOS	-
Spain	Yes (PCM/1030/2020)	Yes	Indirect provisions	CNMC	No data available	Permanent Commission Against Disinformation
Sweden	No	Yes, comprehensive	Yes (Criminal Code)	MPRT	Post and Telecom Authority	Swedish Psychological Defence Agency

Source: Audiovisual Regulators, European Commission[196].

A comparison of legal regulation against disinformation in EU Member States reveals a significant variance in legislative approaches. Dedicated legislation exists in several countries: France (Law No. 2018-1202), Spain (PCM/1030/2020), Portugal (Law 27/2021), Ireland (Online Safety and Media Regulation Act 2022) and Germany (NetzDG), while most countries rely on adaptations of existing criminal and media laws.

The implementation of the DSA is in various stages of implementation, with an important part of the solutions already implemented in France, including the ability of ARCOM to levy penalties of up to six percent of online platforms' global turnover for noncompliance. Regulation of political advertising is particularly developed in Denmark, which has banned political advertisements on television, as well as Sweden and the Netherlands (i.e., Gedragscode Transparantie Online Politieke Advertenties).

In terms of criminal legislation, the most comprehensive regulations exist in Austria (§§ 105f StGB, and others); the Baltic States, including new legislation passed in 2024 by Lithuania and Latvia on, inter alia, deep fakes; and Poland (Art. 130(9) of the Criminal Code on Disinformation in Cooperation with Foreign Intelligence). This analysis suggests significant variations in approaches to the regulation of disinformation between EU Member States, ranging from comprehensive legal solutions to piecemeal provisions.

Different types of regulation in EU countries seek to target manipulation of information, disinformation, fake news, deepfakes, and hate speech more directly. States define the need to combat FIMI in various ways, addressing concerns such as the protection of public order, national security, individual or institutional reputation, constitutional order, sovereignty, territorial integrity, defence capabilities, economic stability, public health, and personal rights that impact human dignity.

However, a lack of clear definitions and specific regulatory frameworks for FIMI complicate efforts to effectively address the issue. Without a precise legal delineation, it becomes

[196] Audiovisual Regulators, European Commission**,** https://digital-strategy.ec.europa.eu/en/policies/audiovisual-regulators [last access: November 10, 2024]; Digital Services Coordinators, European Commission, https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs [last access: November 10, 2024].

challenging to identify and address actions that constitute manipulation or interference. At the same time, penalising FIMI-related activities under existing laws proves difficult, as many fall under the ambiguous umbrella of "non-illegal behaviour". This creates a grey area where certain harmful actions escape accountability, undermining efforts to ensure robust safeguards against such threats.

Table 7: Dedicated regulations to fight FIMI

Stated reasons for fighting with FIMI	Example countries	Criminal law examples
Public order, public peace, public confidence	Italy, Estonia, Latvia, Malta, Greece, and Hungary	**Malta:** "Maliciously spread false news which is likely to alarm public opinion or disturb public good order or the public peace or to create a commotion among the public or among certain classes of the public is considered an offence with the possibility of a three-month sentence" (Article 82 of Malta's Criminal Code).
State or national security	Romania, Italy, Estonia, Latvia, and Poland	**Poland:** "Whoever, taking part in the activities of a foreign intelligence service or acting on its behalf, conducts disinformation, consisting in disseminating false or misleading information" (Article 130(9) of the Penal Code Poland). **Estonia:** §280 specifies that knowingly providing false information to an administrative authority is punishable by a fine of up to 300 Euros or by detention. If the act is committed to obtain official documents, gain rights, or be released from obligations, and does not meet the criteria for offenses outlined in §§209-213 of the Code, it is punishable by a pecuniary punishment or up to two years' imprisonment. For legal persons, such acts are punishable by fines of up to 2,000 euros or a pecuniary punishment (Penal Code, Estonia).
Individual or institutional reputation	Italy	**Italy:** Publishing or spreading false, exaggerated, or tendentious news that may threaten public order (Article 656 the Criminal Code), and defamation, which can be used in cases of spreading false information damaging to the reputation of individuals or institutions (Article 595 the Criminal Code).
Constitutional order, sovereignty, territorial integrity, defence, or economic power	Lithuania	**Lithuania:** "Anyone who, by manipulating the accounts of an online social networking service platform, significantly increased the dissemination of information aimed at acting against the Republic of Lithuania—its constitutional order, sovereignty, territorial integrity, defence, or economic power, shall be liable to a fine or a restriction of liberty, or to arrest, or to imprisonment for up to five years" (Article 118) (Since 2024, Criminal Code).

Stated reasons for fighting with FIMI	Example countries	Criminal law examples
Personal rights that impair a natural person in their human dignity	Austria	**Austria:** The Criminal Code §§ 105f: (severe) coercion; § 107: dangerous threats; § 144: extortion; §§ 146ff: fraud; § 148a: fraudulent data misuse; § 107c: continuous harassment via telecommunication or computer system ("cyberbullying"); §§ 297: slander; § 126a: data damage; § 225a: data falsification; § 293: evidence tampering; § 263: deception in an election or referendum; and § 264: dissemination of false news in an election or referendum.

Source: Own study.

The Dutch strategy acknowledges that more clarity is needed regarding the government's role in respect of illegal and harmful material[197]. Article 134 of the Criminal Code encompasses distribution offenses and states: "Any person who distributes, publicly displays, or posts written matter or an image, in which the provision of information, opportunity, or means to commit any criminal offense is offered, or has such in store to be distributed, publicly displayed, or posted, shall be liable to a term of imprisonment not exceeding three months or a fine of the second category."[198] Article 138ab addresses the topic of computer trespass: "Any person who intentionally and unlawfully gains entry to a computerised device or system or apart thereof shall be guilty of computer trespass and shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category." The trespass may be executed by breach of a security measure, a technical intervention, means of false signals or a false key, or assuming a false identity. Also, a computer trespass committed via a public telecommunication network shall be a punishable offense. Hate speech laws and regulations prohibit libel and slander, incitement to hatred, and sedition and defamation (Articles 113, 119, 137, 261, and 262 of the Criminal Code)[199].

In Estonia, the legal framework concerning FIMI and its consequences are governed by two key provisions: subsection 6 of §12 of the Public Health Act and §§263 and 278 of the Penal Code. Subsection 6 of §12 of the Public Health Act prohibits the dissemination of information that could be harmful to human health or the environment by any person or entity[200]. This was particularly relevant during the COVID-19 pandemic, with entities like Elvis Brauer's MEM Cafe being penalised for not adhering to safety measures[201].

In August 2023, Poland introduced new legislation targeting foreign intelligence-linked disinformation. An amendment made to the Penal Code punishes the spread of disinformation

[197] van Hoboken, J., et.al. *The Legal Framework on the Dissemination of Disinformation through Internet Services and the Regulation of Political Advertising,* The University of Amsterdam, 2019.

[198] The Criminal Code of the Netherlands [translated], October 1, 2012, https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Netherlands-Criminal-Code.pdf, p. 81, [last access: November 12, 2024].
The Criminal Code of the Netherlands in Dutch, July 14, 2024, https://wetten.overheid.nl/BWBR0001854/2024-07-01 [last access: November 10, 2024].

[199] Ibidem.

[200] *The Regulation on Fact-checking and Disinformation in the Baltic States*, *Becid* (blog), May 2024, https://becid.eu/results_and_studies/the-regulation-of-fact-checking-and-disinformation-in-the-baltic-states/, [last access: November 10, 2024].

[201] Henry-Laur, A., *Defiant café ordered to close doors*, December 1, 2021, https://news.postimees.ee/7398387/defiant-cafe-ordered-to-close-doors [last access: November 10, 2024].

in collaboration with foreign intelligence with a minimum sentence of eight years in prison[202]. Article 130(9) aims to prevent serious disruptions in Poland's system or economy and dissuade foreign agents and collaborators from such activities. However, concerns have emerged that the broad definition of disinformation might lead to investigations against journalists and NGOs suspected of foreign ties[203].

In Hungary, the absence of political will to counteract disinformation has resulted in a lack of a legal framework related to FIMI. According to expert survey respondents, the only regulations that have been adopted by state institutions to counter FIMI are non-binding recommendations. These have been ineffective given their lack of enforcement mechanisms like criminal proceedings, financial penalties, or blocking of internet domains and accounts.

In the Hungarian legal system, there is no general prohibition on the disclosure of untruths. In its interpretations and judgments, the Constitutional Court has indirectly formulated the media's obligation to "tell the truth". It has imposed on the legislator the obligation to create the conditions for objective and truthful information when designing the framework within which the media system operates. The constitutional and civil code provisions on the dissemination of untruths mainly concern the context of defamation and freedom of expression[204]. The Criminal Code also refers to slander as "false publication orally or in any other way tending to harm a person's reputation in connection with his professional activity, public office, or public activity; or libellous, before the public at large". Moreover, according to the Criminal Code, false information and untrue statements are punishable if they violate public order or disturb the public peace (Scaremongering and Threat of Public Endangerment)[205].

When evaluating the European legal landscape in the fight against disinformation, one key factor is the varying pace and extent of members' implementation of EU regulations. While some countries, such as Luxembourg, have deliberately withheld the creation of their own regulations while waiting for European solutions, others are actively working to develop national legal mechanisms.

From the centralised French model that is centred around ARCOM and its broad powers to countries with more dispersed systems, like in Belgium, differences in approach to institutional oversight are particularly evident. A clear trend in the evolution of legislation to counter new technological threats can also be observed; examples include Latvian legislation on deepfakes in the electoral context and Lithuanian regulation on the manipulation of social media accounts.

Significant differences can also be seen in approaches to enforcement, from the restrictive German model (NetzDG) requiring removal of illegal content within 24 hours, to softer solutions in other countries. Also noteworthy is the development of specialised institutions such as the Swedish Psychological Defence Agency, the French VIGINUM dealing with foreign digital interference, and the German Central Office for the Recognition of Foreign Information Manipulation (ZEAM); these institutions are indicative of a growing professionalisation in the approach to combating disinformation.

---

[202] Kancelaria Sejmu, *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 grudnia 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy*, Kodeks karny (Dz. U. 2024 poz. 17).

[203] Wahl, T., *Rule of Law Developments in Poland:* May-October 2023, Eucrim, https://eucrim.eu/news/rule-of-law-developments-in-poland-may-october-2023/ [last access: November 10, 2024].

[204] Polyák, G., *Freedom of Speech and the Regulation of Fake News in Hungary: A Legal Fight against State-Generated Disinformation? [in:] Freedom of speech and the regulation of fake news,* Intersentia, Cambridge, 2023.

[205] *Act C of 2012 on the Criminal Code*, 2012, Section 227, Section 337/1, Section 338, https://www.refworld.org/legal/legislation/natlegbod/2012/en/78046 [last access: August 1, 2024].

Regulation of the media and internet (DSA)

The most common practices in regulating FIMI utilize legislation that covers the media, the internet (i.e., Poland, Estonia, Ireland, Germany, Cyprus, Belgium, Romania, Austria, Italy, the Netherlands, Luxemburg, Spain, Portugal, and France), and advertising (i.e., Latvia, the Netherlands, Portugal, and France).

For example, in Spain, Article 10 of the General Audiovisual Communication Law (2022) states that all media and media organisations shall "take measures for the acquisition and development of media literacy skills in all sectors of society, for citizens of all ages and for all media, and will regularly assess progress made" aiming to "enable citizens (…) to use the media effectively and safely, to access and critically analyse information, to discern between fact and opinion, to recognise fake news and disinformation processes, and to create audiovisual content responsibly and safely"[206]. This regulation provides a legal mechanism that holds media organisations (partially) responsible for developing media literacy skills among Spanish citizens.

In Estonia, amendments to the Media Services Act, which came into effect on March 9, 2022, impose obligations on video-sharing platforms to remove content inciting hatred, violence, or discrimination as well as content depicting child pornography; this legislative change has contributed indirectly to combatting against disinformation[207].

In Latvia, the Electronic Mass Media Law restricts foreign media that undermines national integrity. The Latvian authorities used this provision to ban Russian TV channels following Russia's full-scale invasion of Ukraine. Article 26 of the law prohibits content such as pornography, violence, calls for war, and content endangering public health, which was used during the COVID-19 pandemic to issue fines for false claims about the virus. Article 24(4) of the Latvian legislation mandates that the media report facts fairly, objectively, and neutrally, separating opinions from news. And while this provision aims to combat propaganda, it also risks state interference in journalistic content. In 2023, the National Electronic Mass Media Council fined TVnet for not challenging an interviewee's controversial statement, which raised concerns about state overreach in defining journalistic standards.

At the EU regulatory level, the Digital Services Act (DSA) and its implementation are having a notable impact on countries efforts to combat FIMI. Implementing **the DSA**[208] introduces a certain level of harmonisation in terms of administrative sanctions and obligations of digital platforms. Under the act, member states designate various bodies as DSA coordinators, ranging from media regulators to electronic communications authorities; these bodies should be awarded the power to impose a penalty of up to six percent of online platforms' global turnover for DSA violations. Notably, France's ARCOM already has such powers. While the legislation aims to harmonise state efforts, the role of digital services coordinator within EU Member States differ in their scope of competence; this directly impacts their ability to implement regulations and act in accordance with the DSA, particularly in the context of combating FIMI.

Some DSA coordinators deal exclusively with telecommunications (e.g., UKE in Poland), while others combine media and telecommunications supervision (e.g., AGCOM in Italy, ARCOM in France). Some also have broader competences covering competition protection

[206] Presentation titled "Media Literacy in Practice in Spain and Portugal", Iberifier, November 16, 2022, Cidadania e desinformação, [last access: August 1, 2024].
[207] *Media Services Act*, https://www.riigiteataja.ee/en/eli/511012019003/consolide [last access: August 1, 2024].
[208] *European Board for Digital Services*, https://digital-strategy.ec.europa.eu/en/policies/dsa-board [last access: August 1, 2024].

(e.g., CNMC in Spain), consumer protection (e.g., PTAC in Latvia), postal services (e.g., BIPT in Belgium), and transport (e.g., TRAFICOM in Finland).

Furthermore, not all authorities have the same regulatory powers. They can be divided into several categories:

Authorities with full regulatory powers in the area of media and content: These include ARCOM (France), which has specific powers to combat disinformation and can impose penalties on online platforms[209]; AGCOM (Italy), which has a dedicated disinformation monitoring team[210] and Technical Table[211]; and CNAM (Ireland), which oversees the implementation of the Digital Services Act, including disinformation issues.

Regulators with partial competence to combat FIMI: These include the CSA (Belgium), which can act in case of disinformation in audiovisual media, and CRTA (Cyprus), which is limited to traditional media.

The varied technical resources and competences of national authorities have resulted in different approaches to DSA enforcement in disinformation and digital services.

In terms of competences related to combating FIMI, there are also important differences between national DSA coordinators. Thus far, telecommunications authorities (e.g., the Polish UKE, the Swedish PTS) and authorities focused on infrastructure and the protection of competition rules (e.g., the German BNETZA) have not been assigned such competences. In other countries, telecommunications agencies share these competences with other actors through a co-regulation model recommended by the DSA. For example, the Austrian KommAustria and Spanish CNMC work with digital platforms and fact-checkers and have a clearly defined role in the broader strategy to counter disinformation.

In terms of the scope of content supervision, regulators like the French ARCOM or Italian AGCOM have broad powers of direct intervention, while other bodies like the Polish UKE or Swedish PTS are limited to monitoring and reporting functions. Between these two poles are regulators like the Belgian CSA or the Spanish CNMC, which can make recommendations and have limited intervention powers.

Enforcement tools also differ significantly. While ARCOM (France) and CNAM (Ireland) can impose significant financial penalties and demand the immediate removal of content, the competences of other bodies, such as TRAFICOM (Finland) or ANACOM (Portugal), are mainly limited to data collection and analysis. The field of action of regulators also varies, with some bodies, such as Hungary's NMHH or Austria's KommAustria, having comprehensive powers covering both traditional media, online platforms, and social media. Others, such as Germany's BNETZA, focus mainly on traditional media and their associated telecommunications infrastructure. These differences in powers, competences, and regulatory

[209] Blocman, A., *Platform regulation and DSA implementation: ARCOM an European Commission incrase cooperation*, IRIS Legal Observations of the European Audiovisual Observatory, https://merlin.obs.coe.int/article/9903 [last access: August 1, 2024].

[210] The monitoring team works within the Department of Economics and Statistics, https://web.archive.org/web/20200820140058/https://www.agcom.it/documents/10179/18199220/Documento+generico+01-04-2020/47636882-2d30-42dd-945d-ffc6597e685f?version=1.0 [last access: August 1, 2024].

[211] *Tavolo tecnico*, which involves broadcasters, digital platforms, academics, etc. https://www.agcom.it/tavolo-tecnico-07-giugno-2024, [last access: June 27, 2024]. Example of public consultations on regulations regarding removing malicious online videos: https://web.archive.org/web/20230509160315/; https://www.agcom.it/documents/10179/29559719/Delibera+22-23-CONS/1e92c9c1-53fb-4229-b92a-ca91613a42d4?version=1.0 [last access: August 1, 2024].

tools have led to a varied scope, manner, and effectiveness of interventions in the media space related to countering disinformation.

The competence of regulators regularly adapts to EU regulations like the DSA and the Digital Markets Act (DMA) as well as the evolving challenges of disinformation. However, significant differences in the competences and powers of national regulators have directly impacted the way in which these regulators have implemented EU regulations in combating disinformation.

ARCOM (France) and CNAM (Ireland) represent a centralised model that consists of a single authority with broad powers that coincide with the expectations of the DSA, including the ability to impose penalties on digital platforms and respond directly to disinformation incidents.

In contrast, the distributed model, seen in the case of Germany's BNETZA or Poland's UKE, is characterised by a division of powers between different institutions, often leading to prolonged decision-making and potential enforcement gaps.

The hybrid model, represented by Spain's CNMC or Italy's AGCOM, combines different competences in a single institution, maintaining flexibility to respond to new challenges. The Belgian system with CSA and IBPT shows how the division of competences can lead to the need for close cooperation between authorities. This differentiation between member states has resulted in an uneven ability to combat disinformation in the EU. While ARCOM can impose significant fines and demand immediate removal of content, regulators like Hungary's NMHH or Slovenia's AKOS have limited ability to intervene directly, despite being governed by a common legal framework under the DSA.

Despite significant variances, this heterogeneous implementation does not necessarily undermined the effectiveness of a pan-European strategy against FIMI. National implementations should be monitored and their translation into national capacities to counter FIMI should be evaluated. In the event that national actors differ notably in their effectiveness in responding to the same types of attacks, the resulting clarification of such incidents translated into further regulation may help strengthen European information resilience.

Effectiveness of legal instruments to combat disinformation in EU countries

Within the EU, the implementation of regulations to combat FIMI is still in its early stages. In Latvia, spreading false information can be prosecuted under laws like Article 321 (hooliganism) and Article 157 (defamation). According to SAUFEX's expert survey, those regulations have thus far proven "rather adequate". Article 231 of the Latvian Criminal Law also prohibits actions "expressed in obvious disrespect for the public or in dishonesty, ignoring generally accepted behavioural norms," which include activities involved in disseminating knowingly false content or information that hinders the "peace of the people, institutions, or companies".

In 2021, Latvia became the first Baltic State to convict an individual for spreading false information online about the COVID-19 pandemic. The court sentenced him to seven months in prison for hooliganism and incitement to ethnic hatred. In 2024, amendments to the Latvian Criminal Code introduced criminal liability for influencing elections with deep fake technology, which is punishable by up to five years of imprisonment for using such technology to spread false information about political parties or candidates. It "outlaw[s] the use of manipulated social media accounts to disseminate information aimed at harming the constitutional order, territorial integrity, defence, or other interests of the state" (Article 90).

When analysing the practical effectiveness of legal instruments in the fight against disinformation, several Austrian and German cases that have come before law enforcement

authorities or courts in recent years are worth examination. These cases illustrate varied forms of disinformation, from personal defamation to false reports of crimes, to disinformation related to public health in the context of the COVID-19 pandemic. Despite the existence of various legal provisions that are potentially applicable to disinformation cases, successfully prosecuting and convicting perpetrators has proven difficult in practice. Most cases do not go to trial or are settled out of court through, for example, settlements or fines. The cases presented below also illustrate the practical challenges of enforcement within the digital environment.

Table 8: Selected criminal cases related to disinformation in Austria and Germany

Case	Subject	Legal Basis	Verdict
Ignaz Bearth case (2019)	Facebook post with fake quote attributed to politician about a murder case in Freiburg	§ 188 German Criminal Code (Defamation of persons in political life)	Convicted, fined 90 daily rates of €30
Eva Glawischnig case #1	Facebook post claiming political party demanded "sex with minors from age 12"	§ 111 StGB (Defamation)	German user sentenced to two months suspended sentence and €300 compensation
Eva Glawischnig case #2	False health claims about cancer and dementia	§ 264 StGB (Spreading false news during elections)	Complaint filed, no trial mentioned
Innsbruck police officer case (2021)	Facebook post with a photo alleging police misconduct at an anti-COVID-19 restrictions protest	§ 111 StGB (Defamation)	Multiple trials against people who shared the post
Dr. Nashat Kirbaa case	WhatsApp voice message claiming patient deaths and vaccine injuries (COVID-19)	§ 111 StGB (Defamation); § 152 StGB (Kreditschädigung)	Perpetrator identified, further proceedings not known
Kickl v. Rosam case (2021-2023)	Allegations that a prominent anti-vaccine politician received a secret COVID-19 vaccination	Civil case for defamation	Kickl lost when courts ruled that the statement was protected speech
Michael O. case	Fake quote attributed to Eva Glawischnig about refugees	§ 111 StGB (Defamation)	Acquitted after court ruled it was legitimate political satire
Gil Ofarim Case (2021-2023)	False claim of antisemitic discrimination at Leipzig hotel	Defamation and false accusation (German Criminal Code)	Case dismissed after guilty plea and €10,000 fine payment
Duisburg Case (2016)	Blog post about fictional rapes and	Incitement to hatred (§130	Convicted

	kidnappings of schoolgirls by refugees	German Criminal Code)	
Dominik Nepp Case	Statement blaming asylum seekers for rising COVID-19 cases in Vienna, using the term "asylum seeker virus"	Incitement to hatred	Charged, no information on verdict available
Lageso Case (Berlin, 2016)	False report about Syrian refugee's death at health and social affairs office	Faking a criminal offense (§145d German Criminal Code)	No criminal proceedings initiated
Tennengau Case (Austria)	False report about COVID-19 case in community	Landzwang (§275 Austrian Criminal Code) Causing fear and distress to the public or to a large group of persons by threatening an attack on life, health, physical integrity, liberty, or property.	Police report filed, likely unsuccessful due to the lack of a threat element
Kaiserslautern Case (2020)	False online report about coronavirus case	Faking a common danger	Two perpetrators identified, no information on verdict provided
Case against Facebook (Modamani)	False accusations linking Syrian refugee to Berlin Christmas market attack and other crimes through photo manipulations	Civil case against Facebook for content removal	Injunction request rejected by Würzburg District Court

Source: Ritter, S.,*"Die Verbreitung von Desinformation im Lichte des österreichischen Strafrechts"*, Master Thesis University of Vienna, Vienna 2024, pp. 40, 66-68, 70-72, 76-77, 105, 114-115, 124-127.

The problem with implementation does not lie in the lack of appropriate legal tools but in the fundamental difficulties of proving responsibility for disinformation, identifying perpetrators in the digital environment, and the risk that an overly restrictive approach may paradoxically reinforce public distrust and conspiracy theories. Examples from Austria, including its experience with §276 of the Austrian Penal Code[212], or challenges in enforcing the liability of

[212] §276 of the Austrian Criminal Code (repealed in 2015) - a provision criminalising the *dissemination of false and disturbing rumours*, has not led to any conviction in 20 years. Sabina Ritter used this case as an argument against the creation of dedicated criminal laws to combat disinformation due to their practical ineffectiveness while risking excessive interference with freedom of expression. Ritter, S.,*"Die Verbreitung von Desinformation im*

social media platforms, illustrate the limitations of a legal sanctions approach. Some countries suggest that instead of creating new legal mechanisms, greater focus should be dedicated to strengthening societies' resilience to disinformation through media education, fostering professional journalism, and increasing the transparency of digital platforms. In the context of FIMI, it may be more effective to combine existing legal instruments with diplomatic, technical, and educational efforts than to create new regulations.

The effectiveness of enforcing the adopted regulations thus far has also varied. In Italy, according to an expert interviewed by the SAUFEX team, there has not been a single indictment for spreading disinformation, and in many other countries, regulations remain dead. In Malta, Article 82 of the Criminal Code forbids spreading false information and provides for a three-month prison sentence for "maliciously spreading false news which is likely to alarm public opinion or disturb public good order". Some countries, such as Portugal, have taken a more general approach. The Charter on Human Rights in the Digital Age defines disinformation as "any narrative that is demonstrably false or misleading created, presented, and disseminated for economic advantage or to deliberately mislead the public"; however, these provisions have not yet translated into criminal regulation.

In terms of regulatory trends, an increase in the importance of deepfake legislation is evident, as demonstrated by the example of Latvia, which in 2024 passed a law that assigns criminal liability for influencing elections with deep fake technology and is punishable by up to five years of imprisonment. Increased attention is also being paid to the protection of electoral processes, as reflected in French legislation (e.g., Law no. 2018-1202), which aims to protect democracy against false information that could distort the integrity of a vote.

The diversity of regulatory approaches reflects differences in priorities, legal traditions, geopolitical contexts, and perceptions of disinformation threats among EU Member States. At the same time, the common legal framework being developed at the EU level, particularly in the form of the DSA, aims to develop a more unified approach to combating disinformation in the digital space. From this, there is a clear variation in the approach of member states to the regulation of countering disinformation. This analysis allows the identification of several distinctive models of regulatory interference.

Conclusion

The EU addresses FIMI through a broad mix of administrative, civil, and criminal laws aimed at regulating information content. No EU member state has enacted specific legislation to directly target FIMI; so, the issue is managed through indirect regulations on media, internet activities, and advertising. Although constitutional protections for freedom of expression and the right to information exist, they are not effective in combating disinformation due to a lack of legal instruments for practical enforcement; furthermore, they do not adequately address modern realities.

Broad legal tools against disinformation include laws on defamation, incitement to hatred, and hooliganism, among others, and individual EU countries utilize such legislation through varied approaches. In Latvia, laws on hooliganism and defamation have been used to prosecute disinformation, with recent amendments penalising the use of deepfake technology to influence elections. Estonia's legal framework targets disinformation that endangers public health, and Poland recently introduced legislation with severe penalties for disinformation linked to foreign

Lichte des österreichischen Strafrechts", Master Thesis University of Vienna, Vienna 2024, pp. 128, 141, 145-147.

intelligence. In contrast, Hungary lacks regulation due to limited political will, relying instead on non-binding recommendations, which have proven ineffective.

Various types of regulations across EU countries are aimed at directly targeting information manipulation. States define the need to combat FIMI differently, addressing concerns such as public order, national security, individual or institutional reputation, constitutional order, sovereignty, territorial integrity, defence capabilities, economic stability, public health, and personal rights affecting human dignity. Overall, EU efforts to counteract FIMI are still in their early stages, with diverse national approaches reflecting different priorities for protecting public order, security, and institutional integrity. These varied approaches reflect each country's priorities in safeguarding public interests against FIMI.

The geopolitical context has emerged as a crucial determinant in shaping national approaches to disinformation regulation, with a clear East-West divide in regulatory intensity. The Baltic states and Poland demonstrate the most stringent regulatory frameworks, directly influenced by their historical experiences and proximity to Russia. This is evidenced by Lithuania's 2017 security strategy, which explicitly identifies Russia as the primary threat to information security, and Latvia's decisive action to ban Russian TV channels following the invasion of Ukraine[213]. Poland similarly responded with immediate measures, including the removal of Russian propaganda channels through its KRRiT resolution in February 2022.

The influence of **legal traditions** and **EU membership** is another crucial factor in shaping national approaches to disinformation regulation. A distinct pattern can be observed where some member states, exemplified by Luxembourg, deliberately refrain from developing national legislation, preferring instead to defer in anticipation of comprehensive EU frameworks. This wait-and-see approach contrasts with the proactive stance taken by other member states. Romania's swift adoption of Law No. 50/2024 in March 2024 demonstrates its commitment to harmonising national legislation with EU requirements, while Bulgaria's implementation of the DSA has already catalysed significant changes in its legal framework and institutional infrastructure, particularly in the areas of user protection and platform accountability. This varying pace and approach to EU regulatory alignment reflects broader differences in legal cultures and institutional capacities across member states, with some countries viewing EU frameworks as an opportunity to modernise their digital governance structures, while others prefer to maintain regulatory flexibility until EU standards are fully established.

The variation in **political culture and media traditions** across EU Member States has also shaped their approach to disinformation regulation. Sweden exemplifies a strong democratic tradition where freedom of expression is constitutionally enshrined as a paramount right, with explicit legal presumption favouring free speech over other competing interests. This approach starkly contrasts with the situation in countries like Hungary, where a lack of political will to counter disinformation has resulted in minimal effective regulation, relying primarily on non-binding recommendations that SAUFEX survey respondents characterise as highly ineffective.

These divergent approaches reflect deeper differences in democratic traditions and institutional trust across the EU. In countries with strong democratic institutions and high trust in media self-regulation, an emphasis tends to be placed on preserving press freedom while addressing disinformation through media literacy and voluntary compliance mechanisms. Conversely, in

[213] Decision based on Electronic Mass Media Law Article 26 that prohibits "calls for war". *Elektronisko plašsaziņas līdzekļu likums*, Latvijas Vēstnesis, 118, July 28, 2010, https://likumi.lv/ta/id/214039-elektronisko-plassazinas-lidzeklu-likums, [last access: September 12, 2024].

states with different historical experiences and institutional frameworks, the balance between media freedom and state oversight often tilts more toward direct government intervention, though not always resulting in effective countermeasures against disinformation.

Analysis of current trends in EU Member States' approaches to disinformation reveals several significant patterns and emerging challenges. A clear trend toward increased regulation is evident, with countries like Poland, Lithuania, Cyprus, and Latvia introducing new legislative measures accelerated by the implementation of the DSA. However, the approaches vary considerably in their comprehensiveness and institutional structure. France exemplifies a centralised, comprehensive approach with its dedicated VIGINUM, while Austria maintains a more distributed framework, utilising existing legal mechanisms to address various aspects of disinformation.

Such divergent approaches have highlighted critical challenges, particularly in balancing security concerns with freedom of expression. Poland's experience with the Draft Law on the Protection of Freedom of Expression on the Internet illustrates this tension, with the Ombudsman warning against potential restrictions on free speech through arbitrary state decisions. Institutional independence also emerges as a significant concern, as evidenced by Romania's controversy over the appointment of ANCOM's president, raising questions about regulatory body autonomy. The Russian invasion of Ukraine has served as a catalyst for enhanced state authority in combating disinformation, particularly in Central European countries, yet varying approaches among member states continue to reflect their distinct historical contexts, geopolitical positions, and legal cultures.

Such diversity in regulatory responses, while demonstrating the complexity of addressing disinformation, also underscores the ongoing challenge of developing effective countermeasures while preserving democratic values and institutional integrity. Countering FIMI requires comprehensive statutory regulation that ensures democratic control, transparency, and precise delineation of state authorities' responsibilities in disinformation mitigation. A robust legal framework is needed to establish a flexible (framework) definition of disinformation as the intentional, systematic dissemination of false or misleading information designed to harm society, while maintaining interpretative adaptability to emerging technological and strategic contexts. Regulations need to comprehensively define specific tasks and operational mandates of state agencies responsible for FIMI counteraction, digital platforms' responsibilities, state-private sector cooperation principles, and mechanisms protecting freedom of expression. Harmonising these regulations at the EU level, while respecting systemic legal differences, can enhance FIMI counteraction effectiveness, safeguarding fundamental civil rights and maintaining responsiveness to the rapidly evolving information landscape.

Part V – SOCIETAL RESILIENCE

This section seeks to map out the state of democracy among EU countries within the context of societal resilience against FIMI. Although FIMI, by definition, is a tool used by foreign powers against another country, it thrives on internal disputes and domestic political instability. Both desk research and SAUFEX's expert survey indicate that foreign interference uses social controversies and moot points as fundamentals for spreading disinformation. It is built on current events, connections to foreign actors, and social polarisation, which has the potential to create divisions in society's cohesion and deepen those that are already present.

Democracy and societal resilience

Societal resilience refers to the ability of a community to withstand, adapt to, and recover from challenges, including disinformation campaigns and social unrest[214]. The community's capacity for resilience is often augmented by social cohesion, which fosters trust for institutions and collaboration among community members. Meanwhile, media literacy equips individuals with the skills to critically assess information, enabling them to discern fact from falsehood. Together, these elements create a robust foundation for societal resilience, particularly in contexts where disinformation proliferates[215].

EU states vary widely in their internal stability and, thus, in their level of susceptibility to FIMI. This is influenced by local political landscapes, media independence, and societal cohesion. The effectiveness of countermeasures and debunking efforts often hinges on state-media relationships and media funding, with cross-sectoral collaboration proving a crucial and, often, decisive factor in the most resilient states.

At the same time, there is also an opposite vector interaction. Social coherence, trust for the government, cross-sectoral collaboration, and the ability to resolve internal disputes to prevent threat actors' interventions are also strengthened by strong regulations and institutions guaranteeing media freedom and independence. Therefore, the relationship between social coherence and strong, effective regulation regarding FIMI is best described as circular, where one element directly impacts the condition of another.

FIMI and disinformation vulnerability highlight the essential character of robust democratic practices for a stable and resilient society, and European states that embody these democratic strengths tend to have lower FIMI susceptibility. By maintaining stable institutional and social structures through transparent governance, independent media, cohesive social policies, and high media literacy, these states can effectively defend against manipulation. Democratic strength, in this context, is less about form and more about the depth of democratic engagement across media, civil society, and governance—forming a multi-layered defence that empowers citizens to recognise and counter disinformation. Within this context, three variables can be distinguished as influencing societal responses to FIMI. In democracies, citizens trust institutions that are characterised by transparent governance, an accountable judiciary, and a

[214] Stollenwerk, E., Börzel, T.A., & Risse, T., *Theorizing resilience-building in the EU's neighbourhood: introduction to the special issue*, "DEMOCRATIZATION" 2021, VOL. 28, NO. 7, 1219–1238, https://doi.org/10.1080/13510347.2021.1957839.

[215] Humprecht, E., Van Aelst, P., & Esser, F., *Resilience to Online Disinformation: A Framework for Cross-National Comparative Research*, "The International Journal of Press/Politics" 2020, VOL. 25, NO. 3, 493-516, https://doi.org/10.1177/1940161219900126.

responsive government. This foundational trust helps immunise societies against FIMI tactics that aim to exploit cynicism, disenchantment, or apathy toward democratic structures.

Case studies of Bulgaria and Romania indicate that low trust in state institutions is correlated with institutional weakness, which tends to be exploited by threat actors when spreading disinformation. This weakness hampers possibilities for cross-sectoral cooperation and decreases the legitimacy of state-led counter disinformation efforts aimed at strengthening media literacy.

On the other end of the spectrum, Denmark provides an exemplary case of high trust in public institutions paired with a strong conviction that citizens in the country can access accurate information from multiple media sources; this is strengthened by government involvement in awareness raising initiatives.

Levels of political and social polarisation

Threat actors take advantage of pre-existing conflicts or current affairs with the potential to cause or deepen cracks within the social cohesion of a given state. Societies with lower levels of polarisation are generally more resilient to divisive narratives propagated through disinformation. Strong democracies often engage in consensus-driven politics, reducing the appeal of extreme ideologies and limiting FIMI's effectiveness in sowing division[216].

Finland is a demonstrative case of increased resilience to polarisation due, in part, to institutional structures that prioritise representation across diverse communities. In Portugal, the relatively young tradition of democracy and belief that democratisation has brought positive change has decreased the potential for polarisation while at the same time increasing societal resilience.

In Belgium, on the other hand, the linguistic diversity of its population has limited the potential of strong national initiatives[217]. Similarly, in Spain, where local identities often resonate stronger than national ones, pro-independence or separatist aspirations have become platforms for threat actors to spread content that favours regional interests[218]. Moreover, in Bulgaria, a long history of connections to Russia has fuelled polarisation and divisions related to the Russia-Ukraine war[219]; in Romania, growing social polarisation, nationalism, populism, and social conservatism that challenge Western liberal values, as well as high levels of corruption, have enhanced social vulnerability[220]. In Poland, high levels of polarisation have created vulnerability to Russian disinformation, despite historically higher resilience from Polish society against manipulation by this particular actor [221].

---

[216] Ibidem.

[217] Alaphilippe, A., *Disinformation Landscape in Belgium*, EU DisinfoLab May 2023, https://www.disinfo.eu/wp-content/uploads/2023/05/20230509_BE_DisinfoFS.pdf [last access: June 6, 2024].

[218] *Catalonia's bid for independence from Spain explained*, BBC, October 18, 2019, https://www.bbc.com/news/world-europe-29478415, [last access: December 11, 2024].

[219] Sabev, M., Georgiev, G., & McLaren, R., *Safeguarding the Foundations: Strengthening Civil Security in Bulgaria, Montenegro, North Macedonia and Serbia*, Center for the Study of Democracy, 2024, p. 12–15.

[220] Hajdu, D., Sawiris M., & Klingová K., *GLOBSEC Vulnerability Index: Romania*, GLOBSEC, Global Focus listopad 2021, p. 26–29, 32–35, https://www.globsec.org/sites/default/files/2021-11/Vulnerability-Index_Romania.pdf [last access: July 30, 2024].

[221] Tworzecki, H., *Poland: A Case of Top-Down Polarization*, The ANNALS of the American Academy of Political and Social Science, 681(1), 2019, 97–119. https://doi.org/10.1177/0002716218809322 [date published 20.12.2018], p. 97–101, 106–112.

Media landscape and transparency

It is crucial for a strong democracy to possess an independent, diverse media landscape free from excessive political or economic influence. Such a media environment allows citizens access to balanced information and provides checks on disinformation as pluralism in media reduces the dominance of any single narrative or bias. The positive impact of media-driven initiatives focused on fact-checking can be seen in the case of Spain, where organisations such as Maltida.es and Iberifier have adopted a grassroots approach to debunking that allows citizens to directly contact the organisations whenever they doubt the truthfulness of information presented in the media[222]. In Lithuania, the biggest news portal, *delfi.lt*, has developed a tool to combat "fake news" in cooperation with Google, highlighting a (still unfulfilled) potential for big tech to play a positive role in fighting disinformation.

At the same time, the media in countries such as Hungary, Bulgaria, Romania, and Cyprus face constant political pressure. In these countries, major outlets tend to be financed by political parties (i.e., Romania), influenced by business or the church (i.e., Cyprus), lack funding regulations (i.e., Bulgaria), or are subject to political pressure and governmental monitoring through surveillance tools (i.e., Hungary).

Traditional media outlets and fact-checkers are crucial in informing societies; to play its critical role within democracies, the media sector requires stable work conditions as well as independent and sustainable funding. The cases of Ireland, Denmark, and Latvia are prime examples of the impact working conditions and financial constraints can have on the extent to which the media can protect itself and citizens from FIMI and disinformation; recent studies have pointed to the impact of layoffs and financial problems faced by Irish broadcasters[223] and unstable media funding in Latvia[224] and Denmark[225].

The three variables allowed to group EU states accordingly:

Group 1: High strength in democratic characteristics

In Reporters Without Borders' 2024 World Press Freedom Index[226], **Finland, Ireland, the Netherlands, Denmark, Sweden, and Luxembourg** placed between second and 11th place across the world. In the Media Literacy Index, these countries were ranked between first and eighth place, apart from Luxembourg, which ranked 21st. These EU Member States are also characterised by some of the highest levels of trust in democratic institutions and advanced media literacy education programmes integrated into the educational systems. Particularly in Finland and Denmark, effective collaboration between the government and NGOs on disinformation efforts can also be observed. All these characteristics positively influence societal resilience to FIMI and hamper FIMI initiatives by threat actors.

---

[222] Romero Vicente, A., *Disinformation Landscape in Spain*, EU Disinfo Lab, March 2023, 20230224_SP_DisinfoFS.pdf [last access: December 4, 2024].

[223] Reuters Institute, *2022 Reuters Institute Digital News Report*, https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/ireland [last access: December 11, 2024].

[224] *The Regulation of Fact-checking and Disinformation in the Baltic States*, EDMO, May 2024, BECID-D3.4._report.pdf [last access: December 11, 2024].

[225] Simonsen, S., *Monitoring media pluralism in the digital era application of the media pluralism monitor in the European member states and candidate countries in 2023 country report: Denmark*, EUI Centre for Media Pluralism and Media Freedom/Robert Schuman Centre, June 2024.

[226] *2024 World Press Freedom Index*, Reporters Without Borders, https://rsf.org/en/index, [last access: December 11, 2024].

Finland's comprehensive media literacy initiatives and strong civic engagement[227], alongside Ireland's Media Literacy Ireland network and collaboration on fact-checking, underscore these countries' resilience[228]. The Danish government's support for media, driven largely by political will to support and uphold media plurality as well as sustain media in the Danish language, has positively impacted its potential to fight FIMI. Such initiatives are transparent and fair for both state and private media, which has helped Denmark avoid issues with politically affiliated business owners controlling major media outlets to influence public opinion like in other EU countries[229]. Sweden has embraced a "raising the threshold" strategy aimed at deterring information influence activities by fostering societal legitimacy and enhancing public vigilance and resistance to such campaigns[230].

Group 2: Moderate to high strength in democratic characteristics

Countries like **Germany, Austria, Belgium, Estonia, Lithuania, Latvia, and Portugal** exhibit high democratic characteristics but may have specific vulnerabilities, such as moderate polarisation or challenges with media independence. These states are ranked between sixth (i.e., Estonia) and 13th in the World Press Freedom Index, except for Austria, which came in 31st. In the Media Literacy Index, they come in between fourth (i.e., Estonia) and 20th (i.e., Lithuania) place across the world. They are characterised by strong institutional trust and active civil society organisations that work on disinformation countermeasures. They have also implemented media literacy programmes, though with varying degrees of effectiveness. Some of these countries are also negatively influenced by historical connections to Russia, which can serve as a platform for FIMI and a source of polarisation.

Germany's Correctiv initiative, for example, reflects a robust civil society effort to counter disinformation, while Belgium's EDMO BELUX collaboration illustrates active state-civil cooperation. The Austrian approach to FIMI emphasises the need to balance protection against disinformation with respect for fundamental rights, including freedom of expression and the arts. Austria prefers to educate and promote awareness of the dangers of disinformation rather than introduce additional legislation. This is evident in its Deepfake Action Plan that emphasises building social resilience, strengthening digital competences, and promoting reliable information sources[231]. In Baltic states, active civil society and media platforms play an important role in countering FIMI – even at the cross-border level, given their common FIMI vulnerabilities (e.g., Russian speaking minorities, border threats). The most significant of these is Re:Baltica and its project Re:Check, which engages fact-checking and social media research to debunk or investigate posts that may contain misleading or manipulative content[232].

---

[227] The Finnish Security Committee/Turvallisuuskomitea. *Security Strategy for Society/Yhteiskunnan turvallisuusstrategia - Valtioneuvoston periaatepäätös,* https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf [last access: December 11, 2024].

[228] Culloty, E., *Disinformation Landscape in Ireland*, EU DisinfoLab, p. 6, [last access: December 11, 2024].

[229] Simonsen, S., *Monitoring media pluralism in the digital era application of the media pluralism monitor in the European member states and candidate countries in 2023 country report: Denmark*, EUI Centre for Media Pluralism and Media Freedom/Robert Schuman Centre, June 2024, https://cadmus.eui.eu/bitstream/handle/1814/76998/Denmark_EN_mpm_2024_cmpf.pdf?sequence=1&isAllowed=y [last access: December 4, 2024], p. 6.

[230] Försvarsmakten/The Swedish Armed Forces, *Svenskt psykförsvar i backspegeln*, February 26, 2020, https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/svenskt-psykforsvar-i-backspegeln/ [last access: December 4, 2024].

[231] Bundesministerium für Inneres, *Aktionsplan Deepfake*, 2022, https://www.bmi.gv.at/bmi_documents/2779.pdf.

[232] The disinformation landscape in Latvia, https://www.disinfo.eu/publications/disinformation-landscape-in-latvia/ [last access: December 4, 2024].

Group 3: Moderate strength with notable vulnerabilities

Countries like **France, Spain, the Czech Republic, Italy, Poland, Croatia, Slovenia, and Slovakia** show moderate strength in democratic attributes but face issues with either polarisation, lower media trust, or civil society's limited influence, which leaves them more vulnerable to FIMI. These states also face challenges with polarisation and social divides, such as in France and Spain, where regional tensions can be exploited by disinformation. In the World Press Freedom Index and Media Literacy Index, they are ranked below 17th and 15th place, respectively. Trust in democratic institutions in these states tends to be below the EU average (i.e., 36% trust in national parliament, 33% trust in the national government).

Since 2015, Polish society has become increasingly polarised due to divisive and hostile party politics that have spread into communities and social spheres[233]. This has negatively influenced its otherwise resilient society and was one of the factors behind the activity of Russia-connected actors during demonstrations regarding agricultural politics.

Spain's regional polarisation provides an entry point for external narratives, while France's media efforts, such as AFP Factuel, show resilience tempered by lower institutional trust (i.e., only 19% of French respondents trust their national government). In Spain, regional separatist movements, particularly in Catalonia, have facilitated widespread disinformation campaigns and social fragmentation. This vulnerability has been worsened by complex interactions between local autonomy and state intervention, creating fertile ground for external actors to exploit divisions.

The opportunistic character of FIMI can be observed through Russia's instrumentalization of the illegal independence referendum organised in 2017 and the institutional crisis that followed as a vehicle for spreading disinformation. Russian officials reportedly maintained contacts with members of the Catalan independence movement during the referendum period. Support for this campaign was part of a broader effort to cultivate and support separatist sentiments, which served Russia's interest in creating divisions within EU states[234].

Group 4: Lower democratic strength with high vulnerability

Hungary, Bulgaria, Romania, Malta, Greece, and Cyprus face significant challenges, including high polarisation, limited media independence, and lower civil society influence, making them more susceptible to disinformation and FIMI. These countries are also characterised by high polarisation and social divides that external actors can exploit, particularly in Bulgaria and Romania. They are ranked as the weakest in terms of press freedom and media literacy in the EU, with Greece placed at 88th in the World Press Freedom Index and Bulgaria ranked 35th in the Media Literacy Index; these represent the worst scores in the EU within each index. Notably, citizens of these countries have significantly higher trust in the EU than their national governments and parliaments.

Both Hungary's government-controlled media and the strong Russian influence in Bulgaria illustrate how democratic weaknesses can heighten susceptibility to FIMI. Russia has capitalised on Hungary's internal political landscape, particularly its government-controlled media and political polarisation, to spread disinformation and promote narratives sympathetic to Russian interests[235]. Hungary's media landscape is dominated by entities that support the

[233] Tworzecki, H., *Poland: ...,* op.cit.

[234] Romero Vicente, A., *Disinformation Landscape in Spain*, EU DIsinfo Lab, March 2023, 20230224_SP_DisinfoFS.pdf [last access: December 4, 2024].

[235] See Szabolcs, P., *Putin's hackers gained full access to Hungary's foreign ministry networks, the Orbán government has been unable to stop them*, "Direkt36", March 29, 2022, https://www.direkt36.hu/en/putyin-

ruling Fidesz party, which frequently promotes narratives in line with Russian perspectives. This alignment gives Russian narratives an open channel through which they can reach the Hungarian public without strong opposition, effectively blending Hungarian and Russian agendas in the media space. Hungary's Sovereignty Protection Act exemplifies state-led media control and mirrors Russian tactics by targeting NGOs and independent media with foreign funding. The act illustrates how Hungary's approach to media and NGO regulation has enhanced domestic disinformation vulnerabilities[236]. In Romania, political pressure on the media has also increased, particularly in the run up to the 2024 elections, while a lack of transparency regarding media funding continues to persist[237].

Variety of connections to Russia

This subsection evaluates historical and present connections to potential threat actors (i.e., Russia, China, and other autocratic states) and analyses how they have facilitated FIMI operations.

Russia has built its influence in various countries through business contacts (e.g., in Germany and Austria) or historical and religious links (e.g., Cyprus and Bulgaria). Due to their strong historical ties with Russia, a significant minority presence has also impacted Russian influence over the Baltic states. In Cyprus, the financial and political influence of Russia and other foreign actors has become a source of vulnerability to disinformation campaigns and foreign interference. Many Cypriot politicians and influential figures have acted in Russia's interests to the detriment of their own country and the EU, as evidenced by the 2023 Cyprus Confidential study by the International Consortium of Journalists[238]. One reason behind this is the role that Cyprus has played as a tax haven for many Russian oligarchs[239].

Bulgaria faces considerable exposure to Russian influence, driven by its dependence on Russian energy resources and the Kremlin's deep cultural connections within the country. This influence extends beyond public opinion to key state sectors such as intelligence, diplomacy, and the judiciary[240]. A striking example of this is the reported penetration of Bulgarian institutions by Russian intelligence networks. Even high-level bodies like the Chief Directorate for Combating Organised Crime and the State Agency for National Security, which are meant to safeguard against foreign threats, have been implicated in espionage scandals linked to Moscow[241].

---

hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/ [last access: September 22, 2024].

[236] Szakács J., & Bognár, É., *Digital News Report 2024: Hungary*, Reuters Institute for the Study of Journalism 2024, p. 86–87.

[237] Radu, R., *Digital News Report 2024: Romania*, Reuters Institute for the Study of Journalism, 2024., p. 100–101, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf [last access: July 30, 2024].

[238] International Consortium of Investigative Journalists, *About the Cyprus Confidential investigation*, November 14, 2023, https://www.icij.org/investigations/cyprus-confidential/about-cyprus-confidential-investigation/ [last access: December 4, 2024].

[239] In 2016, the Cypriot Parliament adopted a resolution which called for the lifting of sanctions against Russia after the illegal annexation of Crimea. This was orchestrated by a Kremlin-linked lobbying group (i.e., the International Agency for Current Policy) and put forward by Cypriot politicians courted by the lobbyists. International Consortium of Investigative Journalists, *Cyprus Confidential*, 2023 [last access: December 2, 2024].

[240] Sabev, M., Georgiev, G., & McLaren, M., *Safeguarding the Foundations: Strengthening Civil Security in Bulgaria, Montenegro, North Macedonia and Serbia*, Center for the Study of Democracy 2024, p. 12–15.

[241] Todorov, S., *Espionage Allegations Rock Bulgaria's Top Security Agencies*, „Balkan Insight", Sofia 5.02.2024, https://balkaninsight.com/2024/02/05/espionage-allegations-rock-bulgarias-top-security-agencies/ [last access: December 4, 2024].

In Greece, Russia has made efforts to infiltrate the Greek Orthodox Patriarchates and Churches. A significant example of this is Russian financial activity within the semi-independent Mount Athos, an Orthodox spiritual centre with multiple monasteries. Mount Athos' status and connections between Greek and Russian Orthodox churches made it an important destination for money laundering and spreading of narratives that benefit Russia[242].

In Estonia, around 27% of the population is Russian speaking, which has been reported as a significant challenge in integrating this group into Estonian society[243]. According to research conducted by the Fredrich Ebert Foundation, following the full-scale Russian invasion of Ukraine, 50 percent of the Russian-speaking minority agreed that Russia had a right to use military force against Ukraine to prevent it from joining NATO; notably, among Estonian-speaking families, only one percent of citizens supported this statement. Latvia and Lithuania face a similar challenge with Russian speakers constituting 25 to 30 percent[244] and at least 5 percent [245] of the population, respectively.

NGOs' relations with society, the media, and governments[246]

The interplay between social cohesion and media literacy has emerged as a cornerstone of societal resilience, particularly in fragmented and polarised environments. An effective approach involves the collaboration of non-governmental organisations (NGOs) with governmental bodies, the media, and civil society. While instances of cooperation have been documented in various countries, conflicting interests and tensions often complicate these relationships. In some cases, proactive media literacy initiatives and fact-checking programmes exist but are sometimes perceived as ineffective, underscoring the need for a more cohesive strategy. A well-developed NGO sector complemented by educational outreach that promotes media literacy plays a pivotal role in fostering trust and resilience in society. In advanced economies where democratic values are entrenched, the framework for these collaborations tends to be more robust. However, the sustainability of such initiatives requires an ongoing commitment to fostering trust and transparency among all stakeholders.

Fact-checking initiatives and media literacy education

The presence of well-developed NGO networks that engage in fact-checking and media literacy education serves as a foundation for building societal resilience. Various case studies across Europe reveal that cooperation among NGOs, public institutions, and media can yield positive outcomes, with a clear correlation observed between the activities of these organisations and overall trust within society.

---

[242] Orthodox Times, *Greek authorities' investigation into Russian remittances to Mount Athos,* October 3, 2022, https://orthodoxtimes.com/greek-authorities-investigation-into-russian-remittances-to-mount-athos/.

[243] '*Feeling Cornered: An Analysis of the Russian-Speaking Minority in Estonia*, European Website on Integration, https://migrant-integration.ec.europa.eu/library-document/feeling-cornered-analysis-russian-speaking-minority-estonia_en [last access: July 11, 2024].

[244] *Latvia Country Report*, in: Media Literacy Sector Mapping in Georgia, Latvia, Moldova and Ukraine, 2021, Baltic Centre for Media Excellence, https://bcme.eu/en/our-work/research/report-media-literacy-sector-mapping-in-georgia-latvia-moldova-and-ukraine-2, p. 11.

[245] Oficialiosios statistikos portalas: Pradžia. https://osp.stat.gov.lt/en/statistiniu-rodikliu-analize?hash=66b3091a-c738-4d87-b961-ecefdc2613ca#/.

[246] Includes fragments from desk reviews of various authorship of research team members.

For instance, France's Agence France Presse (AFP) has established a global network of fact-checkers that actively monitor misinformation. To date, AFP Factuel has more than 140 fact-checkers in five continents covering over 30 countries and 24 languages, who are in constant contact with other journalists in the AFP network. AFP Factuel is also a member of the International Fact-Checking Network (IFCN)[247].

NGOs such as Correctiv and Forum against Fakes maintain independence while contributing to fact-checking efforts. This collaboration between NGOs and governmental bodies exemplifies a model of resilience founded on mutual support and shared goals.

In the Netherlands, a regional hub from the European Digital Media Observatory initiative, Benedmo[248], focuses specifically on the Dutch-speaking community in Belgium and the Netherlands. It has notably documented specific cross-border disinformation campaigns on health and the impact of fact-checking. deCheckers is a non-profit organisation working in partnership with Dutch-speaking fact-checkers that gathers fact-check articles from various media outlets in a single place. It allows the public to access this information in one portal instead of searching for debunks on multiple websites.

Media literacy has emerged as a vital tool in combating misinformation and fostering societal resilience. It equips individuals with the skills to critically evaluate information, recognise biases, and distinguish between fact and opinion. Educational programmes, supported by governmental initiatives and civil society organisations, play a crucial role in this endeavour.

The effectiveness of media literacy initiatives varies considerably across European nations. For example, Belgium's EDMO BELUX[249] initiative exemplifies a successful cross-community collaboration aimed at combating disinformation. By bringing together fact-checkers, media experts, and academics, EDMO BELUX raises awareness through targeted campaigns and educational programmes. Despite this, the overall resilience of Belgian society to FIMI remains "rather low", underscoring the fact that even well-coordinated efforts are not always sufficient to mitigate the threats posed by misinformation.

In contrast, Finland exemplifies a strong tradition of media literacy that has embedded itself within the educational system. The Finnish National Agency for Education has made media literacy a civic skill, promoting it from early childhood through to vocational training. This proactive stance has yielded high trust levels in news media and a resilient society that is well-equipped to navigate the complexities of the information landscape. Finland's approach underscores the importance of integrating media literacy into the fabric of education and civil society[250].

In Germany, the government has actively supported initiatives to strengthen public resilience to disinformation. A key role is played by the Federal Agency for Civic Education, which offers a wide range of educational materials and programmes on media literacy and critical thinking. In addition to this, the Ministry of Interior has also supported a media literacy initiative, and

[247] Hénin, N., *Disinformation Landscape in France*, EU DisinfoLab, March 2023, https://www.disinfo.eu/publications/disinformation-landscape-in-france [last access: December 2, 2024].
[248] Benedmo, https://benedmo.eu/english/ [last access: December 2, 2024].
[249] Disinfocheck, https://belux.edmo.eu/ [last access: December 2, 2024].
[250] *In Finland trust in media scores among the highest*, Reuters Institute, *Digital News Report 2024*, 2024. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf, [last access: December 2, 2024], p. 73.

the BC4D was launched to create a media literacy initiative in cooperation with the private sector. In Austria, governmental and non-governmental bodies are active in anti-disinformation campaigns and media literacy. Additionally, in 2022, the German-Austrian Digital Media Observatory (GADMO) and fact-checkers Correctiv joined EDMO[251].

In Ireland, the Media Literacy Ireland network has been launched[252], which created an informal alliance of over 250 members working to promote media literacy. The network consists of a broad range of sectors including media, education, NGOs, and libraries. Digital literacy is highly present in the national curriculum in schools, whereas media literacy is only somewhat present, and challenges persist in formalising media literacy within national policies and teacher training programmes. Ireland also has multiple grassroot level networks dedicated to enhancing media literacy in the country.

Numerous civil society organisations (CSOs) in Estonia have played an important role in countering FIMI. They work on various fronts, including fact-checking, media literacy education, and public awareness campaigns. For instance, Estonia established the Cyber Defence League, a group of volunteer IT specialists dedicated to sharing information about threats and cyber security and engaging people in international cyber defence activities.

Another example of a non-state actor working to address FIMI in Estonia is the National Centre for Defence & Security Awareness (NCDSA), established in 2011. The NCDSA is an Estonian non-governmental expert platform dedicated to strengthening national resilience through applied research, strategic communication, and social interaction. The NCDSA runs a state-supported training programme that aims to inform Russian-speaking communities about Estonian national defence and security by initiating and organising public events. Additionally, the NCDSA monitors and analyses the security and defence perceptions of Russian-speakers in Estonia.

In Latvia, efforts against FIMI are being made together with partners, particularly other Baltic states and like-minded countries, through cross-border cooperation at the non-governmental level. For example, the foundation RE: BALTICA has been producing investigative journalism and publishing reports on disinformation efforts in the Baltic states, including on social media (an ever-growing hotbed of disinformation)[253], since 2011.

Complex cases – fragmentation and polarisation

Despite these positive examples, challenges persist. In several instances, tensions and conflicts have arisen between NGOs and state actors, undermining efforts toward cooperation. In fragmented societies where divisions based on ideology, ethnicity, or socioeconomic status deepen, it becomes challenging to implement cohesive strategies that address the threats posed by disinformation. The aim of this section is not only to map NGOs and their initiatives but also

[251] Schäfer, C., *The disinformation landscape in Austria*, EU Disinfo Lab, 2023, p. 6.

[252] Gallagher, A., O'Connor, C., & Visser, F., *Uisce Faoi Thalamh: An Investigation Into the Online Mis- and Disinformation Ecosystem in Ireland*, Report 1 of 3 Summary report. Institute for Strategic Dialogue (ISD), https://www.isdglobal.org/wp-content/uploads/2023/11/Uisce-Faoi-Thalamh-Summary-Report.pdf, [last access: December 2, 2024], p. 2, 13.

[253] Baltic Centre for Media Excellence, *Latvia Country Report*, in: 'Media Literacy Sector Mapping in Georgia, Latvia, Moldova and Ukraine', 2021, https://bcme.eu/en/our-work/research/report-media-literacy-sector-mapping-in-georgia-latvia-moldova-and-ukraine-2, [last access: December 2, 2024], p. 11.

to place them in the wider socio-political system. Within a general trend of a lack of coherence between civil society and non-cooperative governments and polarised society, the dynamics of these relations vary. Each case provides examples of country-specific elements that are disruptive to creating a coherent anti-FIMI ecosystem.

In countries where media literacy is not prioritised, such as Italy, societal resilience is significantly undermined, which is evidenced by low levels of trust in the media and the prevalence of disinformation[254].

In addition to educational initiatives, cooperation between NGOs and media organisations is essential for fostering a culture of fact-checking and accountability. Collaborative platforms that engage citizens in identifying and reporting disinformation can create a community-oriented approach to combating disinformation. For instance, initiatives like "Maldita.es" [255] in Spain and "Poligrafo"[256] in Portugal have mobilised public participation in fact-checking processes, empowering citizens to actively challenge false narratives. Such grassroots efforts not only enhance media literacy but also strengthen cohesion by fostering a sense of shared responsibility towards combating disinformation. Nonetheless, the effectiveness of these initiatives is often contingent upon the broader political and social landscape.

In countries with high levels of corruption or political polarisation, such as Romania and Bulgaria, societal resilience is severely compromised[257]. The public's distrust in state institutions and the media diminishes the impact of educational efforts and grassroots initiatives aimed at enhancing media literacy. In such contexts, fostering social cohesion becomes increasingly critical, as it serves as a counterbalance to the divisive forces perpetuated by disinformation campaigns.

In 2018, experts from the European Values Center in Czechia produced the Prague Manual for countering Russian influence operations in Europe. The country has traditionally featured a strong civil society (e.g. Czech Elves, European Values Center, and Manipulátoři). The elves (i.e., active members of society) in the Czech Republic, inspired by examples from the Baltic states, track accounts and online platforms, flagging activities like the spreading of disinformation through emails about COVID-19. The Czech NGO Demagogue also inspired the work of Polish fact-checkers. One of the biggest achievements of the Czech non-governmental sector in countering disinformation was the development of the Conspiracy Atlas – a web-based database of conspiracy theories, populist framing, and disinformation from the online world[258]. Nevertheless, the country continues to exhibit some vulnerabilities to disinformation, which is due, in part, to the government's low capacity to regulate false narratives; a sizable amount of government-sponsored disinformation; and low levels of civic participation online, media literacy preparedness, and trust in the media.

[254] Corina, A., *Italy*, Reuters Institute, https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024/italy [last access: December 2, 2024].
[255] ECAS, *Interview: How this organisation is fighting against disinformation*, European Citizen Action Service, 2023, https://ecas.org/interview-how-this-organisation-is-fighting-against-disinformation/ [last access: December 2, 2024].
[256] Poligrafo, https://poligrafo.sapo.pt [last access: December 2, 2024].
[257] Hajdu, D., Klingová, K., Sawiris, M., *GLOBSEC Vulnerability Index: Romania*, GLOBSEC, Global Focus listopad, 2021, p. 26–29, 32–35, https://www.globsec.org/sites/default/files/2021-11/Vulnerability-Index_Romania.pdf [last access: July 30, 2024].
[258] Atlas Konspiraci, https://www.atlaskonspiraci.cz/, [last access: December 2, 2024].

The landscape of societal resilience within the EU is far from uniform. In several countries, including Poland and Hungary, the interplay between government entities and NGOs presents complications. In Poland, public trust in state institutions is low, resulting in a fragmented approach to combating disinformation. While NGOs have become increasingly aware of foreign influence operations, their initiatives have often lacked necessary support from government institutions, leading to what experts describe as "cognitive capture" where public institutions between 2016-2023 adopted anti-Western narratives that created further political polarisation.

This fragmentation between the state and NGOs hinders effective cooperation and diminishes the potential impact of media literacy and cohesion initiatives. The low level of trust among citizens in governmental institutions has exacerbated the issue, resulting in a society vulnerable to disinformation. Poland's weaknesses have been identified as: a selectivity of actions in cyber-security, dispersion of competences at the administrative levels, neglect in education and support for independent media, and insufficient cooperation between the administration and NGOs. Furthermore, in Poland, high awareness of the threats posed by disinformation exists primarily among state institutions and NGOs but not the whole of society, which needs to be improved.

In recent years, several initiatives have emerged in Poland to combat disinformation (e.g., InfoOps, DisinfoDigest, PAP Fake Hunter, Pravda), fact-checking (e.g., Demagog) and media education (e.g., Panoptykon, Fundacja Nowoczesna Polska). Representatives of civil society have also highlighted a need to devise a national information security strategy. In the first half of 2022, 11 NGOs and research institutes jointly developed the Code of Good Practice – Together Against Disinformation, which attempts to systematise standards in the fight against disinformation. The experts that co-authored the report included key issues in the area of information security[259].

Hungary presents a particularly stark example of how relations between the state and NGOs can deteriorate. The political climate has increasingly restricted the activities of NGOs, resulting in a media landscape that is dominated by pro-government narratives. The Hungarian government's tactics, including the enactment of the Sovereignty Protection Act, have systematically undermined independent journalism and stifled dissent. In this context, the potential for NGOs to foster social cohesion and enhance media literacy is severely limited, leading to dangerously low levels of societal resilience against FIMI. Moreover, the level of cooperation between state institutions and non-state actors is very low.

Not only do these two spheres remain completely disconnected in Hungary, but the government has taken active steps to try to limit the capacity of NGOs. Hungary has made a practice of arbitrarily monitoring journalists using the anti-terrorist software Pegasus. Independent organisations that aim to strengthen societal resilience in Hungary, including fact-checking initiatives and initiatives aimed at identifying domestic and foreign information manipulation, operate in foreign-founded consortia[260]. These include Lakmusz and AFP for the fact-checking

[259] Forum Przeciwdziałania Dezinformacji, *Przeciwdziałanie Dezinformacji w Polsce Rekomendacje Systemowe*, https://ffb.org.pl/wp-content/uploads/2023/02/Raport_Przeciwdzialanie_dezinformacji.pdf [last access: December 2, 2024].

[260] Bleyer-Simo, K., *Disinformation Landscape in Hungary*, EU DisinfoLab, June 2024, p. 6, https://www.disinfo.eu/wp-content/uploads/2023/06/20230521_HU_DisinfoFS.pdf [last access: August 2, 2024]; Győri, L., *Challenges of Strategic Communication in Hungary*, Political Capital, 2023,

sector, Political Capital and Mertek Media Monitor in the areas of research and policymaking, and Idea Foundation for training activities.

Lithuania has also suffered from an unsustainable media landscape dependent on special interests and business groups. It struggled with corruption and discrimination against national minorities[261], which created a breeding ground for polarisation and other information-related vulnerabilities. However, cooperation between NGOs like Debunk, the government, and an active civil society (i.e., communities of *elves*) allowed for the creation of a quick FIMI response network.

In the Balkans, NGOs actively cooperate with each other, as well as EU institutions and local media. Media literacy, including anti-FIMI training, is provided jointly by NGOs and media associations. Post-Yugoslavian NGOs also hold an annual security conference in Bled with a FIMI-related focus. Many of these NGOs operate in a very polarised and ethnically complex environment, often with low or even hostile attitudes from public bodies, and therefore seek partners abroad, including the EU institutions.

Croatia and Slovenia are a part of a fact-checking network of six organisations from five countries in the Western Balkans, represented by the Association for the Informed Public (with its platform Faktograf.hr) and Ostro.si (with its platform Razkrinkavanje.si). The Croatian model for building a system of fact-checking in the public domain has been evaluated positively by the European Commission; this is indicative of more than just individual projects or institutions and suggests that Croatia is working towards creating anti-FIMI systemic resilience[262]. However, a study conducted by the state Agency for Electronic Media (AEM) indicates that a problem in cohesion between state institutions and society remains[263]. Notably, AEM provides funding for NGOs. Another state institution, the Ministry of Culture and Media has also been accused of trying to censor journalists with its legal proposals[264]. Additionally, the right-wing portals and bloggers have attacked the leading and internationally recognised anti-FIMI NGO, Faktograf, which was closely correlated in time with millions of hacker's attacks and death threats towards the organisation[265].

https://politicalcapital.hu/pc-admin/source/documents/IRI-PC_Study_Hungary_Challenges_StrategicCommunication_231219.pdf [last access: August 3, 2024].

[261] Cheskin, A., Identity and Integration of Russian Speakers in the Baltic States: A Framework for Analysis, *Ethnopolitics*, January 1, 2015, pp.72–93; Kuczyńska-Zonik, A.,'Dyskurs narodowościowy na Litwie w kontekście współczesnych wyzwań', *Instytut Europy Środkowej* /Rocznik 14 (5) (2016).

[262] CroRIS – CROSBI, *Disinformation, Propaganda and Fake News in Croatia*, www.croris.hr/crosbi/publikacija/prilog-knjiga/76122, [last access: December 2, 2024]; Kharazian, Z., Starbird, K., & Hill, B.M., *Governance Capture in a Self-Governing Community: A Qualitative Comparison of the Serbo-Croatian Wikipedias*, https://arxiv.org/abs/2311.03616, [last access: December 2, 2024]; National Security and Future, *Disinformation, Propaganda and Fake News in Croatia (nsf-journal.hr)*; Croatian Wikipedia Disinformation Assessment-2021 - Meta (wikimedia.org) [last access: November 26, 2024].

[263] EPRA, *Disinformation: AEM Croatia publishes landmark study*, Disinformation: AEM Croatia publishes landmark study (epra.org) [last access: November 26, 2024].

[264] European Journalists, *Croatia: Dora Kršul and Telegram.hr accused by the Minister of Culture and Media of publishing "malicious fake news" – European Federation of Journalists*, (europeanjournalists.org), [last access: November 26, 2024].

[265] Balkan Insight, *Croatian Fact-Checkers' War on Fake News Draws Bias Charge*, Croatian Fact-Checkers' War on Fake News Draws Bias Charge, [last access: November 26, 2024].

Some studies suggest that Slovenian society exhibits relatively high resilience against FIMI[266]. Civil society in the country actively cooperates with other states[267] , including within the European Citizen Action Service's (ECAS) international framework. The Slovenian NGO InePA, for example, partnered in the ECAS campaign "Understanding Populism".

In Malta, media and other organisations operate in a highly polarised environment that is strongly influenced by political parties and polarised around the issue of corruption. MEDMO, a network of fact-checkers and experts on FIMI and communication who cover these issues in Malta, Greece, and Cyprus, is working as a bottom-up initiative to tackle disinformation in the country. It is part of the wider EU-level initiative European Digital Media Observatory (EDMO).

Greece is also part of other counteracting disinformation and knowledge sharing bodies like the steering group for the OECD's DIS / MIS Resource Hub, the International Centre for Investigative Journalism, the Journalism Trust Initiative (JTI), and the Mediterranean hub of EDMO. Under its Civic Information Office, the platform MediaWatch is supported; other useful platforms include Voutliwatch and Ekspizo.gr. In the non-governmental sector, Ellenika Hoaxes is a fact-checking organisation funded by Meta.

Cyprus ranked 65 out of 180 countries in the 2024 World Press Freedom Index of Reporters Without Borders (RSF), just after Sierra Leone and before Argentina, under the label of "problematic". The RSF's evaluation held that "although freedom of press is guaranteed by the constitution, the government, the Orthodox Church, and business interests have significant influence over the media in Cyprus". A lack of funds for independent media and adequate salaries for journalists have hindered media pluralism and resilience efforts in the country. Moreover, the unresolved issue of Northern Cyprus has left the island state susceptible to influence campaigns, and the resulting split in the media environment poses[268] further challenges to countering disinformation and FIMI by increasing susceptibility to bias, according to local experts.

In January 2023, the Bulgarian Romanian Observatory of Digital Media (BROD), a regional hub and part of EDMO, was established under a project financed by the European Commission. In March 2021, AFP Proveri, the Bulgarian component of Agence France-Presse's (AFP) international fact-checking initiative, was established. This initiative was unique due to its cooperation with Meta as part of its global Third-Party Fact-Checking Program to investigate viral disinformation across Facebook, Instagram, and WhatsApp. Another important fact-checking institution in the country is Factcheck.bg, led by the Association of European Journalists-Bulgaria (AEJ-Bulgaria), which is a non-profit association and member of the International Association of European Journalists.

---

[266] Fiser, S.Z., & Caks, P., *Strategies for the Minimisation of Misinformation Spread Through the Local Media Environment, Journalism Practice*, 2023, 2241-2262, DOI: 10.1080/17512786.2023.2183235, [last access: November 26, 2024]; Eurobarometer, *Slovenia, Croatia, Greece – trust, social cohesion*, https://europa.eu/eurobarometer/surveys/detail/2183 [last access: November 26, 2024].

[267] With Bulgaria and Hungary: ECAS, *Civil Society Against Disinformation, Civil Society Against Disinformation*, [last access: November 26, 2024].

[268] Friedrich Naumann Foundation for Freedom, *New comprehensive study reveals Cyprus media's complex coverage of the Russia-Ukraine war*, https://www.freiheit.org/greece-and-cyprus/new-comprehensive-study-reveals-cyprus-medias-complex-coverage-russia-ukraine-war [last access: December 2, 2024].

Also noteworthy is BNR Factcheck, which is the only initiative run by a public media organisation, established by the Bulgarian National Radio and supported by competencies within BROD. All the above fact-checking initiatives were started in 2021. Furthermore, various NGOs and other organisations in Bulgaria are working to help tackle disinformation. A non-exhaustive list includes the Bulgarian Coalition against Disinformation and the Center for the Study of Democracy, which is a member of the BROD consortium[269].

Bulgaria has also taken part in several media literacy initiatives, which are often sponsored by private enterprises like Poynter or like-minded embassies (e.g., the UK, the U.S., France, and Germany). The Media Literacy Coalition is a network organisation that is working to integrate media literacy into the educational process and increase media literacy in society by building cooperation with relevant governmental and non-governmental organisations and institutions. Media literacy initiatives are often centred on schools and target young people.

Despite these efforts, Bulgaria also suffers from a level of "cognitive capture"[270]. The anti-European and anti-American narratives to which Bulgarian officials have been exposed over the past ten years has caused an inherent suspicion toward U.S. involvement in projects. Raising public awareness regarding FIMI thus remains in the domain of EU institutions, NGOs, the media, and journalists' associations - but not the national public administration or educational institutions.

In the case of Romania, there is no significant public debate on how the state should tackle disinformation and conduct strategic communications. Big newspapers and media outlets receive funding from political parties (often in a covert manner), which affects their independence. Despite putting relatively low trust in information coming from social media, Romanians still use Facebook as their main source of information. However, Romanians were more than eight times less likely (three percent) to view Russia as a strategic ally after the invasion of Ukraine, compared to Bulgarians (26 percent). According to GLOBSEC's Vulnerability Index, Romania scores 29/100, which represents a high level of resilience, particularly when compared to countries in the Western Balkans.

Misreport, a Romanian fact-checking newsletter, also relies on journalistic methods, which sets it apart from other organisations. Based on developing their own workflow, which involves a combination of media literacy, OSINT, and fact-checking tools, its team does investigative work on disinformation. Misreport's purpose is to map tactics around placing disinformation in the online space; it decides on the validity of an incident based on the popularity and scale of the spread of false information or when it notices a new trend or tactic. It then analyses the reasons for such popularity. Romania also has also had successful initiatives aimed at implementing media literacy into the educational system. The Center for Independent Journalism, together with other organisations, is currently running a media literacy project, though its rate of progress has been slow.

By pooling resources and expertise across various sectors, Spain has made strides toward building a more resilient information ecosystem. Moreover, participatory approaches involving citizens in media literacy programmes have worked to further enhance community cohesion.

[269] Margova, R., Dobreva, M., *Disinformation Landscape in Bulgaria*, EU DisinfoLab, June 2023, p. 6.

[270] Cognitive capture is defined as an inattentional blindness phenomenon in which the observer is too focused on instrumentation, task at hand, internal thought, etc. and not on wider aspects of the present environment. In this case, this may imply an excessive focus on the Russian narrative on a particular issue at the expense of understanding its relevance to the local political context and Russian strategic objectives.

Spain proposed a law in 2019 to protect the media sphere before elections, which was adopted in 2020 as a ministerial order[271]. It also called for collaboration with the private sector and civil society, recognising that their participation is essential to counter disinformation campaigns. This led to the 2022 establishment of the Forum Against Disinformation Campaigns, which gathered experts from different civil society sectors, including academia, media, and think tanks to coordinate with state institutions through different working groups focused on fighting disinformation. Additionally, a new regulation provides for charging media organisations with (partial) responsibility for developing media literacy skills among Spanish citizens. According to a report written by the Forum Against Disinformation Campaigns, gaps in institutional capacity can be seen in the lack of collaboration between universities (and other civil society actors) and local governments in the area of disinformation.

The challenge for both media and its consumers in Spain remains that, according to the Reuters Digital News Report, the country has one of the highest levels of "perceived news outlet polarisation". In the area of social coherence, Spain faces a significant challenge in its division into 17 autonomous communities, with some expressing separatists ambitions. Catalonia is the most prominent of these examples. In 2017, its autonomous government organised an illegal independence referendum, which was met with a police crackdown. One of the most important non-profit organisations fighting disinformation in Spain is Maldita.es. It focuses primarily on fact-checking through operations performed by its team of experts from multiple fields, including scientific disinformation, tech awareness, data and transparency, and scam-debunking. Its engineers are working on AI-based tools that could increase the efficiency of tracking and debunking disinformation. Iberifier was launched in 2021 and is also working to tackle disinformation in both Portugal and Spain through cooperation with around 90 researchers specialising in digital communication, disinformation, computing, and strategic analysis.

Conclusion

The increasing prevalence of echo chambers and selective exposure to media can lead to a populace that is less informed and more susceptible to disinformation. For instance, the rising influence of far-right groups and proliferation of conspiracy theories have highlighted vulnerabilities within a society that, while generally resilient, is not immune to the polarising effects of misinformation. Engaging with marginalised communities, addressing their specific vulnerabilities, and creating tailored media literacy programmes can help bridge the gaps created by that division. Moreover, transparency in communication and the establishment of trust between citizens and institutions will be pivotal in overcoming the scepticism that often arises in polarised environments.

The interplay between societal resilience, social cohesion, and media literacy is complex and multifaceted. While NGOs play a vital role in promoting these elements, the effectiveness of their efforts is contingent upon the dynamics of cooperation with governmental bodies and the media. Societies can bolster their resilience against foreign influence and misinformation by

[271] *Ministerial order PCM/1030/2020. The law provided for creating the Permanent Commission against Disinformation (or Standing Committee against Disinformation)*, Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, https://www.boe.es/eli/es/o/2020/10/30/pcm1030/dof/spa/pdf [last access: November 16, 2024].

prioritising collaborative initiatives and fostering an environment of trust and inclusion. As the challenges of polarisation and fragmentation continue to evolve, it is imperative for stakeholders to remain adaptable and proactive in their approaches, ensuring that the foundations of social cohesion and media literacy are continually strengthened.

Ultimately, a robust and resilient society will be one that actively engages its citizens, cultivates critical thinking, and works collectively to navigate the intricacies of the modern information landscape.

Recommendations for Stakeholders on FIMI, DISARM, OpenCTI, and ABCDE – Challenges and Opportunities

1. EU-Level (European External Action Service – EEAS)

The European External Action Service (EEAS) has provided the foundation for shared frameworks like DISARM, STIX, and OpenCTI, as well as conceptual structures like ABCDE. However, adoption across Member States remains uneven due to lack of knowledge and operational clarity. To address this, the EU should fund structured and recurring **training programs** on these tools, tailored for both government and NGO stakeholders. These programs should focus not only on technical use, but also on contextualising the strategic value of tools—e.g., using ABCDE to frame incidents holistically and DISARM to codify manipulation tactics. Clear, certified training paths would reduce misinterpretation and improve overall tool integration across sectors.

Secondly, the **standardisation of terminology and taxonomy** across the EU is essential. There is currently no universally adopted glossary for key terms like "incident," "manipulation technique," or "FIMI impact," which causes friction during crisis coordination. The EU should lead the effort to codify a shared vocabulary not just for FIMI incidents but also for key elements of the "FIMI Toolbox." Consistent language and classification will improve interoperability between Member States and enable faster, better-aligned crisis response efforts.

Thirdly, the EEAS should **develop and publish good practice manuals** to guide both state and non-state actors. These should offer tiered response plans based on incident typology, severity, and impact, integrating lessons from tools like OpenCTI and the Breakout Scale, and in some cases, provide a package of data about recognized incidents, networks, and networks of FIMI actors. Such manuals would serve as reference points for how to detect, assess, and react to incidents, whether at the pre-bunking, debunking, or legal attribution stage. In addition, these practices should be updated periodically and validated by practitioners across sectors.

Finally, to encourage stakeholders in Member States (including government agencies, researchers and NGOs) to use Open CTI and analytical frameworks, the EEAS, in cooperation with FIMI-ISAC (*Information Sharing and Analysis Centre*), should consider creating **the Open CTI 'starter pack'** that would facilitate the practical use of EU standards for FIMI detection and analysis by entities (e.g. RAS PoCs, analytical units in MFA, members of national Resilience Councils, NGOs, academics and private sector). This package should include TTPs from the DISARM framework and a set of data on open and attributed elements of disinformation distribution infrastructure used by major adversaries (Russia, China and Belarus), including domains, communication channels, accounts and other related resources. These may be also extended to full data sets on ongoing and historical (documented) campaigns. In return, the EEAS and FIMI-ISAC could receive standardised and structured reports from these entities, what would improve information exchange and enhance situational awareness.

2. National Government Institutions

Many Member States lack integrated systems for detection and response, leading to fragmented and reactive efforts. To overcome this, governments should **mandate the use of shared formats** such as STIX and DISARM in FIMI reporting and intelligence sharing. This would standardise inputs and outputs across agencies and contractors, ensuring compatibility and comparability of data. By requiring reports in these formats, governments would also indirectly stimulate adoption of EU-wide standards and foster more effective horizontal and vertical coordination.

Second, states should **establish inter-ministerial coordination bodies** that manage FIMI analysis and crisis response. Currently, responsibilities are often split between ministries of defence, foreign affairs, and digital affairs, resulting in duplicated or contradictory efforts. A centralised node can bridge gaps, harmonise workflows, and ensure adherence to unified FIMI terminology. Such coordination bodies could also serve as primary points of contact for EU-level mechanisms like RAS or FIMI-ISAC.

Third, governments must **invest in professionalising their knowledge ecosystems**, including the establishment of long-term supplier/vendor models. These should deliver ongoing, structured data feeds (e.g., via STIX), rather than relying on sporadic one-off reports. This continuous flow of structured threat intelligence allows for greater automation, early warning capabilities, and reduces the need for governments to maintain their own full-scale infrastructure. It also incentivises private-sector innovation in data provisioning, contributing to a more sustainable information defence ecosystem.

3. Non-Governmental Organizations (NGOs)

NGOs are essential to both monitoring disinformation environments and building societal resilience, but they face structural and technological barriers. To improve participation, the EU and national bodies should **co-develop simplified versions of OpenCTI** adapted for NGO use. While OpenCTI is a powerful tool, its current complexity deters non-technical actors. A simplified interface, combined with tailored training and documentation, would enable civil society to contribute more effectively to data sharing and incident mapping.

Secondly, NGOs should be **actively involved in shaping standard operating procedures and best practices** for FIMI detection and response. This collaboration must go beyond informal partnerships and include structured, co-authored manuals or playbooks. These resources should offer practical guidance for handling real-world scenarios—e.g., reacting to coordinated campaigns, navigating legal grey zones, or working with platforms to restrict amplification. Including NGOs in such processes reinforces their role as trusted partners and increases the system's resilience through diversity of perspective.

Lastly, NGOs must receive support to **adopt standardised analytical frameworks** like DISARM and STIX. While tools like ABCDE offer holistic scoping benefits, NGOs often lack the capacity or knowledge to move beyond that into structured threat categorisation and exchange. Regular, publicly funded training—coordinated through entities like FIMI-ISAC—should be made available, enabling civil society to generate, store, and share knowledge in formats compatible with state systems. Empowering NGOs in this way enhances collective

defence and strengthens the "whole-of-society" approach essential to countering modern information threats.

4. Cooperation among various stakeholders (EU, NGOs, state and private sector)

For NGOs, to **effectively cooperate with the European Union institutions clear communication channels are needed**. Currently, several NGOs do work at joint projects for the European Commission, mostly in the form of grants from the DG CNECT. The remaining majority, however, even if they share their findings with the European Commission they mostly do it throughout their personal contacts within the EC – to fully enhance the NGOs potential, it is thus needed to provide the NGOs with clear information about who and how should they address if they want to share their findings with the EC. On the EC website, an establishment of clear contact channels for the NGOs and think tanks that are countering disinformation is needed. Currently, there are three available options of contact with the DG CNECT that include:

1) Calling the official number of the Directorate General,
2) Press inquiries,
3) General formula for everyone to contact the DG CNECT.

For NGOs to fully use the capabilities that DISARM and ABCDE frameworks open when it comes to interoperability of research, providing such a contact that will be present on the website is needed. In order to make use of the research sent by a variety of NGOs, a person or persons should be designated from the side of the EC in order to respond to the information sent by the NGOs and, if needed, share it further with the EC team. Responsiveness and clear feedback is needed to fully enhance the diverse experience of a variety of the NGOs from all of the EU Member States, especially that they all function in different ecosystems.

Later, the establishment of certain communication channels with the most willing and active NGOs working in the field of countering disinformation is needed. Frameworks, like DISARM or ABCDE, are designed not only for the sake of the methodology and clear data itself; rather, their main goal is enhancing the interoperability of research that could later on lead to more thorough investigations and broader outlook of foreign coordinated and inauthentic behaviour. Thus, to fully use their potential, more than just clear contact details is required. Establishing the designated communication channels between the European Commission and the NGOs is desirable.

Data- and knowledge sharing is a key for a fruitful cooperation between the European Commission and the NGOs. To fully use the capabilities originating from the common frameworks like DISARM the Commission should:

- Create the channels for the effective data-sharing for the data that the NGOs believe are important to be shared with the Commission, especially in regards to the Digital Services Act.
- Use the above-mentioned channels to share the data with the NGOs, especially in time periods when the number of disinformation attacks increases, for example throughout the elections.
- Create and govern a database where the NGOs, if willing, could share certain disinformation incidents with the use of common frameworks, notably the DISARM framework.

Access to information – to make the most effective use of the joint efforts to counter disinformation, especially when it comes to NGOs that are countering disinformation but are less aware of the existing research frameworks, the European Commission should provide relevant resources on its website. Information should focus first on the research frameworks and information relevant for the NGOs to conduct their job. Second, however, these communiques should include all the necessary information about the ongoing projects of the Commission that could involve the NGOs, for example the existing pre-election RRSs. For the NGOs to fully use the capabilities that are in the ABCDE and DISARM frameworks, it could be useful to see long-term financing capabilities from the side of the Commission.

To fully use the capabilities granted by the common use of similar methodological frameworks like ABCDE or DISARM, the reaction from the side of **Very Large Online Platforms is needed (VLOPs)**. Certainly, direct cooperation between the NGOs and platforms seems unlikely. However, with the European Commission as the intermediary this can evolve into a more fruitful cooperation. Thus:

- The European Commission should establish rapid response mechanisms, under the DSA, similar to those conducted throughout the elections in the European Union.
- Those mechanisms should include representatives from the EC, the platforms (namely: Meta, TikTok and YouTube - signatories of the Code of Practice) and the NGOs.
- Via the RRS, the NGOs should be granted a distinct and quick reporting route where they could report the potentially violative content effectively.

Similarly to the cooperation with the EC and with the VLOPs, the NGOs could benefit from clear communication from the side of the public administration, preferably in the form of Resilience Councils or ISAC-s, direct messaging, as well as a provision of relevant sources that could be useful for the NGOs work.

According to the desk research and conducted interviews NGOs and media organisations, although familiar with the existence of FIMI analysis tools, still do not possess a significant experience in implementing them. Therefore, some of their analyses can lack clear methodology or be incoherent with the requirements from the EU or state institutions. In order to be able to exert more effective pressure on governments or the EU to take action after their reports of FIMI/disinformation incidents, it would be necessary to apply methodologies such as DISARM STIX or ABCDE, which will allow all involved stakeholders to operate within the same conceptual framework.

So far, the NGOs and fact-checking organisations involved in countering disinformation use a variety of analytical frameworks, including ABCDE, DISARM, Open CTI and others. This can hinder their cooperation and interoperability as these tools operate with different concepts and languages. Therefore, it would be useful to create a guideline for these stakeholders that could facilitate exchange of knowledge, information and data. The NGOs could also benefit from tools facilitating conversion of files and data between different disinformation tools frameworks.

As our research proved, NGOs and fact checking organisations are more advanced in implementing FIMI and disinformation analyses framework than state institutions. Additionally, their work also often involves direct cooperation with citizens who indirectly (i.e. through communication channels) participate in reporting and analysing suspicious content.

However, to benefit from such a robust approach on the side of these organisations systemic, rather than just technical actions are needed. Most of the third sector and media operate in highly uncertain and unstable conditions, with unclear financial futures for their employees and the organisations themselves, which hinders institutional continuity and internal coherence. The range and reception of their reporting is further inhibited by the monopoly of social media platforms who do not face the same financial constraints (in terms of taxes and other fees) as traditional media and NGOs. Given that the same platforms play a major role in spreading disinformation and often act against traditional media and NGOs, this unequal competition is an important obstacle for the civil society's fight against FIMI and disinformation.

Summary of the report

This report provides a comprehensive analysis of the European Union's strategies, policies, and institutional capacities to counter foreign information manipulation and interference (FIMI).

It begins by tracing the evolution of disinformation into the broader concept of FIMI, exploring the impact of new technologies that enable foreign actors to spread harmful false content as well as the EU's standardisation efforts for detection and response. The first section highlights how the EU has addressed FIMI through sanctions against threat actors and by establishing frameworks to enhance resilience.

The research emphasises efforts to standardise FIMI detection through the use of unified terminology to create a shared understanding of the threat and promote collaboration across society. Additionally, it explores the development of a common framework to optimise knowledge generation, sharing, and activation, grounded in open-source and collaborative standards.

The subsequent chapter delves into EU Member States' strategies, strategic documents, and policy frameworks, offering comparative insights and case studies to illustrate varying national approaches. Greater attention is given to states that have adopted dedicated strategies and general and sectoral policies to address the problem.

The report also examines institutional capacities within EU Member States, emphasising the use of digital tools, inter-agency cooperation and coordination, and partnerships with NGOs to tackle FIMI effectively.

Further, the report evaluates regulatory measures across EU Member States, including the impact of EU-wide regulations like the Digital Services Act, to understand their effectiveness in curbing disinformation and fostering accountability among media and internet platforms. It also emphasises the importance of societal resilience, democracy, and addressing fragmentation and polarisation as key factors in combating FIMI.

Lessons from Ukraine's systemic approach to FIMI based on its experience in fighting Russian disinformation, including its emphasis on institutional capacity and multi-stakeholder cooperation, are presented as a critical case study.

The report deliberately refrains from synthesising these insights into actionable recommendations. Its ambition, however, is to provide valuable knowledge based on a consistently applied research approach and methodology to facilitate the European Union and its member states in developing effective coordinated policy practices to support the fight against FIMI.

The pressing need of such policies is even better understood in light of the fact that the negative consequences of FIMI derivative threats, correctly diagnosed by the EU, have also been recognised by the wider democratic community. At their April 2024 meeting, the G-7 foreign ministers stated: "FIMI negatively affects the ability of citizens to make rational, informed decisions, which lies at the very heart of our democratic institutions, and aims at undermining confidence in democratic governments and societies. Disinformation can be used to polarise society; it often supports violent extremist activities and is fuelled by malicious foreign players.

Online disinformation campaigns are widely used by various malign actors to create and exacerbate tensions."[272]

This report focuses on understanding FIMI-related threats and the varied approaches of EU Member States in addressing them. Our research team also hopes that its observations and inferences will help in improving the systemic capacity of the EU nations and the union as a whole to effectively respond to the problem.

[272] *G7 Foreign Ministers' Statement in Italy. Addressing global challenges and fostering partnership*, April 2024, U.S. Department of State, https://www.state.gov/g7-italy-2024-foreign-ministers-statement-on-addressing-global-challenges-fostering-partnerships/ [last access: October 30, 2024].

APPENDIX 1

Lessons learned from Ukraine

Ukraine is one of the most experienced countries in the world in the fight against Russian disinformation campaigns. Over the last decade, Ukraine has faced Russian actions oriented towards interference in political processes, destabilisation, discrediting in the international arena, as well as information operations in support of its military invasion. The Ukrainian experience is extremely valuable for the EU countries.

A Hybrid CoE and DFRLab report[273] identified ten best practices for countering disinformation used by Ukraine, based on lessons learned from the country's experience during its hybrid war with Russia from the time of Euromaidan/Revolution of Dignity (late 2013 into early 2014) to the February 24, 2022, Russian full-scale invasion of Ukraine. In many cases, the Ukrainian approach differs with the approaches developed by the EU and individual member states.

Table 9: Comparison of Ukrainian and EU approaches to systemic countering FIMI

	Ukraine	EU and its member states
Building a system of resilience against FIMI	Based on state institutions and NGOs	Based on state institutions and NGOs
Coordination	Distributed/decentralised	Drive towards centralisation
Cooperation between civil society and the state	Informal, flexible	Formalised, based on procedures and bureaucracy
Information flow between NGOs and government	Two-way	One-way
FIMI incident response approach	Immediate	Dependent on the scale and harmfulness of the incident
Detection and analysis methods	Differentiated	Drive towards standardisation
Organisation of teams	Mass (involving informal groups of volunteers)	Small, specialised analytical teams
Perception of duplication of tasks (overlapping)	Positive	Negative
Readiness to use countermeasures that impose costs (e.g., sanctions, blockades,	High	Low

[273] See: Kalenský, J. & Osadchuk, R., *How Ukraine fights Russian disinformation: Beehive vs mammoth*, Hybrid CoE Research Report 11, January 2024.

naming and shaming, putting public pressure on propagandists) on the adversary		
Use of satire and parody	High	Low

Source: Own study based on Kalenský, J., Osadchuk, R., *How Ukraine fights Russian disinformation: Beehive vs mammoth*, Hybrid CoE Research Report 11, January 2024.

Systemic approach to detection and response to FIMI

According to Ukrainian practitioners, building a robust and solid system for monitoring the information space and responding rapidly to disinformation campaigns through debunking, refuting lies, and other proactive measures is fundamental for assuring state resiliency to FIMI. In doing so, they emphasise that speed of response is key - rather than considering whether it is appropriate to act at all. This approach differs from the philosophy of the EU and its individual member states. According to practitioners from Ukraine, it is speed that makes debunking effective. Moreover, keeping a database of debunked cases makes it easier to respond to further (including new) narrative lines[274]. In doing so, it is also possible to draw attention to the repetitiveness of their message, which cannot be limited to one-off debunking, or naming and shaming.

Institutional capacity

Inter-institutional complementarity (and even overlapping or duplication of tasks) is an advantage and should not be seen as a mistake. Each relevant state and military institution should have its own team for monitoring and analysis of the information space, using its own methods of detection and analysis. This sharply contrasts with the approach of the EU and member states seeking standardisation (based on DISARM-STIX, ABCDE frameworks).

According to Ukrainian experts, diversity is an asset because it increases the independence and creativity of entities and individual actors. The dispersion of competencies also increases their resilience to disruptions, such as cyber-attacks (e.g. DDoS). Even when one institution is blocked, others can continue to operate.

In Ukraine, situational awareness is provided primarily by two institutions created by the Ukrainian government in March 2021: the Centre for Countering Disinformation (CCD) [within the National Security and Defence Council] and the Centre for Strategic Communications (CSC) [within the Ministry of Culture and Information Policy], alongside monitoring work conducted by various NGOs (among others, this includes StopFake, Detector Media, Ukrainian Crisis Media Centre, Internews, and Texty).

At least two unifying forces work to coordinate counter disinformation efforts under the umbrella of the NDI Disinformation Hub and in cooperation with the CSC. It has communicated with civil society from its inception, understanding the immense importance of the expertise concentrated in the NGO sector. However, this coordination is informal in nature: "the ecosystem of people dealing with Russian disinformation was created a while ago, and it became a self-coordinating group to which people added trusted contacts"[275].

[274] Ibidem, p. 10-13, 16.
[275] Ibidem, p. 18.

The significant human and financial resources allocated by numerous institutions to countering FIMI are crucial. Indeed, limiting them will lead to inefficiency and ineffectiveness in the system. Underfunding and insufficient human resources are a problem for many teams analysing FIMI or responsible for StratCom in EU countries. In Ukraine, hundreds of people are involved in combating disinformation in Ukraine, though we don't have specific figures. In doing so, however, they also consider volunteers ("elves", as they are known in the Baltic states) acting alone or in small groups.

Cooperation between state and non-state entities

The centre of gravity of the counter FIMI system must be based on civil society ("information warriors") and not rely only on the state administration, which is unable to detect and respond effectively to FIMI at the local and national level concurrently. Bottom-up initiatives with their own communication channels play an important role. "Cooperation between civil society and government was often flexible and informal, allowing it to focus on specific, organic problem-solving rather than the creation of formal and systematic procedures for collaboration. It is built on the principle of horizontal cooperation, whereby partners could amplify each other's work by sharing their expertise and findings, or through joint programmes, training, and problem-solving."[276]

Importantly, the flow of information between state and NGOs is two-way. Thanks to this model of state-NGO cooperation, the detection of disinformation is rapid, enabling an immediate response. As the authors of the report point out, "these activities involved individual activists as well as civil society groups and private businesses. Some were loosely connected, while others were more organized as a form of 'territorial defence' for the information space. Regardless of their background or organisational structure, they take on a number of tasks, including debunking false information and disseminating truthful information, calling out Russian and pro-Russian voices, and monitoring the information space, with some even engaging in sophisticated cyberattacks against targets in Russia."[277]

Building resilience and response capabilities

Contingency plans must be in place for times of crisis and war, including alternate communication channels, additional infrastructure, and teams capable of immediate crisis engagement. Communication channels must be tailored to their audience to reach them easily and effectively (e.g., social media). Audiences cannot be counted on to find their way to receive messages from the government. Starting these activities after a conflict has already erupted will be considerably more difficult.

Ukrainian government bodies started to develop their plan in the summer of 2021, but these preparations stepped up as intelligence sources, civil society monitoring, and media reporting revealed increasing signs of an attack. To confront the problem, it was necessary to plan not just general contingency procedures, such as splitting an office into multiple groups in different regions, but also specific prepared messages and instruments that could be deployed at short notice. This preparation included informing Ukrainian society of the impending danger. Government officials also prepared materials on what people should do in case of an emergency[278].

The Ukrainian government established the "United News telethon", a joint effort of various national channels that started broadcasting on February 24, 2022. The channel provided verified

[276] Ibidem, p. 21-22.
[277] Ibidem, p. 15.
[278] Ibidem, p. 24.

information, serving as a crucial source for the Ukrainian public at the beginning of the invasion. Awareness of an impending conflict should also prompt the preparation of specific material in response to anticipated information operations by the adversary. Indeed, making certain intelligence information public[279] (such as the actions of U.S. intelligence agencies revealing Russia's preparations for war, or false flag operations designed to provide a pretext for invasion) enhances the ability to pre-bunk.

To effectively counter FIMI, it is also necessary to have and use measures to punish the adversary by imposing costs on them, influencing their behaviour, and limiting their ability to conduct hostile actions. Imposing sanctions, blocking domains, and naming and shaming are often controversial and questionable in the EU for fear of censorship and violation of freedom of expression.

In 2014, Ukraine banned Russian state TV channels. In 2017, Petro Poroshenko's administration blocked access to Russian social media sites VKontakte and Odnoklassniki, a Russian mail provider and search engine, and several pseudo-media sites; this measure was later extended by Volodymyr Zelensky. In 2021, Zelensky's administration banned TV channels and their information ecosystem (i.e., websites, social media channels, direct messaging platform channels), including those that did not directly belong to the Russian state but spread the same messages[280]. These included channels belonging to pro-Kremlin oligarch Viktor Medvedchuk.

After the Russian invasion, cooperation with the private sector played an important role. For example, Google has blocked 170 YouTube channels that violated the Ukrainian criminal code. A special form delivered to Ukrainian government bodies indicated which law was violated by a channel[281]. While considering bans and blocking domains may seem the most extreme option, there are also other countermeasures that impose costs on an adversary, such as naming and shaming. In 2022, several Ukrainian ministries and state services, including the Military Intelligence Service and the SSU, published a joint statement on "The protection of Ukraine's information space from Russian hostile Telegram channels"; in it, they revealed to the public a list of 100 such channels connected to Russia[282]. The CCD, in collaboration with other state institutions, later created a blacklist of "information terrorist" Telegram channels[283]. They also compiled a list of international influencers who amplified Russian propaganda[284].

[279] Paxton, J., *Operationalizing Intelligence. Shaping the Information Environment and Galvanizing Western Action Against Russia*, "The Three Swords", no. 38, 2022, p. 12-17.
[280] Kalenský, J., Osadchuk, R., *How Ukraine fights…*op.cit., p. 27.
[281] Ibidem, p. 28.
[282] *100 Russian Telegram Channels That Mimic Ukrainian Ones*, Centre for Strategic Communication and Information Security, 2022, https://spravdi.gov.ua/en/100-russian-telegram-channels-that-mimic-ukrainian-ones/
[283] *CCD Announces an Updated List of Infoterrorist Channels Operating in Ukraine*, Center for Countering Disinformation, 2023, https://cpd.gov.ua/en/warnings/ccd-announces-an-updated-list-of-infoterrorist-channels-operating-in-ukraine/, [last access: November 7, 2024].
[284] *Спікери, Які Просувають Співзвучні Російській Пропаганді Наративи* [Speakers who promote narratives consistent with Russian propaganda], Center for Countering Disinformation, 2022. https://web.archive.org/web/20220801015336/https://cpd.gov.ua/reports/, [last access: November 7, 2024]. In contrast to the blacklists, the CSC also created "whitelists" of sources that could be trusted, including Ukrainian government channels.

Such activity did not come from the government alone. The Institute of Mass Information released a blacklist of people spreading genocidal Russian rhetoric[285], and Vox Ukraine created a database of Russian propaganda appearing in European outlets[286].

Responding to disinformation with humour (including irony, satire, jokes, and memes) allows for wider reach, improves the morale of society, and undermines the reputation of an opponent. The NAFO fellas phenomenon is an example of this[287]. Humorous content is more attractive and goes viral more often, reaching audiences outside of the usual filter bubble. It helps to discredit, ridicule, and mock the enemy. It also helps to gain the sympathy of neutral audiences. In the case of Ukraine, it worked to undermine the credibility of the Kremlin and its propaganda channels. The effectiveness of this tactic, however, is also well known and exploited by disinformers.

Actions are more important than words. No debunking or strategic communication is as effective as real action. The Ukrainian military operation in the Kursk region on Russian territory in the middle of 2024 became a serious problem for Kremlin propaganda and a very effective tool for countering it. The inhabitants of the region, deprived of any assistance from the state, saw first-hand the lies they were being told. Not giving credence to the government's assurances of a "stable situation", "organising the evacuation of the population", or "providing humanitarian aid" – they spared no criticism of the authorities in material published on social media[288].

In the case of Ukraine, pro-Russian sympathies were largely eliminated after Russian rockets and artillery began raining down on Ukrainian cities. Images of Russian war crimes committed in Ukraine consolidated the West on the side of Ukraine but did not change the attitudes of societies in the Global South. Russia has denied its war crimes and questioned its responsibility. An example of this is the falsification of the public's perception of the Bucha crime. Despite unequivocal evidence, Russian disinformation channels claimed that the massacre was staged by Ukrainians.

Conclusion

The West can learn from the Ukrainian experience in countering FIMI in wartime. At the same time, not all the methods used by Ukraine are applicable to non-warring democratic states. According to Ukrainian experts, EU countries are insufficiently countering Russian disinformation. This particularly concerns low willingness to apply countermeasures that impose costs on Russia, like blocking disinformation channels.

[285] Нестеренко, Альона, Роман Головенко, and Оксана Романюк. «Ядерний Удар По Вінниці Та Гулаг Для Запорізьких Учителів. Геноцидна Риторика Російської Пропаганди [A Nuclear Attack on Vinnytsia and the Gulag for Zaporizhzhia Teachers. The Genocidal Rhetoric of Russian Propaganda]." Інститут масової інформації, 2022, https://imi.org.ua/monitorings/yadernyj-udar-po-vinnytsi-ta-gulag-dlya-zaporizkyh-vchyteliv-genotsydna-rytoryka-rosijskoyi-i48786.

[286] VoxCheck Team. "Propaganda Diary 2022–2023: Voxcheck Presents the Database of Russian Propaganda in the European Mass Media." Vox Ukraine, 2023. https://voxukraine.org/en/propaganda-diary-2022-2023-voxcheck-presents-the-database-of-russian-propaganda-in-the-european-mass-media, [last access: September 2, 2024]..

[287] See: Giles, K., *Humour in online information warfare: Case study on Russia's war on Ukraine*, Hybrid CoE, November 2023.

[288] EUvsDisinfo, *The Kursk Problem*, "Disinformation Review", https://euvsdisinfo.eu/the-kursk-problem/, August 22, 2024, [last access: November 2, 2024].

There should be no illusion - information warfare will continue, and we will still have competition in the information sphere. It is a war that cannot be won; no winner or loser can be identified, and only its harmful effects can be mitigated. There is no theory of victory in information warfare. The process exploits new events from an endless news cycle, applying tried and tested propaganda techniques to manipulate facts in narrative weapons. The adversary develops its TTPs and adapts to our countermeasures. The potential range of tools, topics, and platforms is constantly growing, making the cycle indefinite while deepening it.

Notes:

1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a Framework for Networked Defence, European Union External Action Service, February 23, 2023, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en [last access: April 7, 2024].

2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence, European External Action Service, January 2024, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en [last access: September 17, 2024].

100 Russian Telegram Channels That Mimic Ukrainian Ones, Centre for Strategic Communication and Information Security, 2022, https://spravdi.gov.ua/en/100-russian-telegram-channels-that-mimic-ukrainian-ones/ [last access: October 23, 2024].

2018 EU Code of Practice on Disinformation, European Commission, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation [last access: July 9, 2024].

2021 StratCom Activity Report, Strategic Communication Task Forces and Information Analysis Division, March 24, 2022, https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis-division_en [last access: July 29, 2024].

2022 Reuters Institute Digital News Report, Reuters Institute, https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/ireland [last access: December 11, 2024].

2024 World Press Freedom Index, Reporters Without Borders, https://rsf.org/en/index [last access: December 11, 2024].

955 Dėl Strateginės Komunikacijos Nacionalinio Saugumo Srityje Koordinavimo Tvarkos Aprašo Patvirtinimo, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3f019ef4eb8511eab72ddb4a109da1b5?jfwid=2r1mkfzc [last access: November 1, 2024].

A National Cyber Security Strategy, Government Offices of Sweden/The Ministry of Justice, 2016, https://www.government.se/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213 [last access: July 26, 2024].

A Strategic Compass for Security and Defence, European Union External Action Service (EEAS), March 24, 2022, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf [last access: April 14, 2024].

About the Cyprus Confidential Investigation, International Consortium of Investigative Journalists, November 14, 2023, https://www.icij.org/investigations/cyprus-confidential/about-cyprus-confidential-investigation/ [last access: December 4, 2024].

Act C of 2012 on the Criminal Code, 2012, Section 227, Section 337/1, Section 338, https://www.refworld.org/legal/legislation/natlegbod/2012/en/78046 [last access: August 1, 2024].

Agenzia per la Cybersicurezza Nazionale National Cybersecurity Strategy 2022 – 2026: Implementation Plan, Presidenza del Consiglio dei Ministri 2022, https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza [last access: June 27, 2024].

Aktualizirana strategiâ za nacionalna sigurnost na Republika B"lgariâ, March 23, 2018, https://www.me.government.bg/files/useruploads/files/akt.strategiq2020.pdf [last access: July 20, 2024].

Alaphilippe, A., *Disinformation Landscape in Belgium*, EU DisinfoLab, 2023, https://www.disinfo.eu/wp-content/uploads/2023/05/20230509_BE_DisinfoFS.pdf [last access: June 6, 2024].
Andric, A., *Sweden – National Digitalisation Strategy for the School System 2023-2027*. The European Union Digital Skills & Jobs Platform, July 24, 2023, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/sweden-national-digitalisation-strategy-school-0 [last access: November 28, 2024].
Artificial Intelligence Act, European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf [last access: March 13, 2024].
Atlas Konspiraci, https://www.atlaskonspiraci.cz/ [last access: December 2, 2024].
ATT&CK Matrix for Enterprise, https://attack.mitre.org/ [last access: August 14, 2024].
Bayer, J., *The European Response to Russian Disinformation in the Context of the War in Ukraine*, Hungarian Journal of Legal Studies, 64 (4), 2023.
Berlińska-Wojtas P., *Bezpieczeństwo informacyjne RP w dobie COVID-19*, Zeszyty Naukowe.
Bleyer-Simo, K., *Disinformation Landscape in Hungary*, EU DisinfoLab, June 2024, https://www.disinfo.eu/wp-content/uploads/2023/06/20230521_HU_DisinfoFS.pdf [last access: August 2, 2024].
Blocman, A., *Platform Regulation and DSA Implementation: ARCOM and European Commission Increase Cooperation*, IRIS Legal Observations of the European Audiovisual Observatory, 2024, https://merlin.obs.coe.int/article/9903 [last access September 12, 2024].
Bryjka, F. *Unravelling Russia's Network of Influence Agents in Europe*, PISM Spotlight, No. 24, https://pism.pl/publications/unravelling-russias-network-of-influence-agents-in-europe [last access: April 5, 2024].
Bundesregierung, *Stelle gegen ausländische Desinformation inimmt Arbeit auf*, June 17, 2024, https://www.deutschlandfunk.de/stelle-gegen-auslaendische-desinformation-inimmt-arbeit-auf-100.html [last access: June 20, 2024].
Capitalisation des campagnes et incidents de manipulation de l'information dans OpenCTI. Doctrine d'utilisation de VIGINUM, Version 1.0, January 2024, https://github.com/VIGINUM-FR/Doctrine-OpenCTI/blob/main/SGDSN_VIGINUM_DoctrineOpenCTI.pdf [last access: June 5, 2024].
Catalonia's Bid for Independence from Spain Explained, BBC, October 18, 2019, https://www.bbc.com/news/world-europe-29478415 [last access: December 11, 2024].
CCD Announces an Updated List of Infoterrorist Channels Operating in Ukraine, Center for Countering Disinformation, 2023, https://cpd.gov.ua/en/warnings/ccd-announces-an-updated-list-of-infoterrorist-channels-operating-in-ukraine/ [last access: November 7, 2024].
Charlevoix Commitment on Defending Democracy from Foreign Threats, Charlevoix, 2018, https://publications.gc.ca/collections/collection_2018/amc-gac/FR5-144-2018-30-eng.pdf [last access: October 23, 2024].
Cheskin, A., *Identity and Integration of Russian Speakers in the Baltic States: A Framework for Analysis*, Ethnopolitics, January 1, 2015.
Chłoń T., Kupiecki R., *Towards FIMI Resilience Council in Poland. A Research and Progress Report*, https://saufex.eu/research [last access: December 20, 2024].
Comité Stratégique du Renseignement et de la sécurité, Stratégie de Sécurité Nationale, December 1, 2021, p. 19, https://www.egmontinstitute.be/app/uploads/2022/02/NVS_Numerique_FR.pdf [last access: June 9, 2024].
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan, European Commission, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0091* [last access: March 24, 2024].

Comunicato Stampa 16 Novembre 2017, Autorità per le Garanzie nelle Comunicazioni, November 16, 2017, https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-16-novembre-2017, Autorità per le Garanzie nelle Comunicazioni [last access: June 27, 2024].

Corina, A., *Italy*, Reuters Institute, 2024, https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024/italy [last access: December 2, 2024].

Costello, T.H., Pennycook, G., & Rand, D.G., Durably Reducing Conspiracy Beliefs Through Dialogues with AI, *Science*, Vol. 385, Issue 6714, September 3, 2024. DOI: 10.1126/science.adq1814.

Council Regulation (EU) 2024/1745 of 24 June 2024 Amending Regulation (EU) No 833/2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine, European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401745 [last access: June 26, 2024].

Council Regulation (EU) No 269/2014 of 17 March 2014 Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine, European Union, March 17, 2014, ttps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0269 [last access: October 29, 2024].

Counter-Disinformation Literature Review, U.S. Department of State, July 2023, https://www.state.gov/counter-disinformation-literature-review/ [last access: October 31, 2024].

Countering Disinformation Effectively: An Evidence-Based Policy Guide, Carnegie Endowment for International Peace, January 2024, https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en [last access: October 31, 2024].

Countering Information Influence Activities – A Handbook for Journalists, Swedish Civil Contingencies Agency/Swedish Psychological Defence Agency, https://mpf.se/download/18.5ed1a83718d2a5fd639d524/1706648817558/countering-information-influence-activities-a-handbook-for-journalists.pdf [last access: July 26, 2024].

Countering Information Influencing - Preliminary Report/Informaatiovaikuttamisen Torjunta – Esiselvitys, Finnish National Emergency Supply Agency/Huoltovarmuuskeskus, December 1, 2021, https://www.huoltovarmuuskeskus.fi/files/d601de13993e8873d2d66bf379c35f13309dc42a/hvk-informaatiovaikuttamisen-torjunta-esiselvitys.pdf [last access: December 2, 2024].

Croatia: Dora Kršul and Telegram.hr Accused by the Minister of Culture and Media of Publishing "Malicious Fake News", European Federation of Journalists, europeanjournalists.org/ [last access: November 26, 2024].

Croatian Fact-Checkers' War on Fake News Draws Bias Charge [last access: November 26, 2024].

Culloty, E. *Disinformation Landscape in Ireland*, EU DisinfoLab [last access: November 11, 2024].

Cybersicherheitsstrategie für Deutschland, Bundesministerium des Innern 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.html [last access: September 20, 2024].

Cyprus Criminal Code, https://www.cylaw.org/nomoi/arith/CAP154.pdf [last access: July 14, 2024].

Danish National Strategy for Cyber- and Information Security 2022–2024, Danish Agency for Digital Government, December 2021, https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/strategic-objectives/ [last access: November 29, 2024].

Danish Security and Defence Towards 2035, Danish Ministry of Defence, September 2022, https://www.fmn.dk/globalassets/fmn/dokumenter/strategi/rsa/-regeringens_security-policy-report_uk_web-.pdf [last access: November 29, 2024].

Danmarks Digitaliseringsstrategi Sammen Om Den Digitale Udvikling, Danish Ministry of Finance, May 2022, https://www.regeringen.dk/media/11324/danmarks-digitaliseringsstrategi-sammen-om-den-digitale-udvikling.pdf [last access: November 29, 2024].

De Agostini, L., Catena, B., & Autolitano, S.*Mitigating AI-Generated Disinformation: A Cyber Collaborative Framework for G7 Governance*, Policy Brief, Think7, May 2024, https://think7.org/wp-content/uploads/2024/05/T7it_tf1_pb01.pdf [last access: October 23, 2024].

Décret n° 2021-1587 du 7 Décembre 2021 Portant Autorisation d'un Traitement Automatisé de Données à Caractère Personnel Dans le But d'Identifier les Ingérences Numériques Étrangères, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044454057 [last access: May 14, 2024].

Décret n° 2021-922 du 13 Juillet 2021 Portant Création, Auprès du Secrétaire Général de la Défense et de la Sécurité Nationale, d'un Service à Compétence Nationale Dénommé « Service de Vigilance et de Protection Contre les Ingérences Numériques Étrangères, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361 [last access: May 14, 2024].

Defalsif-AI, Austrian Presse Agentur, https://science.apa.at/project/defalsifai-en/ [last access: October 29, 2024].

Defence of Democracy – Commission Proposes to Shed Light on Covert Foreign Influence, European Commission, *https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453* [last access: December 12, 2024].

Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016–2020, Global Challenges Election Disinformation, https://successfulsocieties.princeton.edu/sites/g/files/toruqf5601/files/TM_Estonia_Election_FINAL%20edited_JG.pdf [last access: November 29, 2024].

Deibler D., *Strengthening Digital Resilience*, DAD-CDM, April 23, 2025, https://dad-cdm.org/strengthening-digital-resilience/ [last access: 05.06.2025].

Denmark: Education and Training Media Literacy and Safe Use of New Media, March 25, 2024, European Commission, https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/denmark/68-media-literacy-and-safe-use-of-new-media [last access: November 28, 2024].

Deutscher Bundestag - 71. Sitzung, n.d., https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1022350-102235 [last access: November 2, 2024].

Disinformation and Foreign Interference: Speech by High Representative/Vice-President Josep Borrell at the EEAS Conference, Brussels, January 21, 2024, https://www.eeas.europa.eu/eeas/disinformation-and-foreign-interference-speech-high-representativevice-president-josep-borrell-eeas_en [last access: October 21, 2024].

Disinformation, Propaganda and Fake News in Croatia, Croatian Wikipedia Disinformation Assessment 2021, Meta, wikimedia.org [last access: November 26, 2024].

Disinformation, Propaganda and Fake News in Croatia, www.croris.hr/crosbi/publikacija/prilog-knjiga/76122 [last access: December 2, 2024].

Disinformation: AEM Croatia Publishes Landmark Study, European Platform of Regulatory Authorities, epra.org [last access: November 26, 2024].

DON'T BE FOOLED -A Handbook to Help You Recognise and Deal with Disinformation, Misleading Information, and Propaganda, The Psychological Defence Agency, 2023, https://www.bliintelurad.se/assets/uploads/2024/04/Handbok-Dont-be-fooled-2023-EN-TA_240417.pdf [last access: September 15, 2024].

ECAS, *Civil Society Against Disinformation* [last access: November 26, 2024].

Elektronisko Plašsaziņas Līdzekļu Likums, Latvijas Vēstnesis, 118, July 28, 2010, https://likumi.lv/ta/id/214039-elektronisko-plassazinas-lidzeklu-likums [last access: September 12, 2024].

European Media Freedom Act, European Commission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en [last access: March 15, 2024].

Feeling Cornered: An Analysis of the Russian-Speaking Minority in Estonia, European Website on Integration, https://migrant-integration.ec.europa.eu/library-document/feeling-cornered-analysis-russian-speaking-minority-estonia_en [last accessed July 11, 2024].

FIMI-ISAC Collective Findings I: Elections, October 2024, https://fimi-isac.org/wp-content/uploads/2024/10/FIMI-ISAC-Collective-Findings-I-Elections.pdf [last access: September 23, 2024].

Finland's Cyber Security Strategy 2024–2035, Finland's Prime Minister's Office, October 2024, https://julkaisut.valtioneuvosto.fi/handle/10024/165893 [last access: November 28, 2024].

Finnish National Emergency Supply Agency Builds Capabilities to Counter Information Influencing/ Huoltovarmuuskeskus rakentaa kykyä torjua informaatiovaikuttamista, Finnish National Emergency Supply Agency/Huoltovarmuuskeskus, August 17, 2022, https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuskeskus-rakentaa-kykya-torjua-informaatiovaikuttamista# [last access: December 3, 2024].

Fiser, S.Z. & Caks, P., "Strategies for the Minimisation of Misinformation Spread Through the Local Media Environment," *Journalism Practice*, 2023, pp. 2241-2262, DOI: 10.1080/17512786.2023.2183235 [last access: November 26, 2024].

Fjäder, C. & Schalin, J., *Building Resilience to Hybrid Threats: Best Practices in the Nordics*, The European Centre of Excellence for Countering Hybrid Threats (HybridCoE), May 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf [last access: June 17, 2024].

Foro Contra las Campañas de Desinformación en el Ámbito de la Seguridad Nacional, Trabajos 2023, *Catálogo de publicaciones de la Administración General del Estado*, https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf [last access: November 18, 2024].

Freedom of Speech Objection to Fake News Criminalisation Push, July 04, 2024, https://cyprus-mail.com/2024/07/04/freedom-of-speech-objection-to-fake-news-criminalisation-push/ [last access: July 14, 2024].

G7 Foreign Ministers' Statement in Italy: Addressing Global Challenges and Fostering Partnership, U.S. Department of State, April 2024, https://www.state.gov/g7-italy-2024-foreign-ministers-statement-on-addressing-global-challenges-fostering-partnerships/ [last access: October 30, 2024].

G7 Working Group Meeting on Disinformation at the Farnesina, July 3, 2024, https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2024/07/riunione-alla-farnesina-del-gruppo-di-lavoro-g7-su-disinformazione/ [last access: October 24, 2024].

Gallagher, A., O'Connor, C., & Visser, F., *Uisce Faoi Thalamh: An Investigation into the Online Mis- and Disinformation Ecosystem in Ireland*, Report 1 of 3 - Summary Report, Institute for Strategic Dialogue (ISD), https://www.isdglobal.org/wp-content/uploads/2023/11/Uisce-Faoi-Thalamh-Summary-Report.pdf [last access: December 2, 2024].

GEC Special Report: Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem, U.S. Department of State Global Engagement Center, January 2022, ttps://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf [last access: June 26, 2024].

Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG), https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Hasskriminalitaet/20220721_NetzDG.pdf?__blob=publicationFile&v=2 [last access: September 2, 2024].

Giandomenico, J., & Linderstål, H., *Disinformation Landscape in Sweden*, May 2023, https://www.disinfo.eu/wp-content/uploads/2023/05/Sweden_DisinfoFactsheet.pdf.

Giles, K., *Humour in Online Information Warfare: Case Study on Russia's War on Ukraine*, Hybrid CoE, November 2023.

Gniazdowski, M. & Wasiuta, M., *Russian Attacks in the Czech Republic: Domestic Context, Implications, Perspectives*, Center for Eastern Studies, April 20, 2021, https://www.osw.waw.pl/en/publikacje/analyses/2021-04-20/russian-attacks-czech-republic-domestic-context-implications [last access: June 19, 2024].

Gonzales M., "Spain's National Security Strategy to Include Risk of Disinformation Campaigns", El Pais, December 1, 2017, https://english.elpais.com/elpais/2017/12/01/inenglish/1512122156_659936.html [last access: November 1, 2024].

Government Report on Finnish Foreign and Security Policy/Ulko- ja turvallisuuspoliittinen selonteko, The Finnish Government/Valtioneuvosto, June 20, 2024, https://urn.fi/URN:ISBN:978-952-383-890-1 [last access: November 29, 2024].

Government's Defence Report/Valtioneuvoston puolustusselonteko, The Finnish Government/Valtioneuvosto, September 09, 2021, http://urn.fi/URN:ISBN:978-952-383-820-8 [last access: November 29, 2024].

Government-Wide Strategy for Effectively Tackling Disinformation, Ministry of the Interior and Kingdom Relations (of the Netherlands), December 23, 2022, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation [last access: November 23, 2024].

Greek Authorities' Investigation into Russian Remittances to Mount Athos, Orthodox Times, October 03, 2022, https://orthodoxtimes.com/greek-authorities-investigation-into-russian-remittances-to-mount-athos/ [last access: September 2, 2024].

Győri L., *Challenges of Strategic Communication in Hungary*, Political Capital, 2023, https://politicalcapital.hu/pc-admin/source/documents/IRI-PC_Study_Hungary_Challenges_StrategicCommunication_231219.pdf [last access: August 3, 2024].

Hajdu, D., Sawiris, M., & Klingová, K., *GLOBSEC Vulnerability Index: Romania*, GLOBSEC, https://www.globsec.org/sites/default/files/2021-11/Vulnerability-Index_Romania.pdf [last access: July 30, 2024].

Hansson, S., "COVID-19 Information Disorder: Six Types of Harmful Information During the Pandemic in Europe", *Journal of Risk Research*, 24, no. 3–4, April 3, 2021, https://doi.org/10.1080/13669877.2020.1871058.

Hénin, N., *Disinformation Landscape in France*, EU DisinfoLab, March 2023, https://www.disinfo.eu/publications/disinformation-landscape-in-france [last access: December 2, 2024].

Hénin, N., *FIMI: Towards a European Redefinition of Foreign Interference*, EU Disinfo Lab, April 2023, https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [last access: April 7, 2024].

Humprecht, E., Van Aelst, P., & Esser, F., "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research", *The International Journal of Press/Politics*, 2020, Vol. 25, No. 3, pp. 493-516, https://doi.org/10.1177/1940161219900126.

Hungary's National Security Strategy, 2021, https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html [last access: July 30, 2024].

In Finland, Trust in Media Scores Among the Highest, Reuters Institute, *Digital News Report 2024*, 2024, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf [last access: December 2, 2024].

Informacinę erdvę NATO viršūnių susitikimo metu stebėjo pirmą kartą Lietuvoje suburta tarpinstitucinė analitikų komanda, July 14, 2023.

Interview: How this Organisation is Fighting Against Disinformation, European Citizen Action Service, 2023, https://ecas.org/interview-how-this-organisation-is-fighting-against-disinformation/ [last access: December 2, 2024].

Is Romania Ready to Combat Disinformation and Communicate Effectively? Preparedness to Identify and Counter Information Manipulation and Malign Influence in the Context of the War in Ukraine, Global Focus, January 9, 2023, https://www.global-focus.eu/wp-content/uploads/2023/01/Is-Romania-ready-to-combat-disinformation-and-communicate-effectively-1.pdf [last access: November 16, 2024].

Kalenský, J., & Osadchuk, R., *How Ukraine Fights Russian Disinformation: Beehive vs Mammoth*, Hybrid CoE Research Report 11, 2024.

Kalenský, J., *The Structure and the Effect of the Disinformation Ecosystem*, Information Security Summit IS2, https://is2.cz/en/articles/speakers-2020/jakub-kalensky-en [last access: September 9, 2024].

Kharazian, Z., Starbird, K., & Hill, B.M., *Governance Capture in a Self-Governing Community: A Qualitative Comparison of the Serbo-Croatian Wikipedias*, 2023, https://arxiv.org/abs/2311.03616 [last access: December 2, 2024].

Kuczyńska-Zonik, A., Dyskurs narodowościowy na Litwie w kontekście współczesnych wyzwań, *Instytut Europy Środkowej* /Rocznik, 14 (5), 2016.

Kupiecki, R., Bryjka, F., Chłoń, T., *International Disinformation. A Handbook for Analysis and Response*, Brill, Leiden/Boston, 2025. DOI: 10.1163/9789004715769.

Kupiecki, R., & Legucka, A., (Eds.).*Disinformation and the Resilience of Democratic Societies*, PISM, Warsaw, 2023.

Latvia Country Report, in *Media Literacy Sector Mapping in Georgia, Latvia, Moldova and Ukraine*, Baltic Centre for Media Excellence, 2021, https://bcme.eu/en/our-work/research/report-media-literacy-sector-mapping-in-georgia-latvia-moldova-and-ukraine-2 [last access: December 2, 2024].

Les Lumières à l'ère numérique (2022), https://www.elysee.fr/admin/upload/default/0001/12/127ff0d2978ad3ebf10be0881ccf87573fc0ec11.pdf [last access: June 16, 2024].

Legucka, A., Kupiecki, R., (Eds.), *Disinformation, Narratives and Memory Politics in Russia and Belarus*, Routledge, London, 2022. DOI: 10.4324/9781003281597.

Letter to Parliament on Tackling State Threats and Presenting a Threat Assessment of State Actors Government of the Netherlands, 2022, https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/28/tk-aanpak-statelijke-dreigingen-en-aanbieding-dreigingsbeeld-statelijke-actoren-2 [last access: November 28, 2024].

Lietuvos Respublikos Visuomenės Informavimo Įstatymo Pakeitimo Įstatymas, July 11, 2006, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.280580 [last access: November 29, 2024].

Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018, Autorità per le Garanzie nelle Comunicazioni, January 31, 2018, https://www.agcom.it/node/11720 [last access: June 27, 2024].

Margova, R., & Dobreva, M., *Disinformation Landscape in Bulgaria*, EU DisinfoLab, 2023.

Matejova, M., Drmola, J., & Spáč, P., Measuring the Effectiveness of Counter Disinformation Strategies in the Czech Security Forces, *European Security*, 2024. DOI: 10.1080/09662839.2024.2362153.

Mazzucchi, N., *AI-Based Technologies in Hybrid Conflict: The Future of Influence Operations*, Hybrid CoE Paper 14, 2022, https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf [last access: July 9, 2024].

Media Literacy and Safe Use of New Media – Sweden, the European Commission, https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/sweden/68-media-literacy-and-safe-use-of-new-media [last access: November 28, 2024].
Media Services Act, https://www.riigiteataja.ee/en/eli/511012019003/consolide [last access: August 1, 2024].
Munkacsoport, J., *Hungarian government further weakens access to information*, K-Blog, January 23, 2024, https://k.blog.hu/2024/01/23/hungarian_government_further_weakens_access_to_information?utm_medium=doboz&utm_campaign=bloghu_cimlap&utm_source=nagyvilag [last access: September 22, 2024].
Notions of Disinformation and Related Concepts (ERGA Report), European Regulators Group for Audiovisual Media Services (ERGA), 2021, https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf [last access: July 14, 2024].
National Counter Disinformation Strategy Working Group, Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland), 2023, https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group/ [last access: September 30, 2024].
National Security Strategy, Government Offices of Sweden/Prime Minister's Office, July 2024, https://www.government.se/globalassets/government/national-security-strategy.pdf [last access: November 20, 2024].
National Strategic Review 2022, https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022 [last access: June 9, 2024].
National Strategy for Countering Hybrid Interference, Prague, 2021, https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/national-strategy---aj-final.pdf [last access: June 19, 2024].
Nationell digitaliseringsstrategi för skolväsende/National digitization strategy for schools, The Government Offices of Sweden, October 19, 2017, https://www.regeringen.se/contentassets/72ff9b9845854d6c8689017999228e53/nationell-digitaliseringsstrategi-for-skolvasendet.pdf [last access: November 28, 2024].
Návrh Koncepcie pre boj Slovenskej republiky proti hybridným hrozbám, Úrad vlády Slovenskej republiky, July 11, 2018, https://rokovania.gov.sk/RVL/Material/23100/1 [last access: November 29, 2024].
New Comprehensive Study Reveals Cyprus Media's Complex Coverage of the Russia-Ukraine War, Friedrich Naumann Foundation for Freedom, https://www.freiheit.org/greece-and-cyprus/new-comprehensive-study-reveals-cyprus-medias-complex-coverage-russia-ukraine-war [last access: December 2, 2024].
Newman, H., *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'*, Hybrid CoE Research Report 7, 2022.
Nimmo, B., *The Breakout Scale: Measuring the Impact of Influence Operations*, Brookings, 2020, https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations [last access: December 3, 2024].
Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 grudnia 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy, Kodeks karny (Dz. U. 2024 poz. 17).
OECD Information Integrity Hub, https://www.oecd.org/en/networks/oecd-information-integrity-hub.html [last access: October 24, 2024].
Operation and Responsibilities, The Security Committee of Finland/Turvallisuuskomitea, https://turvallisuuskomitea.fi/en/security-committee/operation/ [last access: August 2, 2024].
Our Mission, Psychological Defence Agency, March 15, 2024, https://mpf.se/psychological-defence-agency/about-us/our-mission [last access October 30, 2024].

Pamment J., *The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework Report*, Carnegie Endowment for International Peace, 2020, ttps://www.jstor.org/stable/resrep26180.6 [last access: June 6, 2025].

Par Latvijas Nacionālo attīstības plānu 2021.–2027. gadam (NAP2027), Latvijas Vēstnesis, 127, July 6, 2020, https://likumi.lv/ta/id/315879-par-latvijas-nacionalo-attistibas-planu-20212027-gadam-nap2027 [last access: October 19, 2024].

Par Valdības rīcības plānu Deklarācijas par Evikas Siliņas vadītā Ministru kabineta iecerēto darbību īstenošanai, Latvijas Vēstnesis, 16, January 23, 2024, https://likumi.lv/ta/id/349266-par-valdibas-ricibas-planu-deklaracijas-par-evikas-silinas-vadita-ministru-kabineta-iecereto-darbibu-istenosanai [last access: October 19, 2024].

Paxton, J., *Operationalizing Intelligence. Shaping the Information Environment and Galvanizing Western Action Against Russia*, The Three Swords, no. 38, 2022.

Policy Efforts to Protect Democracy Against Disinformation, House of Representatives of the Netherlands, 2019, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019D41916&did=2019D41916 [last access: October 18, 2024].

Polyák, G., *Freedom of Speech and the Regulation of Fake News in Hungary: A Legal Fight against State-Generated Disinformation?* in *Freedom of Speech and the Regulation of Fake News*, Intersentia, Cambridge, 2023.

Portal Kombat. A Structured and Coordinated Pro-Russian Propaganda Network: Technical Report, VIGINUM, February 2024, https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf [last access: September 23, 2024].

Premier powołał Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP, https://www.gov.pl/web/sluzby-specjalne/premier-powolal-pelnomocnika-rzadu-ds-bezpieczenstwa-przestrzeni-informacyjnej-rp [last access: September 9, 2022].

Presentation: *Media Literacy in Practice in Spain and Portugal*, Iberifier, November 16, 2022, Cidadania e desinformação [last access: August 1, 2024].

Prison for Fake News: A Proposal to Criminalize Fake News in Cyprus, July 12, 2024, https://verfassungsblog.de/prison-for-fake-news/ [last access: July 14, 2024].

Projekt Doktryny bezpieczeństwa informacyjnego RP, Biuro Bezpieczeństwa Narodowego, July 24, 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [last access: November 29, 2024].

Propaganda Diary 2022–2023: Voxcheck Presents the Database of Russian Propaganda in the European Mass Media, Vox Ukraine, 2023, https://voxukraine.org/en/propaganda-diary-2022-2023-voxcheck-presents-the-database-of-russian-propaganda-in-the-european-mass-media [last access: September 2, 2024].

Przeciwdziałanie Dezinformacji w Polsce Rekomendacje Systemowe, Forum Przeciwdziałania Dezinformacji, 2023, https://ffb.org.pl/wp-content/uploads/2023/02/Raport_Przeciwdzialanie_dezinformacji.pdf [last access: December 2, 2024].

Questions and Answers on the Digital Services Act, European Commission, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 [last access: February 23, 2024].

Radu, R., *Digital News Report 2024: Romania*, Reuters Institute for the Study of Journalism, 2024, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf [last access: July 30, 2024].

Rapport du Comité Éthique et Scientifique sur l'Activité du Service de Vigilance et de Protection Contre les Ingérences Numériques Étrangers (VIGINUM): Juillet 2021 – Décembre 2022,

Secrétariat général de la défense et de la sécurité nationale, https://www.sgdsn.gouv.fr/files/files/Viginum%20-%20rapport%20CES.pdf [last access: June 5, 2024].

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng [last access December 17, 2024].

Rekomendacje do Strategii Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, July 4, 2024, https://www.bbn.gov.pl/ftp/dokumenty/REKOMENDACJE_SBNRP_4_lipca_2024.pdf [last access: July 4, 2024].

Report of the Future of Media Commission, July 12, 2022, https://www.gov.ie/pdf/?file=https://assets.gov.ie/229731/2f2be30d-d987-40cd-9cfe-aaa885104bc1.pdf#page=null [last access: September 15, 2024].

RESIST 2 Counter Disinformation Toolkit, Government Communication Service, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/ [last access: June 24, 2024].

Ritter, S., *Die Verbreitung von Desinformation im Lichte des österreichischen Strafrechts*, Master Thesis, University of Vienna, 2024.

Romero Vicente, A., *Disinformation Landscape in Spain*, EU Disinfo Lab, March 2023, 20230224_SP_DisinfoFS.pdf [last access: December 4, 2024].

Sabev, M., Georgiev, G., & McLaren, R., *Safeguarding the Foundations: Strengthening Civil Security in Bulgaria, Montenegro, North Macedonia and Serbia*, Center for the Study of Democracy, 2024.

Sarkadi Nagy, M., *"International News Agency" informing Hungarians about a declining West from London has actually never left Budapest*, Atlatszo.hu, September 8, 2022, https://english.atlatszo.hu/2022/09/08/international-news-agency-informing-hungarians-about-a-declining-west-from-london-has-actually-never-left-budapest/ [last access: Auguat 1, 2024].

Sarkadi Nagy, M., London-based *V4 Agency is Orbán's propaganda machine disguised as global media product*, Atlatszo.hu, May 25, 2020, https://english.atlatszo.hu/2020/05/25/london-based-v4-agency-is-orbans-propaganda-machine-disguised-as-global-media-product/ [last access: August 1, 2024].

Security Strategy for Society/Yhteiskunnan turvallisuusstrategia - Valtioneuvoston periaatepäätös, The Finnish Security Committee/Turvallisuuskomitea, November 02, 2017, https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf [last access: November 29, 2024].

Security Strategy for the Kingdom of the Netherlands, Government of the Netherlands, 2023, https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands [last access: April 3, 2024].

Security Strategy of the Slovak Republik, 2021, https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf [last access: September 2, 2024].

Seimas pritarė naujam krizių valdymo ir civilinės saugos modeliui, December 8, 2022, https://lrv.lt/lt/naujienos/seimas-pritare-naujam-kriziu-valdymo-ir-civilines-saugos-modeliui/?fbclid=IwAR3Ks1Idn6VDLM5UYzviZ2TQiVLbs8DvKPNAALAn2IGmrDReyzngGRdygs [last access: September 19, 2024].

Simonsen, E., *Monitoring media pluralism in the digital era application of the media pluralism monitor in the European member states and candidate countries in 2023: Country Report: Denmark*, EUI Centre for Media Pluralism and Media Freedom/Robert Schuman Centre, June 2024.

Slovenia, Croatia, Greece – trust, social cohesion, https://europa.eu/eurobarometer/surveys/detail/2183 [last access: November 26, 2024].
State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity, Joint Cybersecurity Advisory, https://www.ic3.gov/CSA/2024/240709.pdf [last access: July 9, 2024].
Stollenwerk, E., Börzel, T.A., & Risse,T., *Theorizing resilience-building in the EU's neighbourhood: introduction to the special issue*, Democratization, 2021, Vol. 28, No. 7, pp. 1219–1238, https://doi.org/10.1080/13510347.2021.1957839.
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [last access: December 30, 2019].
Strategia națională în domeniul inteligenței artificiale 2024-2027, 2024, https://www.mcid.gov.ro/wp-content/uploads/2024/02/Strategie-Inteligenta-Artificiala-22012024_clean_final.pdf [last access: November 16, 2024].
Strengthened Code of Practice on Disinformation, European Commission, 2022, https://op.europa.eu/en/publication-detail/-/publication/c1c55f26-063e-11ed-acce-01aa75ed71a1/language-en [last access: December 17, 2024].
Svenskt psykförsvar i backspegeln, Försvarsmakten/The Swedish Armed Forces, February 26, 2020, https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/svenskt-psykforsvar-i-backspegeln/ [last access: December 4, 2024].
Szabolcs, P., *Putin's hackers gained full access to Hungary's foreign ministry networks, the Orbán government has been unable to stop them*, Direkt36, March 29, 2022, https://www.direkt36.hu/en/putyin-hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/ [last access: September 22, 2024].
Szakács, J., & Bognár, E., *Digital News Report 2024: Hungary*, Reuters Institute for the Study of Journalism, 2024.
Tackling Disinformation, Foreign Information Manipulation and Interference. Stratcom Activity Report, European External Action Service (EEAS), October 2021, https://www.eeas.europa.eu /eeas/2021- stratcom-activity-report-strategic-communication-task-forces-andinformation-analysis_en [last access: December 11, 2024].
Tackling online disinformation: A European Approach, European Commission COM(2018) 236 Final, 201, https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEXper cent3A52018DC0236 [last access: November 30, 2024].
Tavolo tecnico, which involves broadcasters, digital platforms, academics, etc., https://www.agcom.it/tavolo-tecnico-07-giugno-2024 [last access: June 27, 2024].
The Criminal Code of the Netherlands [translated], October 1, 2012, https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Netherlands-Criminal-Code.pdf [last access: November 12, 2024].
The Criminal Code of the Netherlands in Dutch, July 14, 2024, https://wetten.overheid.nl/BWBR0001854/2024-07-01 [last access: November 10, 2024].
The Digital Services Act Package, the European Commission, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [last access: February 16, 2024].
The Disinformation Landscape in Latvia, https://www.disinfo.eu/publications/disinformation-landscape-in-latvia/ [last access: December 4, 2024].
The Finnish Comprehensive Security Concept/Turvallinen Suomi - Tietoja Suomen kokonaisturvallisuudesta, Finland's Security Committee/Turvallisuuskomitea, October 4, 2018, https://turvallisuuskomitea.fi/turvallinen-suomi-2018-tietoa-suomen-kokonaisturvallisuudesta/ [last access: November 29, 2024].
The Framework to Counter Foreign State Information Manipulation, U.S. Department of State, January 18, 2024, https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/ [last access: October 31, 2024].

The Hungarian Government Further Weakens Freedom of Information and Transparency, DemNet, June 11, 2019, https://demnet.hu/en/blog-en/hungarian-government-further-weakens-transparency/ [last access: September 22, 2024].

The Kursk Problem, *Disinformation Review*, https://euvsdisinfo.eu/the-kursk-problem/, August 22, 2024 [last access: November 2, 2024].

The Monitoring Team Works within the Department of Economics and Statistics, https://web.archive.org/web/20200820140058/https://www.agcom.it/documents/10179/18199220/Documento+generico+01-04-2020/47636882-2d30-42dd-945dffc6597e685f?version=1.0 [last access: August 1, 2024].

The National Concept on Strategic Communication and Security of the Information Space 2023–2027, Cabinet of Ministers of the Republic of Latvia, 2023, https://www.mk.gov.lv/en/valsts-strategiskas-komunikacijas-un-informativas-telpas-drosibas-koncepcija?utm_source=https%3A%2F%2Fwww.google.com%2F [last access: March 20, 2024].

The National Security Strategy of the Republic of Poland, Biuro Bezpieczeństwa Narodowego, May 12, 2020, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf [last access: November 29, 2024].

The Netherlands Cybersecurity Strategy 2022-2028, Ministry of Justice and Security of the Netherlands/National Cyber Security Centre, 2022, https://english.ncsc.nl/publications/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028 [last access: January 31, 2023].

The Regulation of Fact-Checking and Disinformation in the Baltic States, EDMO, May 2024, BECID-D3.4._report.pdf [last access: December 11, 2024).

Thépaut, C., *Deputy Director of Monitoring and Strategy at the Ministry of Europe and Foreign Affairs*, Twitter, February 12, 2024, https://x.com/diplocharlie/status/1757158603897626942 [last access: June 05, 2024].

Todorov, S., *Espionage Allegations Rock Bulgaria's Top Security Agencies*, Balkan Insight, Sofia, February 5, 2024, https://balkaninsight.com/2024/02/05/espionage-allegations-rock-bulgarias-top-security-agencies/ [last access: December 4, 2024].

Tomasz Chłoń pełnomocnikiem Ministra spraw zagranicznych ds. przeciwdziałania dezinformacji międzynarodowej, https://www.gov.pl/web/dyplomacja/tomasz-chlon-pelnomocnikiem-ministra-spraw-zagranicznych-ds-przeciwdzialania-dezinformacji-miedzynarodowej [last access: May 14, 2024].

Tworzecki, H., *Poland: A Case of Top-Down Polarization*, The ANNALS of the American Academy of Political and Social Science, 681(1), 2019, https://doi.org/10.1177/0002716218809322.

Veress, C., *The Comparison Between the Hungarian and Romanian National Security Strategies*, European Scientific Journal, ESJ, 2022/39.

Vicente, A.R., *Disinformation Landscape in Spain*, EU DisinfoLab, March 2023, https://www.disinfo.eu/wp-content/uploads/2023/03/20230224_SP_DisinfoFS.pdf [last access: October 29, 2024].

Voltri, J., *Countering Russian Information Influence in the Baltic States: A Comparison of Approaches Adopted in Estonia, Latvia, And Lithuania*, 2022, https://www.kvak.ee/files/2023/01/Sojateadlane-19-2022-Johannes-Voltri-COUNTERING-RUSSIAN-INFORMATION-INFLUENCE-IN-THE-BALTIC-STATES-A-COMPARISON-OF-APPROACHES-ADOPTED-IN-ESTONIA-LATVIA-AND-LITHUANIA.pdf [last access: October 19, 2024].

Wahl, T., *Rule of Law Developments in Poland: May-October 2023*, Eucrim, https://eucrim.eu/news/rule-of-law-developments-in-poland-may-october-2023/ [last access: November 10, 2024].

Walker, S., *London Media Agency Carries Viktor Orbán's Nativist Message*, The Guardian, May 5, 2019, https://www.theguardian.com/world/2019/may/05/london-based-media-agency-channels-victor-orban-nativist-message-hungary [last access: August 1, 2024].

Wiseman, J., & Panyi, S., *MFRR Podcast: Navigating Hungary's New Sovereignty Protection Act*, October 31, 2023, International Press Institute, https://ipi.media/ipimedia/mfrr-podcast-navigating-hungarys-new-sovereignty-protection-act/ [last access: August 2, 2024].

Zahorjan, D., Haburaj. P., & Milo, D., *Recommendations to Future Parliamentarians on Responses to FIMI: A Selection of Case Studies – Slovakia*, New Security Threats Institute, September 2024.

Zarządzenie nr 30 Ministra Spraw Zagranicznych w sprawie Rady Konsultacyjnej do spraw Odporności na Dezinformację Międzynarodową przy Ministrze Spraw Zagranicznych, September 11, 2024, https://www.gov.pl/web/dyplomacja/zarzadzenie-nr-30-ministra-spraw-zagranicznych-z-dnia-11-wrzesnia-2024-r-w-sprawie-rady-konsultacyjnej-do-spraw-odpornosci-na-dezinformacje-miedzynarodowa-przy-ministrze-spraw-zagranicznych [last access: October 29, 2024].

Нестеренко А., Головенко Р., Романюк О., «Ядерний Удар По Вінниці Та Гулаг Для Запорізьких Учителів. Геноцидна Риторика Російської Пропаганди [A Nuclear Attack on Vinnytsia and the Gulag for Zaporizhzhia Teachers. The Genocidal Rhetoric of Russian Propaganda]." Інститут масової інформації, 2022, https://imi.org.ua/monitorings/yadernyj-udar-po-vinnytsi-ta-gulag-dlya-zaporizkyh-vchyteliv-genotsydna-rytoryka-rosijskoyi-i48786 [last access: November 7, 2024].

Спікери, Які Просувають Співзвучні Російській Пропаганді Наративи [Speakers who promote narratives consistent with Russian propaganda], Center for Countering Disinformation, 2022, https://web.archive.org/web/20220801015336/https://cpd.gov.ua/reports/ [last access: November 7, 2024].