INSTITUTIONAL RESPONSE TO FOREIGN INFORMATION MANIPULATION AND INTERFERENCE IN NORTH MACEDONIA: MODELS AND POLICY OPTIONS

POLICY PAPER

Publisher:
Institute of Communication Studies
Jurij Gagarin 17-1-1, Skopje
www.iks.edu.mk

For the publisher:
Prof. Dr. Zhaneta Trajkoska

Edition:
ResPublica

Authors:
Aleksandar Grizhev, PhD, Assoc. Prof.
Vesna Poposka, PhD, Assoc. Prof.

Editor:
Dejan Andonov, MSc

Original title:
„Институционален одговор на странско мешање и манипулирање со информации во Северна Македонија: модели и опции за политика" - документ за јавна политика

Translation from Macedonian to English:
Olivera Celeska

Graphic design:
Ivana Temelkoska

Place and year:
Skopje, 2025

Contents

EXECUTIVE SUMMARY

Awareness of the risks posed by Foreign Information Manipulation and Interference (FIMI) exists in North Macedonia, but the national system for coordinated response remains fragmented, without functional inter-institutional coordination and clearly defined responsibilities. There is a lack of a centralized mechanism for information exchange, timely analysis and joint response. Most activities are carried out reactively, depending on the initiative of individual institutions or sectors, which can lead to overlapping authorities, wasted resources and inconsistent communication with the public.

The fight against FIMI is impeded by the limited capacities and resources, such as staff, tools and budget for monitoring, analysis and strategic communication, as well as the lack of systematic education in the public sector in the domain of digital and media literacy. This is compounded by the low level of public trust (IRI, 2024) and social resilience, fuelled by polarization and insufficient transparency of institutional communication.

Foreign Information Manipulation and Interference is not clearly defined in the regulatory framework, and existing strategies are not sufficiently operationalized through clear roles, protocols, and indicators for monitoring and measuring their performance. The Security Intelligence Community Coordination Council is not performing its intended functions, and in practice there is no established structure for rapid analysis and joint response to cases of disinformation or foreign influence.

Hence, the key recommendation of this policy paper is for North Macedonia to establish a national FIMI coordination and resilience mechanism, which will ensure institutional connectivity, regulated information exchange, and systematic threat monitoring with clear roles, protocols, and performance indicators.

The paper lays out the following options for an institutional solution:

- Creation of a stand-alone centre for digital or national resilience - implies the establishment of an independent public institution with a clear mandate, responsibilities and budget, which would integrate the functions of analysis, coordination and education. The advantage is in the centralized and visible structure, but the model requires new resources and administrative setup.

- Formation of a national coordination mechanism under the Government – it envisages integrating the mechanism through a "core + network" coordination office. This will ensure political gravitas, interoperability and rapid response in crisis situations, but there is a potential risk of overload with other issues, dependence on political continuity and the possible lack of deep analytics if the core is small.

- Integration into the Security and Intelligence Community Coordination Council - enables the strengthening and operationalization of an existing structure by expanding its mandate to cover the area of FIMI. The advantage is in the rationalization of an already

established structure, but the risk is in the reduced public visibility and the coordination remaining "on paper", which requires discipline and clear standard operating procedures.

Regardless of the selected option, this paper provides the following **recommendations for establishing a reliable and functional system for addressing FIMI:**

- Define an institutional model and a lead entity and appoint focal points in all relevant institutions;
- Establish a regular calendar of activities, develop a standard "report - assess - respond" procedure for incident management and develop universal scenarios and checklists;
- Strengthen human capacities;
- Ensure preventive communication about expected manipulative narratives;
- Exchange information through a common base; and
- Establish indicators for monitoring efficiency.

It is also necessary for institutions to take additional measures and policies that will strengthen the system and its resilience, such as:

- Revise and upgrade the existing Hybrid Threats Resilience Strategy (2021–2025);
- Strengthen institutional capacities for monitoring and analysis;
- Introduce media and digital literacy programmes in the public sector;
- Involve academia and civil society through formalized partnerships; and
- Increase integration with NATO and EU mechanisms to combat FIMI.

Establishing a national model for countering FIMI will enable North Macedonia to move towards an integrated, functional and sustainable institutional response system.

INTRODUCTION

In the contemporary security and information context, Foreign Information Manipulation and Interference (FIM) poses a serious and growing threat to democratic systems, public trust and the stability of institutions. The rapid development of digital technologies, greater connectivity and the transnational nature of information flows allow such operations to be carried out more efficiently, making them more difficult to detect. Through the use of coordinated networks, covert identities and generative artificial intelligence, state and non-state actors can sway public opinion, electoral processes and foreign policies of other states. In the European context, FIM is recognized as a security and foreign policy threat that requires a coordinated, cross-sectoral response, with an emphasis not only on the content, but also on the tactics, techniques and procedures of influence and interference. European institutions have already activated coordinated mechanisms for increased preparedness during election periods, which emphasizes the importance of proactive, not just reactive measures.

In North Macedonia, FIMI is becoming increasingly important in the context of Euro-Atlantic integration and the need to strengthen national resilience to hybrid threats. There is a nation-wide consensus on the significance of the phenomenon in the framework of national policies on hybrid threats and electoral integrity, reinforced by the adoption of the National Strategy for Building Resilience and Countering Hybrid Threats (2021–2025) and the accompanying Action Plan. As the strategy says, resilience is based on strategic orientation towards an integrated, better coordinated approach and capacity building at the national level, aligned with NATO commitments for civil preparedness and the needs for national resilience. However, the institutions are still faced with the challenge of putting the strategy and action plan into practice, these phenomena are not criminalized, the institutional response in insufficiently coordinated and has limited human and technical resources, there is an unclear distribution of responsibilities, and a lack of systematic monitoring, analysis and response to risks.

There is no explicitly adopted definition of FIMI in the Macedonian legal system, which contributes to the problem remaining partly misunderstood and inadequately treated in public policies. From the perspective of EU policies and regulations, the term encompasses both content and behaviour - in many cases, FIMI is a form of disinformation of foreign origin, but also includes operational tactics and procedures, such as coordinated inauthentic behaviour, technical breaches, leaks of materials and hybrid operations, aimed at the free formation and expression of political will (Bleyer-Simon, 2025).

This paper is guided by this double anchor - the national framework for hybrid threats and the European framework for the integrity of the information environment, i.e. the definition used is more operational (based on behaviours and processes) and is aimed at prevention, detection and coordinated response.

This policy paper aims to identify and analyse the problem of inter-institutional coordination in dealing with FIMI, as well as to propose concrete and feasible solutions for establishing a national response system, as part of broader efforts to build institutional and societal resilience to hybrid threats. The focus is on organizational models, coordination mechanisms, and monitoring and response instruments. This combined approach allows for linking the narratives and the processes, i.e. the manner in which the impact unfolds, to the institutional capacities, i.e. how to manage the risk with applicable recommendations.

The paper builds on the existing European and national framework, including the obligations arising from NATO membership and the process of EU approximation. NATO is strengthening the role of strategic communication through the StratCom - NATO Strategic Communications Center of Excellence in Riga, to support allied and partner countries in building capacities for analysis, communication and deterrence, while the EU Rapid Alert System (RAS) serves for coordination and exchange of information between Member States in the event of information incidents. In parallel, the EU establishes obligations for the management of systemic risks, including disinformation, for large online platforms through the Digital Services Act (DSA) and sets standards for media independence and pluralism through the European Media Freedom Act (EMFA). Finally, the document builds on the previous two studies of the Institute of Communication Studies: Foreign Information Manipulation and Interference in the Republic of North Macedonia: Baseline Analysis (Hadzi-Janev, Stoilkovski, 2025) and Addressing Foreign Information Manipulation in the context of European Regulations (Bleyer-Simon, 2025).

The paper describes the current state ("where we are") in the institutional set-up, capacities and regulatory framework, identifies the essential gaps between strategic intentions and actual practice, offers policy options (alternative institutional models) based on comparative experiences and proposes a roadmap for implementation. Hence, it is structured in the following sections:

Chapter 1: Towards an integrated response to information threats;

Chapter 2: Status and challenges of the institutional response to FIMI in North Macedonia;

Chapter 3: Comparative experiences and FIMI response models;

Chapter 4: Policy options for FIMI response in North Macedonia; and

Chapter 5: Concluding observations and recommendations for implementation.

With this structure, the document allows decision-makers, experts, and the general public to see the current institutional constraints and recognize specific directions for developing an integrated, proactive, and coordinated system of resilience to FIMI.

Methodology

1. Methodological framework and approach

The analysis is based on a combined methodological approach that links (1) desk analysis of relevant national, EU and NATO policies and documents (2) qualitative findings from focus groups and interviews with representatives of key institutions; (3) GAP analysis of the institutional system; and (4) comparative analysis of good practices from EU and NATO member states (Estonia, Finland, France, Poland and Sweden). The aim is to get an integrated picture of: (a) how FIMI manifests and is perceived in practice; (b) to what extent the institutional framework and capacities enable an efficient response; and (c) which models are applicable in North Macedonia. The results of the analysis serve as a basis for developing policy recommendations, which will enable the building of a more comprehensive and integrated system for preventing and managing FIMI risks.

2. Data sources

(a) Desk analysis. Relevant EU and NATO regulations and policies were reviewed (Digital Services Act - DSA; European Media Freedom Act - EMFA; NATO Strategic Concept (2022); FIMI Toolbox, Rapid Alert System - RAS etc.), the National Strategy for Building Resilience and Dealing with Hybrid Threats (2021–2025) with the Action Plan, as well as previous ICS publications to provide the normative-political context. The results of the desk analysis are triangulated with the findings from the focus groups to build a coherent interpretation of the systemic gaps, and to increase the validity of the findings by combining the sources and techniques (Bryman, 2016). In the design of monitoring and evaluation we were guided by the guidelines of the Organization for Economic Cooperation and Development for monitoring and evaluation of public policies (OECD, 2017).

(b) Focus groups. Two focus groups were conducted with representatives from key institutions and regulators in September 2025. The discussions were semi-structured, following a guide with five thematic areas: understanding FIMI, institutional coordination, legal or strategic framework, capacities and resources, and international cooperation. The sessions were held in a controlled environment (90-120 minutes), moderated by a research team, and recorded as notes and transcripts. Respondents who were unable to participate in the focus groups responded to an interview questionnaire. Statements in the document are paraphrased to illustrate recurring trends, and the findings are presented as an overview of common perceptions and systemic challenges, in order to draw analytical points about the current level of institutional maturity and resilience.

(c) GAP analysis. A comparison is made between strategic intentions and commitments and actual institutional practice in terms of roles and responsibilities, coordination and information exchange processes, human and technical resources, and monitoring and evaluation mechanisms. The gaps are summarized by domain and used as a bridge to policy options and a roadmap for implementation.

(d) Comparative analysis. Five reference models from EU and NATO member states (Estonia, Finland, France, Poland and Sweden) were selected according to the following applicability criteria: clearly defined mandate and processes, intersectoral coordination, tools and staff, transparent strategic communication and measurable results.

3. Sample and participants

The qualitative research used purposive sampling, where the relevance of the participant to the research purpose takes precedence over statistical representativeness (Bryman, 2016). The sample covered the different levels of public administration (strategic, operational and analytical), in order to provide a multi-layered insight into the processes of planning, implementation and evaluation. The representation of representatives from government coordination structures, security-intelligence sectors, the diplomatic-consular sector and the sectors for digital transformation, public administration, ICT security and media regulation allowed to compare institutional perspectives (normative and organizational) with operational experiences (real procedures, bottlenecks, constraints). The following institutions were included in the research: the Ministries of Foreign Affairs, Interior, Digital Transformation and Public Administration, the National Committee for Preventing Violent Extremism and Combating Terrorism, the Intelligence Agency (IA), the Agency for Audio and Audiovisual Media Services (AAVMS), the National Center for Computer Incident Response (MKD-CIRT), the Crisis Management Center and the Directorate for Special Purpose Production at the Ministry of Economy.

4. Ethics

Given the sensitivity of the topic, especially for institutions with security authorities, the research was conducted according to clear ethical protocols. All participants were informed about the purpose, the manner of data use and the identity protection measures. The report does not mention names, positions or specific institutions in order to preserve confidentiality and avoid implicit attribution of views to a specific institution. Segments that could point to specific operational practices are aggregated at the thematic level, and conclusions are formulated as a synthesis of recurring trends, rather than as individual statements. This reduces the risks of misinterpretation and preserves confidentiality without compromising analytical value.

5. Limitations

Typically for qualitative studies, focus groups do not claim representativeness, but provide an in-depth understanding of processes and perceptions. The use of paraphrased quotes reduces the possibility of literal quoting, but at the same time allows the essence of the argument to be retained. The potential bias of socially desirable behaviour is mitigated through moderation techniques (fragmenting questions, seeking specific examples, focusing on processes rather than personal attitudes) and through triangulation with documents and comparative experiences. The final claims in the paper are based on convergence between multiple sources, rather than on single statements (Bryman, 2016).

CHAPTER 1:

TOWARDS AN INTEGRATED RESPONSE TO INFORMATION THREATS

1.1. Information threats and the need for a coordinated institutional response

Foreign Information Manipulation and Interference (FIMI) encompasses the spectrum of substantive and, more importantly, behavioural practices by which foreign actors attempt to distort or direct public discourse, influence democratic processes, and erode trust in institutions. In the European approach, FIMI is not only treated as "harmful content", but also as tactics, techniques, and procedures (TTPs), such as hack-and-leak, computerized disinformation, coordinated inauthentic activities, etc. (Bleyer-Simon, 2025). The literature further describes this as cognitive operations and algorithmic influence on the public sphere (Pamment, 2020). Modern active measures operate as long-term campaigns with recognizable behavioural patterns (Rid, 2020). This notion is framed within the broader framework of hybrid threats (Hoffman, 2007), for which a national strategy requires a more integrated and better coordinated response at the national level, with clear roles and resilience mechanisms.

The definition of FIMI according to the European External Action Service - EEAS is: "FIMI is 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. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory" (EEAS, 2025).

- *"Mostly non-illegal"* - this makes it difficult to deal with the phenomenon through the existing legal framework and creates pressure on legislators to establish new sets of rules.

- *"Pattern of behaviour"* – While the efforts for countering disinformation often focus on content and narratives, this definition shifts the focus from content to behaviour, as FIMI represents the intentional manipulation of information. The pattern of tactics, techniques, and procedures (TTPs) also leads to the identification of threat actors.

- "*Threatens or has the potential to negatively impact values, procedures and political processes"* - FIMI is strategic in nature and encompasses any information manipulation that could cause public harm, prioritizing four main domains:

  - Political disinformation, which tends to favour one side of the political competition or undermine trust in institutions and the democratic process;
  - Health disinformation, which endangers communities;
  - Environmental disinformation, especially related to climate change;
  - Disinformation that may pose a security threat or disrupt public order.

- *"Manipulative, intentional, and coordinated"* - FIMI operations use manipulation tactics to deceive, mislead, and destabilize their target. The targets are most often democratic societies, but foreign interference and influence are present globally, including in developing countries.

FIMI actors aim to polarize society by promoting extreme views to deepen conflicts, which in turn hinders democratic dialogue. They manipulate content by altering authentic information or media, such as editing images or videos to change their meaning, and create fabricated content, such as fake websites that mimic legitimate sources, deepfake videos and audios and visual materials generated with artificial intelligence. Furthermore, they create false narratives, impersonating people and abusing diplomatic or institutional profiles on social media, while discrediting reliable sources and reformulating the context to confuse audiences, and amplification is carried out through the use of bots, trolls or coordinated networks to artificially increase the visibility and credibility of disinformation. At the same time, cyber tools are used, including hacking and other activities to steal, modify or fabricate information (Popovska, 2024).

FIMI emerges through a combination of narratives (how the topic is framed and what emotions are triggered), channels (traditional media, online platforms, messaging apps), and techniques (planned tactics and actions). Here are some typical examples:

- Coordinated inauthentic behaviour on social media (coordinated posts, fake profiles/"bots", artificially starting trends);
- "Hacking and posting" materials shortly before sensitive events (elections, crises), to direct attention and undermine trust;
- Intermediary organizations and media with non-transparent financing, including practices of media capture (control over editorial policies and ownership);
- Manipulation of content visibility on platforms (rigged rankings, "staged" citizen support, engineered reach-boosting);
- Combining with other hybrid instruments (cyber-attacks, economic pressure, diplomatic framing) for greater effect.

These practices are difficult to address with measures targeting individual content alone. Therefore, **the emphasis is placed on risk assessment and clear response procedures for state authorities and platforms, under a broader policy on hybrid threats and institutional resilience** (Bleyer-Simon, 2025).

Hence, generally speaking, **states should independently, in accordance with risk assessments, national security strategies and defence doctrines, define, detect and counter this type of threat.**

Within NATO, the approach focuses on "information threats" – deliberate, harmful, manipulative and coordinated activities carried out by state and non-state actors, including hostile information operations, information manipulation, interference by foreign actors and disinformation disseminated through traditional and social media (NATO, 2020). The Alliance works closely with Allies and partners to understand, prevent and build resilience to these information threats. NATO's responses encompass proactive short-term, mid-term and long-term measures, based on four key functions: (1) understanding the information environment *(Understand*), (2) preventing the effectiveness of information threats (*Prevent*),

(3) containing and mitigating specific information incidents (*Contain and Mitigate*) and (4) recovery and learning (*Recover*). **Proactive communication is one of the key tools for countering information threats.** The NATO Alliance communicates with target audiences through various channels (official website, editorial and press releases, *NATO Review*, podcasts, official profiles on X, Facebook, Instagram, YouTube and LinkedIn), providing accurate information that helps people recognize and counter information threats. This proactive approach to explaining and prebunking narratives is aligned with the information ecology framework and the classification of types of disinformation (Wardle & Derakhshan, 2017). Research shows that brief forewarnings before exposure increase resistance to manipulative narratives (Banas & Miller, 2013).

European regulations, such as the Digital Services Act (DSA) and the European Media Freedom Act (EMFA), add a systemic perspective (European Commission, 2020): instead of one-off responses to individual content, the focus is on managing systemic risks, protecting media pluralism and interoperable reporting and coordination mechanisms (Bleyer-Simon, 2025). This implies that **an effective response to FIMI must combine institutional coordination, operational protocols and communication resilience, and not just legal prohibitions or technical measures.**

1.2. Interference in elections is among the most complex operations of FIMI

A Eurobarometer survey on citizenship and democracy from December 2023 showed that 81 percent of EU citizens believe that foreign interference in democratic systems is a serious problem that needs to be addressed, and 78 percent are concerned that disinformation can influence people's voting decisions (European Commission, 2023). Previously limited to intimidation, electoral fraud, or hacking, today interference encompasses much more innocent, yet ubiquitous and everyday interactions. A seemingly harmless and casual conversation can now be considered part of a hostile influence campaign.

On December 30, 2024, the German government accused Elon Musk of trying to influence the election through open support for the political party "Alternative for Germany" (AfD), after which the Bundestag administration launched an investigation in January and February 2025 into whether such support could be considered an illegal party donation. Musk previously published a column in the German newspaper *Welt am Sonntag* with praise for the AfD and on January 9, 2025 participated in a live chat on X with the party's co-leader Alice Weidel (with over 200 million followers on the platform). In parallel, the European Commission, as part of the existing procedure for infringement of the European Digital Services Act (DSA) against X (on January 9 and 17, 2025), conducted additional checks and requested documentation on the algorithms and the live chat held (Reuters, 2025).

Following the start of the war in Ukraine in 2022, Russia launched a large-scale disinformation campaign aimed at destabilizing the EU and its Member States. In response, the EU imposed sanctions on Russian assets and actors involved in the FIMI. On 8 October 2024, additional restrictive measures were adopted against Russia's destabilizing activities, including undermining electoral processes, disrupting the functioning of democratic institutions, and coordinated disinformation attacks and foreign interference.

During the 2022 Brazilian elections, disinformation spread through WhatsApp and Telegram significantly influenced voter attitudes. The Electoral Supervisory Court (TSE) frequently requested the removal of content, and a fact-checking chatbot was activated. Research has shown that these platforms enabled the massive spread of false information, especially about electronic voting machines, leading to distrust in the electoral process and increased tensions (Mozilla Foundation, 2024).

Examples of interference in elections and other key state processes are also observed in the region.

In the Romanian presidential election, held on 24 November 2024, ultranationalist pro-Russian candidate Calin Georgescu took the lead in the first round with 22.94 percent of the votes cast. This result contradicted pre-election polls, which had predicted his support to be between 5 and 10 percent. Georgescu, a vocal critic of NATO and the EU, beat incumbent Prime Minister Marcel Ciolacu, who secured only 19.5 percent of the votes cast, marking the first time in post-communist Romania that the Social Democratic Party (PSD) failed to reach the second round. Georgescu's campaign was marked by a suspicious uptick in social media activity, particularly on TikTok and Telegram, fuelled by paid influencers and a coordinated network of social media accounts. Romanian intelligence services have found that actors linked to Russia played a key role in amplifying pro-Russian and anti-Western narratives. TikTok removed millions of fake accounts promoting Georgescu's messages, even though the campaign had already caused significant damage. Intelligence assessments confirmed that many of these accounts were linked to entities linked to Russia, proving Moscow's direct involvement in manipulating public opinion. On December 6, 2024, Romania's Constitutional Court took the unprecedented step of annulling the election results due to widespread irregularities and credible suspicions of foreign interference (House of Commons Library, 2024).

During a press conference in March 2025, Kosovo Prime Minister Albin Kurti said that Serbian President Aleksandar Vučić interfered in the parliamentary elections in Kosovo through the Serbian government, intelligence services and organized crime groups. Kurti also mentioned that Milan Radojićić, former deputy leader of the Srpska Lista party, played a significant role in the interference. Radojičić claimed responsibility for organizing the attack in the village of Banjska in the Serb-majority municipality of Zvechan in northern Kosovo, on September 24, 2023. Kosovo has requested his extradition from Serbia. In a response on Facebook, Srpska Lista rejected the accusations made by Kurti and Rashich, calling them "brutal lies". "Srpska Lista is proud that it has received the greatest support from the Serbian people and that, despite all the pressure, blackmail and threats, it has

managed to persevere, thanks to the unity of our people, proving once again that there will be no giving up", the party said. The European Union Election Observation Mission stated on 11 February 2025, during the presentation of preliminary findings on the elections held, that Serbia interfered in the elections by exerting pressure on Serbian voters in Kosovo (EU EOM, 2025).

The 2021 local elections in Nikshich were a turning point for Montenegro, particularly due to the strong involvement of neighbouring Serbia in the election campaign. The presence of affiliated individuals or members of Serbia's ruling party, the Serbian Progressive Party (SNS), raised concerns. Some were detained and others were banned from entering the country on suspicion of bringing in money to buy votes. After the elections, the City of Belgrade, as promised in the campaign, donated 2 million euros to the municipality of Nikshich, further fuelling suspicions of electoral integrity violations and foreign influence (CDT, 2024).

Montenegro faced political turmoil just before and after joining NATO, which were the result of various seemingly social issues, the most pronounced of which were those related to religious issues. The demoralization phase included a huge presence of false information, hate speech, disinformation and calls for defence against an imaginary enemy. In the disinformation campaign, one web portal played a leading role, creating a serious quantum of disinformation. Although the web portal was not registered in the media register, it presented itself as a news media outlet. In doing so, it created a lot of content aimed at provoking an emotional reaction from the audience, using the misuse of historical contexts and linking the President of Montenegro to the fascist regimes of World War II. The pro-Kremlin media outlet Sputnik acted similarly. Cases of disinformation by these two portals were documented by the Digital Forensic Center in Podgorica (IREX, 2023).

From this perspective, interference is not so much about how people vote, but about shaping the motivations, intentions, and contexts in which voters think about politics. And it is precisely these processes - debates, persuasions, and chaotic arguments - that are an essential part of democracy.

1.3. EU's responsive and analytical approach to FIMI

The European Union has a well-developed and comprehensive infrastructure that enables the operationalization of activities aimed at building resilience to foreign malicious influence. This infrastructure is based on several strategic documents, regulations and mechanisms. Through these instruments, the EU not only defines standards for identifying and countering FIMI and hybrid threats, but also establishes specific operational mechanisms for coordination between institutions, risk monitoring and engagement of the private sector and civil society. Moreover, through the European External Action Service

(EEAS) and specialized teams such as the EU Hybrid Fusion Cell and StratCom Task Forces, timely collection, analysis and dissemination of information on potential impacts are enabled, in order to support Member States and partners in developing their own resilience capacities. Interoperability in international networks enhances resilience in an interdependent environment (Keohane & Nye, 1998).

Among the mechanisms available to the Council of the EU, the following stand out:

- FIMI Toolbox, EEAS;
- Hybrid Rapid Response Teams - HRRTs;
- EU Cyber Diplomacy Toolbox;
- European Cooperation Network on Elections - ECNE;
- Strengthened Code of Practice on Disinformation, 2022;
- Rapid Alert System - RAS;
- European Digital Media Observatory - EDMO.

In addition, the EU has adopted several **acts and directives** aimed at increasing the accountability of online platforms, strengthening cybersecurity, the resilience of digital infrastructure and regulating the use of new technologies in communication. These legislations include:

- Digital Services Act - Regulation (EU) 2022/2065;
- Artificial Intelligence Act - Regulation (EU) 2024/1689;
- Directive on the Resilience of Critical Entities (EU) 2022/2557;
- Network and Information Security Directive NIS2 – (EU) 2022/2555;
- Regulation on the transparency and targeting of political advertising (EU) 2024/900;
- European Media Freedom Act – Regulation (EU) 2024/1083.

These measures are outlined in the Council of Europe conclusions of May 2024 on protecting electoral processes from foreign interference and in the Presidency conclusions of May 2025 on strengthening democratic resilience.

The EU has developed two key mechanisms for dealing with foreign information influence: FIMI Toolbox and the Rapid Alert System - RAS, which can be taken over and implemented with adaptation to national needs and context (EU StratCom Task Force, 2022).

FIMI Response Toolkit created by the European External Action Service is a conceptual and operational framework mechanism, more preventive than reactive, and is based on four pillars:

1. Situational awareness - through monitoring, analysis and information gathering techniques from public or other open sources (*OSINT*), narratives, sources and methods of manipulation are identified;

2. Resilience - capacity is being built among citizens, media and institutions to recognize and reject disinformation;
3. Regulation - policies and legal mechanisms for sanctioning and prevention are developed;
4. External action - diplomatic responses, partner support and global coordination.

The Rapid Alert System (RAS) is a digital platform that functions as an information alarm - when a disinformation campaign is detected, the system enables a rapid exchange of information between Member States, institutions and partners. The mechanism includes a network of national contact points that are connected in real time and allows the integration of data from media, fact- checkers, academic sources and technological platforms. Coordinated responses can take the form of public communications, diplomatic responses or technical interventions.

The EEAS has also established an advanced **analytical framework for FIMI threats,** which can serve as a model for how the process of monitoring, analysis and information exchange between institutions should be structured (EEAS, 2023; EEAS, 2024). The analytical framework represents an integrated system that brings together methodological (ABCDE), process (analytical cycle), technical (DISARM) and structural (STIX) elements:

- ABCDE. The ABCDE framework model represents a basic approach for differentiating FIMI incidents according to five dimensions: Actor, Behaviour, Content, Degree, and Effect. Its application in a national context would enable the creation of standards for analysing FIMI incidents, recognizing recurring patterns, and developing countermeasures.

Table 1: ABCDE Framework for FIMI Analysis

Element	Question	Purpose
Actor	What types of actors are involved?	To determine whether the incident involves a foreign state or non-state actor.
Behaviour	What activities have been observed?	To identify evidence of coordination, intent, and techniques used.
Content	What type of content is being created and distributed?	To establish whether the information is deceptive, manipulative, or partially accurate.
Degree	What is the distribution of the content?	To analyse target audiences and distribution volume.
Effect	What is the impact and who does it affect?	To assess the real damage and the seriousness of the case.

- Analytical cycle. The EEAS builds on this framework by establishing an analytical cycle, which enables a strategic and self-sustaining process of monitoring, analysis and upgrading of institutional knowledge. The phases of the analytical cycle include:

1. Strategic Monitoring - maps the ecosystem of known resources used by threat actors, tracks amplification patterns and new distribution channels;
2. Prioritisation and Triage - the highest priority incidents are selected, especially those that have direct political or security significance;
3. Incident Analysis and Evidence Collection - an analysis of the connection of channels and content is made, and the evidence is archived in accordance with the General Data Protection Regulation - GDPR and the Berkeley Protocol on Digital Open-Source Investigations;
4. Knowledge Pooling and Sharing - results are shared with relevant institutions and partners for rapid response and building collective awareness;
5. Situational Awareness - a database is updated, new actors and techniques are added, and long-term trends are extracted through comparative analysis.

- DISARM. To operationalise element "B" of the ABCDE framework, i.e. the behaviour of actors behind FIMI, the EEAS uses the DISARM framework. It is a common, open and adaptable system for categorising the techniques, tactics and procedures (TTPs) used by threat actors, enabling the identification of their recurring techniques and tactics and the early detection and disruption of their operations. The DISARM framework divides the phases of a FIMI incident into:

1. Planning - defining the goal and expected impact;
2. Preparation - creating infrastructure and selecting channels;
3. Execution - carrying out the operation through coordinated activities;
4. Assessing - measuring the effect and adjusting the strategy.

- STIX™. Finally, to ensure that the threat information is shared, the EEAS encodes FIMI incidents in the STIX™ (Structured Threat Information Expression) format. The application of this format enables interoperability among institutions and the integration of partial information into a bigger analytical picture. In this way, each identified narrative or technique contributes to the creation of situational awareness and early warning. This format, originally developed for cybersecurity, allows the representation of all relevant objects and connections in a single incident in FIMI.

Table 2: STIX™ Format (Structured Threat Information Expression)

STIX facility	Description
Incident	*Contains basic information about the incident (name, description, start date, purpose, etc.)*
Observable	*URL or file that was observed within the incident.*
Channels extension	*Any online or offline communication channel (website, social media profile or page, TV station, etc.) that publishes the monitored elements.*
Identity	*Individuals, organizations, or locations, including countries. Typically includes the targets of incidents.*
Threat Actor	*Contains information about threat actors.*
Event (extension)	*A description of a real-life event, such as an election, show, anniversary, etc., to provide a context in which incidents may occur.*
Vulnerability	*A description of the vulnerability that was exploited to enable the incident to occur.*
Language (extension)	*The language(s) used in the incident.*
Attack Pattern	*Description of the manipulative techniques (TTPs) used to carry out the attack.*
Course of Action	*Description of countermeasures against the incident.*
Narrative (extension)	*Description of the narratives used in incidents. Narratives can be nested and presented as meta- and sub-narratives.*

The analytical framework of the EEAS, adapted to national specificities and institutional structure, could become the foundation of the national FIMI early warning and response system, which would enable institutions to establish a common methodology and terminology for the analysis of information incidents, to create a unified database of actors, techniques and content, to enable coordinated and timely responses and to develop capacities for prediction and prevention in the long term.

CHAPTER 2:

STATUS AND CHALLENGES OF THE INSTITUTIONAL RESPONSE TO FIMI IN NORTH MACEDONIA

2.1. Synthesized findings from the qualitative research

2.1.1. General observations and perceptions

There is awareness among state actors in North Macedonia about the general issue of hybrid threats, disinformation and the potential for foreign malign influence. North Macedonia is perceived to be in a highly exposed regional setting, where information influences, especially external ones, often feed into existing political and social divisions. However, **the level of understanding of the issue varies and, unsurprisingly, is higher among representatives of the security and intelligence community.** FIMI is recognized as a complex and dynamic phenomenon that lies at the intersection of security, information and communication policies. However, given that this threat is not defined in the national legislation, it still does not have a unified institutional understanding. Some state actors identify FIMI primarily through the prism of cyber-attacks, online propaganda and manipulative content, while others associate it with broader forms of foreign influence and destabilizing communication practices. Hence, **there is a certain need for intervention in the policy-making framework.**

There is a basic institutional infrastructure in the country, but it is necessary to connect the isolated points into a system that functions coherently and decisively, with precisely defined responsibilities and activities. Although FIMI is perceived as a real and growing threat to democratic processes and national security, institutions, for the most part, approach it selectively and depending on the context, with activities most often focused on current crisis situations (electoral processes, disinformation campaigns or regional events), and not as part of a continuous, systemic mechanism for prevention and resilience. Not all stakeholders recognize their role in the broader system, and most point to the absence of institutional communication and memory, as well as a lack of human and technical capacities. Most do not recognize their institutions as either responsible or competent in this area, which implies **the need for intervention at both the strategic and political levels.**

The processes initiated in the Ministry of Digital Transformation towards the approximation of the European Network Security Directives and the Digital Services Act (DSA) **are expected to yield strong results in terms of increased cyber resilience,** and the already established **cooperation with partner countries and organizations is considered key in overcoming the challenges.**

Most **state actors were not aware of the existence of the Action Plan related to the Strategy for Building Resilience from Hybrid Threats,** and some indicated that the responsibilities entrusted to them by the strategy are not part of their institutional competence. Although it is not known whether there is a mechanism for monitoring the

implementation of the Action Plan related to the Strategy, it is evident that it has not achieved the projected results, which is why **an in-depth analysis is needed when preparing the next strategic and/or action document in the cycle.**

This indicates that **state institutions are at different stages of institutional adoption of the FIMI concept**: from basic awareness, through developing internal capacities, to practical integration into strategic documents and operational policies. This implies that awareness, knowledge and response to FIMI is **an area that needs upgrading.** Institutions recognize that building societal resilience to FIMI requires a long-term approach that goes beyond administrative and technical frameworks and relies on partnership with academia, civil society and the media. Therefore, systematic education in the area of **media and digital literacy and transparent and accountable communication** is key to raising the level of resilience to this type of threat.

2.1.2. Institutional setup and coordination

In the current institutional context, there is a need to establish a systematized and sustainable coordination mechanism between relevant actors. Although certain forms of inter-institutional communication exist, they are mainly based on informal relations and personal contacts, which creates a risk of inconsistency, limited transparency and dependence on individual capacities. This approach, although sometimes effective in the short term, does not provide long-term institutional stability and predictability in decision-making and implementation processes. Although the National Strategy for Building Resilience and Countering Hybrid Threats and its Action Plan envisage the establishment of structures and mechanisms for regular information exchange and coordination, the Security and Intelligence Community Coordination Council, which is formally envisaged as a coordinating body, does not hold regular meetings and has no visible results in the area of FIMI.

In the absence of an active centralized mechanism, institutions respond ad hoc, within their respective mandates, resulting in a fragmented response system. Individual institutions carry out limited activities such as media literacy campaigns, monitoring of disinformation content, or activities related to the protection of critical information infrastructure, but these efforts are carried out in isolation, without a common framework for coordination and information sharing.

This situation is not the result of a lack of will, but of insufficiently clearly defined roles, communication channels and coordination procedures. As a result, responses to disinformation and narratives with the potential to influence the public depend on the initiative of individual departments or persons/individuals, rather than on a systemic assessment and response mechanism.

Nevertheless, **there is potential for establishing a functional network of institutional focal points, which would enable faster communication and information exchange**

in the event of an information incident or crisis. Such a model could represent a transitional step towards establishing centralized coordination, located within existing state structures or by creating a new institution, with clearly defined protocols and responsibilities.

2.1.3. Legal and strategic framework

Although important steps have been taken in recent years towards defining national policies and strategies related to resilience to hybrid and information threats, the legal and institutional framework for dealing with hybrid threats is not yet fully established. There are relevant documents, primarily the National Strategy for Building Resilience and Countering Hybrid Threats (2021 –2025), the National Cyber Security Strategy 2025-2028, the Public Administration Reform Strategy 2023-2030, as well as activities of several line ministries and regulatory bodies, but their operationalization is limited and not coordinated.

There is no clear division of responsibilities in the area of prevention, monitoring and response to the emergence of FIMI, nor a mechanism for coordinated reporting and information exchange between institutions. As a result, some of the measures envisaged in the Action Plan of the National Strategy for Building Resilience and Countering Hybrid Threats have not been implemented or are implemented partially, most often at the sectoral level.

In terms of the normative aspect, existing laws do not recognize specific forms of foreign information influence, but focus on related areas: media regulation, cybersecurity, personal data protection and electoral processes. This creates a fragmented regulatory environment, in which some aspects of FIMI remain outside of clearly defined institutional jurisdiction, without a lead-institution to implement an integrated approach.

Nevertheless, the existing strategic framework is a good basis for further development. **It is necessary to link the strategic documents and update them in view of new challenges, as well as to create a single national document that would integrate aspects of media literacy, digital security, strategic communications and prevention of foreign information manipulation and forms of communication influence.**

2.1.4. Capacities and resources

Institutions responsible for FIMI activities face limited human, technical and financial resources. In most institutions, there are no separate departments or individuals with defined tasks for monitoring and analysing information impacts, and the existing capacities are often distributed among different organizational units.

There is a lack of continuous education for public administration employees in the areas of media and digital literacy, information analysis skills and understanding of hybrid threats. Although several training programs have been implemented in recent years (e.g. within NATO, EU and bilateral partnerships), they are not systematized and are rarely multi-sectoral.

Technical resources, especially for monitoring and analysing online content, are limited, and information exchange between institutions often relies on informal contacts. It is recognized that civil society and the media have relevant tools and expertise that the state could more effectively integrate into joint efforts to monitor and analyse disinformation campaigns.

In this context, **the need to develop a national early warning system and establish a single reference point for coordinating activities related to information manipulation, which would connect existing institutional and non-governmental resources, is underlined.**

2.1.5. Perception of opportunities and suggestions for improvement

Despite the perceived limitations, there are several positive opportunities and potential for improving the institutional response to FIMI:

- **Clear defining of roles and responsibilities through revising and updating existing strategic documents and introducing operational protocols for inter-institutional cooperation;**
- **Creating a formalized coordination mechanism or strengthening the existing Security and Intelligence Community Coordination Council with specific tasks for FIMI monitoring, analysis, and reporting;**
- **Establishing a system for continuous training and regulated exchange of experiences between institutions, the media and the academic community;**
- **Integration and promotion of media literacy and digital resilience as a permanent component in educational and administrative programs;**
- **Deepening international cooperation, especially with NATO, the EU, the Hybrid Center of Excellence in Helsinki and other partnership initiatives to combat disinformation;**
- **Supporting partnerships with academic, civic, and media organizations as a resource for fact-checking and detection of disinformation trends.**

2.1.6. Key challenges

Based on all discussions, several systemic challenges stand out that limit the state's capacity to address FIMI.

Table 3: Systemic challenges for responding to FIMI

Area	Key challenge
Institutional coordination	Absence of an active coordination mechanism and clear distribution of roles between institutions.
Capacities and resources	Insufficient number of trained personnel, limited technical tools and weak inter-sectoral exchange.
Legal framework	Lack of a legal basis that directly addresses FIMI; overlapping authorities.
Information exchange	Informal communication and lack of reporting and coordination standards.
Social resilience	Insufficient media literacy and low level of trust in institutions.
International cooperation	Limited use of existing NATO, EU and partner initiatives to combat disinformation.

2.2. GAP Analysis

This section systematizes the critical gaps between the existing strategic and legal framework and the actual institutional practice in responding to FIMI. The domains are directly mirrored by the themes of the qualitative research (2.1.), to ensure a clear transition from "where we are" to "what is missing" and later to "what we need to do" (Chapters 3 and 4). The analysis is developed by comparing: (a) the findings from the focus groups and interviews (routines, processes, capacities) and (b) the existing policies and strategies and the formal institutional set-up. Each domain is assessed according to three questions: what is missing (gap), what is the consequence and what is the necessary measure.

2.2.1. Institutional setup and coordination

Gap	Consequence	Measure
Partially formalized focal points - communications officers, with uneven functioning and unclear reporting lines; Lack of unified standard operating procedures (SOPs) and routines for inter-institutional FIMI coordination; There are communication channels, but they are not institutionalized: there are no clear procedures, routines and responsible entities in charge, insufficient awareness of their use and uneven practical application for regular and structured exchange of information, views and recommendations among stakeholders; Clear SOPs have not been developed for dealing with different scenarios, cases of escalation or crisis situations; Infrequent and unregulated short situational briefings, to provide a consolidated and updated picture of current conditions.	Difficulties in timely information sharing, joint planning, decision-making and synchronized action, especially in situations that require precise risk assessment and rapid response; Improvisation without relevant and accurate data and untimely and ineffective reaction; Ad hoc reactions to a threat or incident - different institutions react separately, without a strategy and coordinated communication, which can lead to confusion among the public and reduced trust in institutions; Duplication of efforts without clearly allocated responsibilities - different institutions may undertake similar activities without being aware of it, which wastes resources and complicates the analysis and decision-making process; Inconsistent messages to the public are key to managing public perception and maintaining social stability.	Focal points in each relevant institution, as primary contacts in the inter-institutional network, with clear responsibilities for coordination and communication for the purpose of rapid exchange of information, initiation of joint activities and timely information to decision-makers; Uniform and routine use of channels and tools for coordination, with clear entities in charge, time triggers and procedures for regular and urgent information and referral to relevant institutions; Standard operating procedures for identifying incidents, their assessment according to pre-determined criteria and coordinated institutional response for different types of situations (steps for internal communication, activation of focal points, informing the public and escalation to higher decision-making levels); Regular situational briefings between institutions for assessments of current risks, analyses of previous incidents and recommendations for improving coordination.

2.2.2. Strategic framework (operationalization)

Gap	Consequence	Measure
There are strategies, but the FIMI operational framework is insufficient: there is no common working term, roles and responsibilities are imprecise, and procedures are rarely reduced to protocols and indicators.	Uncertainty about "who is in charge" during an incident, overlapping responsibilities, and slow decision-making; Risk of overregulation due to unclear processes.	An operational framework (working definition, map of roles and responsibilities, checklists and scenarios, decision templates and public messages), supported by bylaws and guidelines, rather than immediately adopting a new law.

2.2.3. Capacities and resources

Gap	Consequence	Measure
Limited staff in key profiles (OSINT, data analytics, strategic communication); Lack of common monitoring and analysis tools; There is no policy for institutional memory.	Dependence on individuals; Uneven coverage of risks, slow detection and poor quality of analyses; Lack of institutional memory.	Training plan by level (basic–advanced–specialized); Organizing regular crisis communication trainings to ensure consistency and credibility in public messages; Institutionalizing a central "toolkit" with technical support and licenses; Formalized practices for knowledge transfer and retention (lectures, knowledge bases, mentoring).

2.2.4. Information exchange standards

Gap	Consequence	Measure
The exchange of information is most often informal; There is no standard incident template (minimum fields and metadata); There is no central repository.	Partial image and data loss; Parallel versions of the same analyses; A delayed joint response.	Standard template for reporting and tracking incidents; Joint repository with controlled access for information exchange; Designated national contact for the EU Rapid Alert System - RAS (where applicable).

2.2.5. Communication resilience and literacy

Gap	Consequence	Measure
There is a lack of systematic prebunking and debunking communication, as well as common guidelines for transparency; Low media and digital literacy in the public sector.	A void in public discourse that is easily filled with manipulative narratives; Decline in trust and greater vulnerability.	Short communication standard operating procedures (who, when, how, message); Preventive messages about expected narratives (before elections or crises); Media and digital literacy programs and formalized partnerships with academia, civil society organizations, and media.

2.2.6. Monitoring and evaluation

Gap	Consequence	Measure
There is no set of key performance indicators and a routine for monthly or quarterly reporting; Measures are rarely monitored through results.	It is difficult to measure the effect; Limited institutional learning and weak argumentation for the resources needed.	A package of key performance indicators by domain (coordination, capacities, response, communication); Quarterly briefings, annual report and review of measures.

CHAPTER 3:

COMPARATIVE EXPERIENCES AND MODELS OF FIMI RESPONSE

A comparative analysis of different national approaches allows for the identification of good practices, weaknesses and potential for adaptation in the local context. The table systematizes institutional solutions that different countries apply to deal with FIMI. By comparing legal frameworks, operational mechanisms, the role of security services, independent bodies and civil society, a clearer picture is obtained of which models have proven effective and which face structural or political limitations.

Additionally, this analysis allows for a critical review of the degree of integration between different institutions – from intelligence services to media regulators, and their ability to act in a coordinated manner. In conditions where threats are rapidly changing their nature, flexibility and an interdisciplinary approach are crucial. Therefore, the table not only serves as an analytical tool, but also as a practical resource for creating recommendations for an institutional framework applicable to North Macedonia.

Table 4: Systematized overview of national models for FIMI response

Country/ Organization	Institution / Model	Structure type	Key functions	Source
France	VIGINUM	Civil service under the Prime Minister	OSINT, digital impact analysis, inter-ministerial coordination	https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
Germany	FIMI-ISAC	Network of organizations (informal)	Information sharing, support for electoral bodies, media and civil society	https://neweasterneurope.eu/state-responses-to-fimi-and-recommendations-for-resilience/
Sweden	Psychological Defence Agency	Independent government agency	Monitoring, education, support for media and public institutions	https://cospr.org/evolving-threat-of-foreign-information-manipulation-and-interference-fimi-critical-insights-from-3rd-eeas-report/
Finland	National Media Literacy Strategy	Educational and governmental-institutional model	Education, public campaigns, research	https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU%282021%29653632_EN.pdf
Estonia	Center for Strategic Communication	Government office	Disinformation prevention, media literacy, digital resilience	https://www.hybridcoe.fi/

Lithuania	Full defence strategy, Ministry of Interior, strategic communication units	Whole-of-government and whole -of- society model	Civil and information resilience, strategic communications, cyber defence, information resilience, strategic communication, cyber defence	https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323902/lithuanias-total-defense-review/
Poland	Resilience Council, INFO OPS Polska, FIMI-ISAC (Electoral Integrity)	Coordination between multiple actors (government + civil society)	Election protection, public awareness, incident reporting, strategic coordination	https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/
Czech Republic	Government Coordination for Strategic Issues, BIS, FIMI-ISAC	Government coordination plus security community	Cybersecurity, disinformation, elections, monitoring, education	https://www.informedsociety.cz/wp-content/uploads/2024/10/EN_Safeguarding_Democracy_2024-09-26.pdf
Slovakia	Center for Countering Hybrid Threats (CCHT)	Unit at the Ministry of Interior	Monitoring, strategic communications, education, regulatory updates	https://www.hybridnehrozby.sk/ccht/
Ukraine	Centres for strategic communication	Government and military structure	Counter-propaganda, impact analysis, international cooperation	https://www.hybridcoe.fi/
Romania	National initiatives for election protection and monitoring with AI	Government strategy + regulatory bodies	TikTok monitoring, AI manipulation, election security	https://visegradinsight.eu/safeguarding-democracy-against-information-manipulation-and-hybrid-threats/
Montenegro	Ministry of Foreign Affairs (Memorandum of Understanding with the USA), CDT, Media Strategy 2023–2027	Government coordination and civil society	Disinformation, monitoring, legislative reform, transparency, protection of electoral processes	https://www.gov.me/en/article/memorandum-of-understanding-signed-between-the-ministry-of-foreign-affairs-of-montenegro-and-the-us-department-of-state-close-cooperation-for-more-effective-fight-against-disinformation
EU	EEAS / EUvsDisinfo	Pan-European institution	Archive of disinformation, diplomatic responses, sanctions	https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
NATO	Support teams against hybrid attacks	Multinational platform	Member State support, analysis, strategic communication	https://www.nato.int/cps/en/natohq/topics_156338.htm

USA	Global Engagement Center (GEC)	Interagency platform	Analysis, partnerships, strategic communication	https://govfacts.org/federal/eop/how-the-national-security-council-fights-foreign-disinformation-campaigns/
Canada	Rapid Response Mechanism (RRM)	Government platform + G7 coordination	Monitoring, public education, international coordination	https://2021-2025.state.gov/the-framework-to-counter-foreign-state-information-manipulation/
Taiwan	National digital resilience programs	Government strategy + civil society	Technological solutions, education, election protection	https://neweasterneurope.eu/state-responses-to-fimi-and-recommendations-for-resilience/

Below are five models that, although different in institutional form, share common characteristics: central/core capacity, a network of focal points, protocols (SOPs), regular risk assessment, and embedded public communication.

3.1. Estonia: a digital state with routines for awareness and coordination

Estonia bases its institutional resilience on its public administration's "digital-by-default" approach, in which (meta)data management and access to it is a standard part of everyday work. The response to information threats is carried out through the Government's Strategic Communication Centre and is ritualised: short, fixed situational briefings (1–2 pages) that are regularly prepared and distributed; focal points in ministries, agencies and critical infrastructure with clear reporting and escalation duties; and table-top exercises (TTX) that are held annually, often before sensitive periods (elections, geopolitical tensions, etc.).

The processes rely on standardized formats: incident templates with a minimum of fields (date/time, source, description, probability/impact, measures taken), a common glossary of terms, and minimum technical metadata.

An important feature is the merging of technical and communication functions: ICT/cyber and public communication teams regularly sit at the same table, which reduces the gap between technical findings and indicators and a coordinated communication message and announcement.

Strengths	Weaknesses/risks
Discipline in routines, interoperability, rapid exchange.	High dependence on digital systems; need to constantly maintain standards and plan investment and operating costs (CAPEX / OPEX) for tools and maintenance.

3.2. France (Viginum): a core government capacity against digital interference

Viginum is an example of a centralized operational capacity built into the government architecture. The team is small, professionalized, and operates under a clear mandate: monitoring the digital space for foreign interference, analytical synthesis, and alerting line departments when a criterion is met (election or crisis periods, significant impact).

The work is strictly protocolized: signal levels (indicative significant critical), reporting time windows, matrices of responsible entities in charge and formats for "ready-to-use" materials (questions and answers, fact sheets, message line). The principle is to ensure interoperability with different ministries and regulators without creating a parallel hierarchy. In terms of transparency, the model practices "minimum necessary" public information, sufficient to indicate the risk without amplifying the narrative.

Strengths	Weaknesses/risks
Clear mandate, fast line "signal decision message".	Centralization requires constant interdepartmental trust; excessive public exposure can open up unnecessary debates.

3.3. Poland: intersectoral risk assessment and quarterly briefings

The Polish model places risk assessments as the engine of coordination. Security services, ICT departments and communication teams regularly cross-reference findings and convert them into risk matrices (probability x impact), with short mitigation measures and carriers. These matrices are not administrative redundancy, but a working tool for quarterly briefings, where small, but continuous corrections are made: updating standard operating procedures for different scenarios, planning exercises, harmonizing messages.

An important element is the channel for interstate coordination: when a case has cross-border implications, there is a habit of engaging the Rapid Alert System (RAS), not to shift responsibility, but to coordinate information and response time windows.

Strengths	Weaknesses/risks
Predictable rhythm and culture of shared assessment; easy format transferability.	Danger of a "just mark it as done" approach if briefings are reduced to a mere formality; leadership that insists on actionable results is needed.

3.4. Sweden: Psychological Defence Agency

The Swedish Psychological Defence Agency institutionalizes the strengthening of societal resilience through training, counselling, and operational support. The setup is horizontal: the agency is not a centre for denial, but helps to increase capacity, which helps the relevant institutions communicate to the public in complex situations (from influential operations to crisis events).

The key practices are: training catalogues (from basic to specialized modules for communication teams, analysts, managers), guidelines for public communication in elections and crisis periods (formulating messages without amplification, working with the media, visual standards) and after-action reviews that provide institutional memory and learning.

Strengths	Weaknesses/risks
Stable focus on responsibilities and long-term learning; public trust due to advisory (not police) role.	Success depends on the good will and openness of the relevant institutions; clear criteria for priorities are needed.

3.5. Finland: literacy, partnerships and preventive communications

Finland treats the information environment as a public capacity and invests in media and information literacy programs for public administration, teachers, students, journalists and local communities. In parallel, prebunking is being developed: short, repetitive cycles of messages targeting expected narratives before elections, referendums or crisis events.

Methodologically, the Finnish approach relies on co-design with the public service, academia and civil society, which increases legitimacy and reach. Messages are tested for clarity and trustworthiness, rather than just reach, and indicators such as understanding, trust and "time to correction" are regularly measured. This creates a culture in which public institutions possess communication competence, rather than relying solely on immediate correction in a crisis.

Strengths	Weaknesses/risks
High social legitimacy and partnerships; measurability of effects.	Slower cycle of results; long-term support and political consensus for programs are needed.

CHAPTER 4:

POLICY OPTIONS FOR FIMI RESPONSE IN NORTH MACEDONIA

This chapter offers three realistic architectures for a systemic response to FIMI. The intention is to provide a clear choice between different paths, each with distinct functions, advantages, and limitations.

4.1. Option A: Standalone National Resilience Center

Management setup

An independent public entity (agency, centre) established by a separate act, with its own budget and a clearly defined mandate. The centre is independent in analytical work, but responsible for coordination with line institutions through formalized mechanisms (memoranda, rulebooks). A supervisory or advisory committee ensures transparency and alignment with national strategies.

Key functions:

- National monitoring and analysis of the information landscape (FIMI), including trends, narratives and techniques;
- Coordination of institutions through a network of focal points and regular briefings;
- Standards for information exchange and central repository (formats, metadata, confidentiality levels);
- Catalogue and implementation of training courses (basic–advanced–specialized);
- Support for institutional communication (prebunking and debunking, Q&A, fact sheets);
- Monitoring and evaluation logic (performance indicators, quarterly and annual reports).

Processes and standard operating procedures

The Centre adopts a "minimum set" of standard operating procedures: report-assessment-response (with time windows), a matrix of decision-makers, alert levels and situation templates (elections, crises, sensitive events). A cycle of regular situational (monthly) briefs and thematic analytical notes is built in.

Resources and staff

Core of 15–25 professionals (OSINT/data analytics, cyber/technical profiles, strategic

communications, regulatory lawyer, monitoring and evaluation). Central set of monitoring and analytics tools, with shared licenses and technical support.

Public relations and communication

Not a centre for issuing rebuttals, but a service for the entities in charge of the messages (ministries and agencies): it prepares communication recommendations, coordinates preventive messages before sensitive periods, and provides materials for immediate application.

International cooperation

Official contact with European mechanisms (e.g. RAS) and with thematic centres (e.g. Hybrid CoE), participation in training and simulation exercises and sharing of standards.

Advantages

Clear institutional identity; centralized expertise and tools; stable institutional memory; high accountability and visibility.

Limitations

Need for a new legal framework and budget; risk of duplication if roles are not precisely defined; time needed for staffing and procedures.

4.2. Option B: National Coordination Mechanism under the Government

Management setup

A coordination office embedded in the Government (under the Prime Minister, General Secretariat, etc.), which functions as a "core + network". The core coordinates, and the departments implement and carry out. The political vertical line allows for rapid escalation and synchronization between ministries and agencies.

Key features

- Organizing monthly situational briefings and quarterly risk assessments (probability x impact). The PMESII and AIC frameworks are practical for structuring assessments (US Army, 2015);

- Agreed standard template for reporting and monitoring incidents and interdepartmental repository (can technically be hosted by an existing institution);
- Harmonization of public communication (guidelines, Q&A, fact sheets);
- Coordination of training catalogue (implementation through departments and partners);
- Connection with NATO and EU mechanisms.

Processes and standard operating procedures

The basis is "simple but binding" standard operating procedures for application-assessment-response: clear steps and deadlines; a matrix of entities that are in charge; an escalation ladder (who-to-whom-when). The internal calendar creates a rhythm (monthly at the technical level, quarterly at a higher level).

Resources and staff

The core consists of 8-12 people (coordinators, analysts, communications specialists, a lawyer and a monitoring and evaluation coordinator). Monitoring and analysis tools are provided through framework agreements and licenses and are used through the existing platforms and capacities of the institutions, without duplicating infrastructure.

Public relations and communication

Message coordination is a supporting function: agreed communication guidelines, a calendar of authorized speakers, and short pre-emptive briefings before sensitive topics. Public visibility is moderate, as the main emphasis is on timely internal coordination and providing lists of facts, questions, and answers that departments can immediately use. Online channels allow for "connective action" and rapid mobilization of audiences (Bennett & Segerberg, 2012).

International cooperation

The Government Office acts as a single point of contact towards RAS, EEAS and partner governments, enabling rapid and formal exchange of information, timely participation in forewarnings and involvement in joint analyses and exercises.

Advantages

Quick start without a new institution; strong interdepartmental weight; minimal institutional footprint; easy alignment with existing resources.

Limitations

Dependence on stability of political leadership and priorities; risk that analytical depth will be limited if the core is too small; visibility to the public and academia may be lower.

4.3. Option C: Strengthening the existing Security and Intelligence Community Coordination Council

Management setup

Building on the existing Security and Intelligence Community Coordination Council, with a clear mandate for FIMI. A "secretariat core" is created to provide processes, documentation and analytical support, while the sectors remain as primary implementing bodies.

Key features

- Calendar of routine meetings (monthly at technical level, quarterly at management level);
- Adopting standard operating procedures with scenarios, checklists and clear escalation channels;
- Common repository and standard format for incidents and analyses;
- Internal communication line: a clear path "who writes - who checks - who approves - who publishes", with templates for questions and answers and designated spokespersons, and coordination with relevant stakeholders as needed;
- Involvement in European mechanisms through designated contact points.

Processes and standard operating procedures

The focus is on "bringing coordination to life": regular briefings, documented decisions, and monitoring of execution. Routines and "careful organization" increase organizational certainty and resilience (Weick & Sutcliffe, 2007). Standard operating procedures must be specific (who, what, when), with brief status indicators.

Resources and staff

A secretariat core of 5-8 people with process and analytical competence, a network of focal points in relevant institutions, and the use of existing tools and infrastructure without

duplication. Investments in human capacity, processes, and infrastructure are a prerequisite for sustainability (UNDP, 2021).

Public relations and communication

The Council traditionally functions as an internal coordination body, and public communication is carried out through the relevant institutions. Clear rules are needed on when and how to issue coordinated messages and who is the authorized speaker in specific situations. Greater transparency is associated with higher trust in the institutions (Grimmelikhuijsen et al., 2013).

International cooperation

Contacts with external partners are maintained through the departments and through appointed focal points, and the secretariat coordinates documents, formats and deadlines.

Advantages

Lowest institutional cost; utilization of existing architecture and trusted channels; relatively fast operationalization.

Limitations

Lower public visibility; risk that coordination will remain formal without real implementation; dependence on discipline and stable leadership in the Council.

Table 5: Architecture options for FIMI system response

Options	Option A: Standalone centre	Option B: Coordination mechanism under the Government	Option C: Strengthened Security and Intelligence Community Coordination Council
Management setup	An independent public entity (agency/centre) with its own budget and supervisory/advisory committee.	Coordination office under the Prime Minister/ General Secretariat ("core + network").	Existing Council with a secretariat core and an expanded mandate.

Options	Option A: Standalone centre	Option B: Coordination mechanism under the Government	Option C: Strengthened Security and Intelligence Community Coordination Council
Mandate and functions	Monitoring and analysis of FIMI; coordination through focal points; standards and repository; training; communication support; monitoring and evaluation; EU/NATO liaison.	Routine coordination; monthly briefings and quarterly assessments; standard template and sharing; harmonized public communication; training catalogue; EU/NATO liaison.	Regular meetings (technical/management level); standard operating procedures with scenarios; common repository; internal communication lines; EU contacts through focal points.
SOPs	Formalized SOPs (report-assessment-response); alert levels; situation templates; monthly briefings.	"Easy" but binding standard operating procedures; calendar (monthly/quarterly); escalation channels.	Revitalizing coordination: specific standard operating procedures, checklists; documented decisions and monitoring.
Staff (approx.)	Core 15–25 (OSINT/analytics, cyber /technical, communications, law, monitoring and evaluation).	Core 8–12 (coordination, analytics, communications, law, monitoring and evaluation).	Secretariat 5–8 + focal points in institutions.
Tools/ repository	A central toolkit and hosted national repository of metadata standards.	Coordinated approach (framework agreements/ licenses); repository hosted at an existing institution.	Using existing tools; agreed repository and format.
Communication with the public	Prepares "ready-to-use" recommendations/ materials; supports the departments in charge of messages.	Coordinates messages and scheduling of the entity in charge; medium public visibility.	Mainly internal coordination; public communication through departments.
International cooperation	Formal interface to EU and NATO mechanisms; participation in training and specialized exercises.	Natural government interface to EU/NATO mechanisms; rapid formal communication.	Contacts through departments and designated points; coordination through the secretariat.
Advantages (summary)	Clear identity; centralized expertise; stability and high accountability.	Quick start; strong interdisciplinary weight; minimal institutional footprint.	Lowest institutional cost; uses existing channels; fast operationalization.

Options	Option A: Standalone centre	Option B: Coordination mechanism under the Government	Option C: Strengthened Security and Intelligence Community Coordination Council
Limitations (summary)	New legal/budgetary framework and separation of roles needed.	Dependence on political continuity; risk of shallow analytics if the core lacks capacity.	Historical inertia; lower public visibility; success depends on discipline.
Time to operationalize	Longer term (requires design and establishment before launch).	Short term (operational in a few months).	Short–medium term (reforming what is in place and establishing routines).

CHAPTER 5:

CONCLUDING OBSERVATIONS AND RECOMMENDATIONS FOR IMPLEMENTATION

5.1. Concluding observations

North Macedonia, as a country with a strategic geopolitical position, a NATO member and clearly expressed ambitions for EU integration, is at a point where it must develop a national response to FIMI within a comprehensive and coordinated framework. Building societal and institutional resilience cannot be achieved through isolated activities, but by setting up an integrated system based on strategic advancement, institutional coordination, education, public awareness and international cooperation.

The National Strategy for Building Resilience and Countering Hybrid Threats (2021-2025) needs to be revised and upgraded, based on modern analyses and new threat typologies, such as cognitive operations and algorithmic influence. The strategy must be a living document that will adapt to the changing security environment through a built-in monitoring and evaluation mechanism, which will allow for dynamic adaptation of policies. In addition, legislative intervention is essential. The legal definition of FIMI is a prerequisite for effective institutional coordination and accountability. To enable informed decision-making, it is necessary to establish assessment tools that will use models applicable to the analysis of hybrid threats and the assessment of risks in the operational environment.

Resilience to FIMI depends on the existence of a national coordination mechanism, which will enable regular information exchange, joint assessment and coordinated response. To achieve this, it is necessary to strengthen institutional capacities through investment in human resources, digital infrastructure and analytical technologies. At the same time, the state must build institutional memory, i.e. a system for archiving, analysis and learning from previous cases, which will prevent the repetition of failures and increase prevention. The involvement of civil society, academia and the media in the processes will enable the creation of a more transparent, inclusive and sustainable system of resilience.

Education and media literacy also play a central role in building a resilient society. National media and digital literacy programs that reach all age groups and are integrated into formal and non-formal education need to be promoted. In addition, specialized training for public administration and media professionals is needed to strengthen their capacities to recognize, analyse, and respond appropriately to information manipulation.

Building societal resilience also requires citizen engagement. Systematic information and educational campaigns are a key instrument for strengthening critical thinking and recognizing disinformation. In that process, transparent and accountable institutional communication is the foundation of trust between institutions and citizens.

Finally, regional and international cooperation is a prerequisite for an effective response to FIMI. Integration into the European mechanisms FIMI Toolbox and Rapid Alert System (RAS), developed by the European External Action Service (EEAS), is particularly important for the timely recognition and neutralization of foreign influences.

5.2. Recommendations for implementation

For North Macedonia to transform its institutional architecture for an integrated response that not only reacts to threats, but also anticipates, analyses, and prevents them, this policy paper recommends three policy options: (1) A stand-alone National Resilience Center, (2) A National Coordination Mechanism under the Government, or (3) A Strengthened Security and Intelligence Community Coordination Council. The approach envisions steady building of routines that will endure across leadership and priorities, with the intention that the system will work in normal circumstances, not just in crises.

Regardless of the selection of institutional model, this document provides the following **recommendations or roadmap for implementation:**

- **Ensure a clear ownership of the process and formal legitimacy.** Whether it is a stand-alone centre, a government coordination mechanism, or a strengthened **council, the mandate should be explicitly described in brief: w**ith stated objectives, scope, responsibilities, and clear channels and rules for cooperation with key institutions.

- Each relevant institution should nominate a focal point and a deputy, with a one-page description of the role, the steps when and to whom the case is forwarded, and the obligations for regular reporting.

- Establish a calendar of routines once this minimum infrastructure is set up, including: short technical meetings with a monthly situational briefing and more compact higher-level meetings once a quarter, where guidance is provided, decisions are monitored and course corrections are made where necessary. To ensure that nothing is lost in operational speed, a short decision record is prepared after each meeting on what was decided, who is responsible and what comes next.

- Define the main procedure of "report-assessment-response". It is established by a clear document that states: what information is reported, in what minimum format, to whom it is submitted and the deadline for submittal; how a risk assessment is performed (a simple matrix: probability x impact); and how a decision to respond is made, with clearly defined responsibilities and time thresholds. This logic is complemented by several universal scenarios (election period, crisis situations, sensitive events), for which checklists, bearers and format of output materials are prepared in advance. The clear definition of when and to whom the case is forwarded is raised to a higher level. On one page it is determined: who decides at the technical level, when the political entity in charge is involved and at what point the public is informed. These thresholds make the procedure predictable and fair.

- Develop institutional competences. At least three types of profiles are needed at the "core" of the system: analytics and open sources (with data literacy), ICT/ cyber connectivity with the ability to translate a technical signal into an operationally understandable message, and strategic communication to formulate accurate, clear and reliable communication materials. This is complemented by legal support for regulatory issues and coordination for monitoring and evaluation, even if some of these roles are shared. This staff profile only

makes sense if it is supported by a common set of monitoring and analysis tools and by a simple, stable infrastructure for recording cases.

- Create a three-level training catalogue: basic modules for all focal points, advanced for analysts and communicators, and specialized for election and crisis scenarios. Each training should have a clear objective, a timeline, and a visible outcome (a tool or document for use), with an official certificate of completion that will maintain institutional memory even during staff rotations.

- Prepare short, understandable messages about expected narratives before they appear in sensitive periods. Instead of waiting for a rebuttal, communication with the public deserves special, preventive treatment. These explanations for prebunking threats *are* not propaganda, but a service for citizens: what is fact, what is speculation and where to check information. When correction is necessary, a standard format of Q&A and fact-lists are used that can be quickly taken over by the institutions in charge. The rule of "minimum necessary" exposure is important: the public should be informed, but without unnecessarily amplifying manipulative narratives. For this to work, there should be an updated list of contacts and a clear protocol for working with the media and platforms, with guidelines for transparency and time coordination.

- Standardize information exchange to reduce noise and speed up decisions. Each incident or relevant observation is recorded with a minimal but mandatory set of fields: date and time, source or link, short description, probability and impact assessment, actions taken, and current status. These records are stored in a shared, controlled location with versioning and basic metadata; where the repository it is hosted is not paramount, rather it is most important that it is stable, consistent and with clear levels of access. When the case has cross-border aspects, the internal protocol should specify who and when initiates the activation of European channels, in particular the Rapid Alert System (RAS), thus making the national effort part of a wider coordination.

- Establish minimum measurability so the system can learn. There is no need for complex indicator frameworks; a small set of indicators in each domain is sufficient: regularity and quality of briefings and meetings; number and coverage of trained focal points; time from signal to first coordinated message; reach and understandability of communications; and percentage of records arriving in a standard format. These indicators are consolidated into a short monthly situational brief and a quarterly review in which there is always room for two or three specific corrective measures. Establishing a system of lessons learnt feeds institutional memory and reduces dependence on individuals.

This roadmap sets out the minimum, but key infrastructure: clearly established entity in charge, a network of contact points, practical procedures, core competences, predictable communication and measurability that fosters learning. Thus, no matter if a stand-alone centre, a government coordination mechanism or a reformed council is selected, the system develops a "rhythm" that turns good intentions into everyday practice.

ABOUT THE AUTHORS

Aleksandar Grizhev, PhD, is an Associate Professor at the Military Academy "General Mihailo Apostolski" – Skopje and Head of the Department of Social and Human Sciences. His teaching and research focus is on security and defence studies, post-conflict stabilization and reconstruction, security sector reform (SSR), radicalization and violent extremism, cognitive operations and gender perspective in the armed forces and the broader security sector. He has operational experience from international missions, including participation in the OSCE Special Monitoring Mission to Ukraine (2019–2021), as well as previous engagements in conflict and post-conflict environments. He regularly participates in international forums and is part of various projects and activities with national and international partners (NATO Science and Technology Organization, NATO Committee him Gender Perspective, OSCE, UN, RACVIAC, PfP Consortium). With a particular interest in the cultural and religious dimensions of operations, he researches building institutional resilience to hybrid threats, with a particular focus on FIMI, institutional coordination, public resistance to manipulative narratives, and ethical communication in the security sector.

Vesna Poposka, PhD, is a university professor, independent analyst and the only woman to have defended her doctorate at the Military Academy "General Mihailo Apostolski" in Skopje - a feat that makes her a woman pioneer in security and defence studies in North Macedonia. Her expertise covers issues in the field of national security, hybrid threats, democratic resilience and the legal framework of defence policies. As an associate professor at the Military Academy in Skopje, she actively contributes to the development of contemporary curricula in the field of security and defence, with a focus on hybrid threats, strategic communication and building institutional resilience. Her academic engagement is accompanied by numerous public appearances, panel discussions and publications. Poposka has attended the Council of Europe School of Political Studies, the Presidential School for Young Leaders and the Warsaw Security Forum - three prestigious platforms that shape her strategic perspective and connect her with leading European and global security networks. She is a visiting researcher at the Prespa Institute, where she works on projects related to democracy, human rights and regional stability, with a particular emphasis on institutional resilience to hybrid influences. Vesna Poposka is a vocal supporter of gender equality in the security sector and advocates for greater inclusion of women in decision-making and policy-making processes.

REFERENCES

- Banas, J.A. & Miller, G., 2013. *Inducing resistance to conspiracy theory propaganda: Testing inoculation and metainoculation strategies. Human Communication Research*, 39(2), pp.184–207.
- Bennett, W.L. & Segerberg, A., 2012. The logic of connective action. Information, Communication & Society, 15(5), pp.739–768.
- Bleyer-Simon, K. (2025). Addressing Foreign Information Manipulation and Interference in the Context of European Regulations. Institute of Communication Studies. ResPublica, Skopje.
- Bryman, A. (2016) Social Research Methods. 5th edn. Oxford: Oxford University Press. Government of the Republic of North Macedonia (2021).
- Center for Democratic Transition (CDT) (2024). *Foreign Influences on the Electoral Process in Montenegro* 2016–2023. Podgorica: CDT. Available at: https://en.cdtmn.org/wp-content/uploads/2024/05/CDT-Foreign-Influences-on-the-Electoral-Process-in-Montenegro-2016%E2%80%932023.pdf
- EU Election Observation Mission (2025). *Preliminary Statement - Parliamentary Elections, Kosovo, 9 February 2025*. Pristina: EU EOM, 11 Feb. Available at: https://www.eods.eu/library/EU%20EOM%20Kosovo%202025_Preliminary%20Statement_ENG.pdf
- European Commission, 2020. *Action Plan Against Disinformation*. Brussels.
- European Commission (2023) *Flash Eurobarometer 528: Citizenship and Democracy*. Fieldwork: April–May 2023; Published: 6 December 2023. Luxembourg: Publications Office of the EU.
- European External Action Service – EEAS (2023). *1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. Towards a framework for networked defence. Brussels: EEAS.*
- European External Action Service – EEAS (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence.*
- European External Action Service (2025) *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI).*
- EU StratCom Task Force, 2022. *FIMI Toolbox Overview.*
- Grimmelikhuijsen, S.G. et al., 2013. *The effect of transparency on trust in government: A cross-national comparative experiment. Public Administration Review*, 73(4), pp.575–586.
- Hadzi-Janev, M. And Stoilkovski, M. (2025). Foreign Information Manipulation and Interference in the Republic of North Macedonia: Baseline study. Skopje: Institute of Communication Studies. ResPublica. Skopje.
- Hoffman, F.G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies.

- House of Commons Library (2024). *Romania: recent political developments and 2024 elections* (CBP-10164), 23 December. London: UK Parliament. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-10164/?utm_source=chatgpt.com
- International Republican Institute (2024). Western Balkans Regional Poll February–March 2024.
- IREX (2023) *Vibrant Information Barometer 2023: Montenegro*. Washington, DC: IREX. Available at:https://www.irex.org/files/vibrant-information-barometer-2023-montenegro.pdf?utm_source=chatgpt.com
- Keohane, R.O. & Nye, J.S., 1998. *Power and Interdependence in the Information Age*. Foreign Affairs, *77*(5), pp.81–94.
- Livingstone, S. & Helsper, E.J., 2007. *Gradations in digital inclusion: Children, young people and the digital divide*. New Media & Society, 9(4), pp.671–696.
- Mozilla Foundation (2024). *Election Manipulation in Brazil's 2022 General Elections: The Role of WhatsApp and Telegram on the Attacks Against Electoral Integrity*. 27 February. Available at: https://www.mozillafoundation.org/en/research/library/global-elections-casebook/brazil-case-study/
- National Strategy for Building Resilience and *Countering Hybrid Threats* 2021–2025 (with Action Plan). Skopje.
- NATO, 2020. Countering Hybrid Threats. NATO Review.
- OECD, 2017. *Evaluating Development Activities: 12 Lessons from the OECD DAC*. Paris.
- Pamment, J., 2020. *Resilience to Foreign Information Manipulation: The Role of Strategic Communication*. Carnegie Endowment.
- Popovska V. (2024). Информирана одбрана – Вовед за хибридните закани за критичната инфраструктура. PRESPA Institute – Skopje. Available at: http://www.prespa-institute.mk/wp-content/uploads/2024/02/Informirana-odbrana.pdf
- Reuters (2025). '*Does Musk's interview with German AfD leader square with EU laws?*', 9 January. Available at: https://www.reuters.com/world/europe/how-musks-interview-with-german-afd-leader-squares-with-eu-laws-2025-01-09/
- Rid, T., 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
- UNDP, 2021. *Institutional Capacity Assessment Framework*.
- US Army, 2015. *Operational Environment Assessment*: PMESII-PT.
- Wardle, C. & Derakhshan, H., 2017. *Information Disorder: Toward an Interdisciplinary Framework*. Council of Europe.
- Weick, K.E. & Sutcliffe, K.M., 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Wiley.

CIP - Каталогизација во публикација
Национална и универзитетска библиотека «Св. Климент Охридски», Скопје

342.5:[316.776.23:327.8(497.7)(047.31)

GRIZHEV, Aleksandar
Institutional response to foreicn information manipulation and interference In North Macedonia [Електронски извор] : models and policy options : policy paper / [authors Aleksandar Grizhev, Vesna Poposka ; translation from Macedonian to English Olivera Celeska]. - Skopje : Institute of communication studies, 2025. - (Edition ResPublica)

Начин на пристапување (URL):
https://respublica.edu.mk/wp-content/uploads/2025/12/institutional-response-to-fimi_en.pdf.
- Превод на делото: Институционален одговор на странското мешање и манипулирање со информации во Северна Македонија : модели и опции за политика : документ за јавна политика. - Текст во PDF формат, содржи 53 стр. - Наслов преземен од екранот. - Опис на изворот на ден 05.12.2025.
- За авторите: стр. 51. - Библиографија: стр. 52-53

ISBN 978-608-4805-66-3

1. Гл. ств. насл. 2. Poposka, Vesna [автор]
а) Дезинформации -- Странски влијанија -- Институционален одговор -- Македонија -- Истражувања

COBISS.MK-ID 67628549

Institute of Communication Studies
www.iks.edu.mk
info@iks.edu.mk

British Embassy Skopje
UK International Development
Partnership | Progress | Prosperity

This product was prepared as part of the UK Government-funded project "TRACE: Tracking, Exposing, and Countering Hidden Foreign Manipulations and Interferences", with support from the British Embassy in Skopje. The opinions and views expressed in this content do not necessarily reflect those of the British Government.