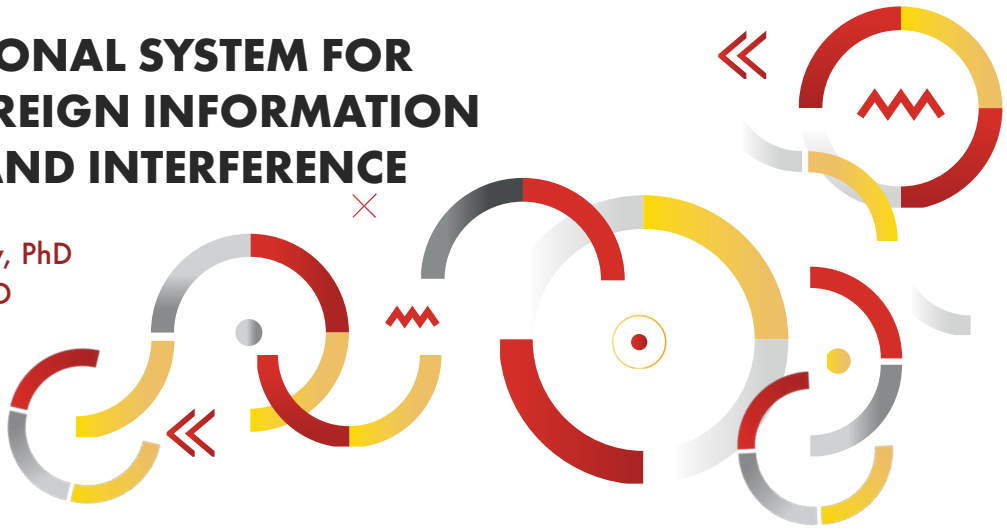
POLICY BRIEF

Institute of Communication Studies

TOWARDS A NATIONAL SYSTEM FOR RESILIENCE TO FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

Assoc. Prof. Aleksandar Grizhev, PhD
Assoc. Prof. Vesna Poposka, PhD
Dejan Andonov, MSc



SUMMARY

Foreign Information Manipulation and Interference (FIMI) is a silent, but powerful threat that aims to undermine trust in institutions, disrupt the democratic process, and deepen polarization in society. North Macedonia, as a country at the crossroads of geopolitical interests, urgently needs to establish an integrated and functional system to respond to such threats. Although there is awareness of the problem and basic institutional infrastructure is in place, the national approach is still fragmented, reactive, and dependent on individual initiatives, lacking a coordinated and sustainable mechanism.

Therefore, an institutional solution is needed that will unite public institutions, the media, academia and civil society in joint defence against information influences. To this end, three models present as options: the creation of a standalone centre for digital or national resilience, the formation of a national coordination mechanism under the Government, or integration into the Security and Intelligence Community Coordination Council.

Regardless of the model, the goal is the same – to establish a national system based on inter-institutional coordination, media literacy, public awareness raising, and international cooperation.

RECOMMENDATIONS FOR THE GOVERNMENT

- Define an institutional model and a lead institution 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 the human capacities;
- Establish preventive communication about expected manipulative narratives;
- Exchange information through a common base; and
- Establish performance indicators.

Additional measures and policies should be taken, such as:

- Revision and upgrade of the Strategy for Building Resilience and Countering Hybrid Threats (2021 – 2025);
- Strengthening institutional capacities for monitoring and analysis;
- Introducing media and digital literacy programs in the public sector;
- Involving academia and civil society through formalized partnerships;
- Greater integration with NATO and EU mechanisms to combat FIMI.

Information threats as a new front line

Foreign Information Manipulation and Interference (FIMI) is a generic term for (mal)intent and coordinated activities by foreign state or non-state actors, whose aim is to shape public opinion, disrupt democratic and electoral processes, and weaken stability and trust in the institutions of another country. FIMI is essentially an abuse of democratic principles and tools - it attacks the adversary with disinformation campaigns by using the open systems (free media, social media, political pluralism) that democracy guarantees.

The rapid development of digital technologies, expanding connectivity and the transnational nature of information flows allow such operations to be carried out more efficiently - through the use of coordinated networks, covert identities and generative artificial intelligence, while becoming more difficult to detect.

In the European context, FIMI is recognized as a security and foreign policy threat that requires a coordinated, inter-sectoral response, with an emphasis not only on the content, but also on the tactics, techniques and procedures of influence and interference. Therefore, we should not dismiss FIMI as a distant threat. A clear and coordinated mechanism is needed that brings the institutions, media, technology, and citizens together in united defence.

Challenges of the institutional response to FIMI

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 its national response to FIMI in a comprehensive and coordinated framework.

There is awareness among state actors about the general issue of hybrid threats, disinformation and the potential for foreign harmful influence. It is evident that the state is located in a highly exposed regional environment, where information influences of external origin often build on existing political and societal divisions. However, **the level of understanding of the issue varies and, understandably, is higher among representatives of the security and intelligence community.** FIMI is recognized as a complex and dynamic phenomenon that stands at the intersection of security, information and communication policies. However, given that this threat is not defined in domestic legislation, there still isn't a unified institutional understanding of it. Some state actors identify FIMI primarily through the lens 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 definite need for intervention in the policy-making framework.**

The country **has a basic institutional infrastructure, but it is necessary to connect the isolated dots into a system** that functions coherently and decisively, with precisely defined competences 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 dependently on the context, with activities most often focused on current crisis situations (electoral processes, disinformation campaigns or regional events), and not in the framework of a continuous, systemic mechanism for prevention and resilience. The Security and Intelligence Community Coordination Council, which is formally envisaged as a coordinating body in the Strategy for Building Resilience and Countering Hybrid Threats (2021–2025), does not hold regular meetings and has no visible results in the area of FIMI. 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 leading institutions or competent institutions in that area, which implies that **intervention at both the strategic and political levels is necessary.**

It is expected for the processes initiated in the Ministry of Digital Transformation to yield strong results in terms of increased cyber resilience, and the already established **cooperation with partner countries and organizations is considered crucial in overcoming the challenges.**

Most **state actors are not aware of the existence of the Action Plan that is linked to the Strategy for Building Resilience and Countering Hybrid Threats**

(2021–2025), nor do they recognize the responsibilities entrusted to them by the Strategy as 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 clear 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 concept of FIMI**: 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 are **areas in which upgrading is needed.** 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** are key to raising the level of resilience to this type of threat.

Institutional response and coordination options

Establishing a national model for countering FIMI will enable North Macedonia to move towards an integrated, functional and sustainable institutional response system. Building societal and institutional resilience cannot be achieved through isolated activities, but by building a system based on inter-institutional coordination, media literacy, strengthening public awareness, and international cooperation. Hence, the following options for an institutional solution are proposed:

- **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**
  Envisages integrating the mechanism through a "core + network" coordination office. This will ensure political gravitas, interoperability and rapid response in crisis situations, but potential risks are it being overburdened with other issues, being dependent 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 existent structure by expanding its mandate in the area of FIMI. The advantage is in the rationalization of an already established structure, but the risk is in the lower public visibility and the coordination remaining just "on paper", which requires discipline and clear standard operating procedures.

Works consulted:

- Grizev A., Poposka V. (2025). Institutional Response to Foreign Information Manipulation and Interference in North Macedonia: Models and Policy Options. Institute of Communication Studies. ResPublica Edition, Skopje
- National Strategy for Building Resilience and Countering Hybrid Threats 2021 – 2025 (with Action Plan). Skopje.
- European Commission (2020). Action Plan Against Disinformation. Brussels.
- European External Action Service (2023). 1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. Towards a framework for networked defence. Brussels: EEAS.
- European External Action Service (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence.



Read more on this topic in the Policy Paper

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

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.