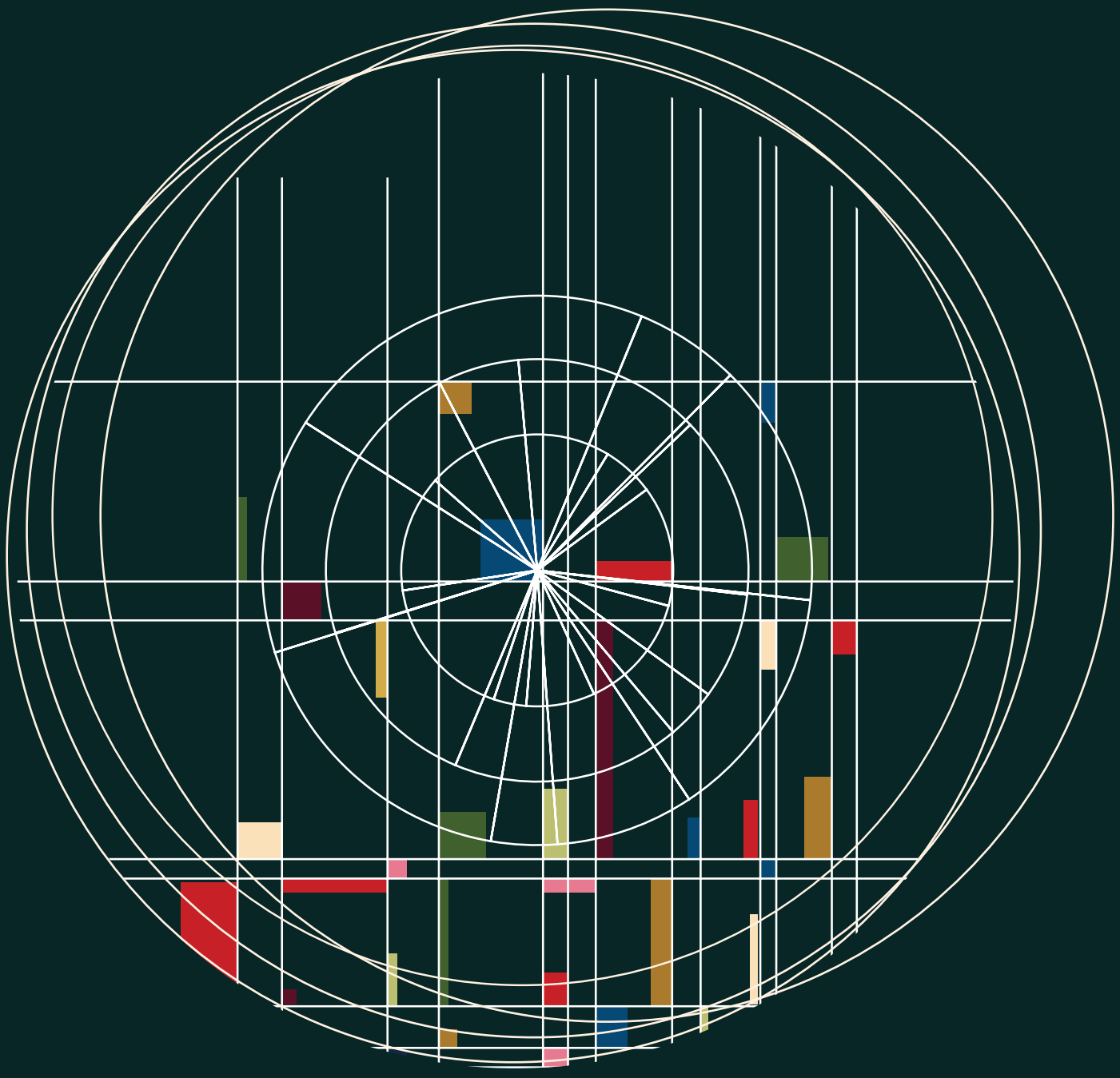
THE MEDIA ECOSYSTEM AND Foreign Information Manipulation and Interference in North Macedonia

Policy Paper



DOI: 10.64370/ETZL4884

Institute of Communication Studies

respublica

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

For the publisher:
Prof. Dr. Zaneta Trajkoska, PhD

Edition:
ResPublica

Authors:
Assoc. Prof. Marina Tuneva, PhD
Dragan Sekulovski, PhD

Editors:
Dejan Andonov, MSc
Aleksandra Temenugova

Translation from Macedonian to English:
Olivera Celeska

Original title:
Медиумскиот екосистем и странското мешање и манипулирање со информации во Северна Македонија - документ за јавна политика

Graphic design:
Zoran Kardula

Graphic editing:
Dejan Joveski

Place and year:
Skopje, 2026

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

004.738.5-05:327.8]:34(4-672ЕУ:497.7)(078.7)

TUNEVA, Marina
The media ecosystem and foreing information manipulation and interference in North Macedonia [Електронски извор] : policy paper / [authors Marina Tuneva, Dragan Sekulovski ; translation from Macedonian to English Olivera Celeska]. - Skopje : Institute of communication studies, 2026. - (Edition ResPublica)

Начин на пристапување (URL): http://respublica.edu.mk/wp-content/uploads/2026/01/the-media-ecosystem-and-fimi-policy-paper-en.pdf. - Превод на делото: Медиумскиот екосистем и странското мешање и манипулирање со информации во Северна Македонија : документ за јавна политика. - Текст во PDF формат, содржи 50 стр. - Наслов преземен од екранот. - Опис на изворот на ден 29.01.2026. - Фусноти кон текстот. - Библиографија: стр. 47-50

ISBN 978-608-4805-79-3

1. Sekulovski, Dragan [автор]
а) Медиуми -- Странски влијанија -- Македонија -- Истражувања

COBISS.MK-ID 67993861

Contents

EXECUTIVE SUMMARY **5**
INTRODUCTION **8**
Methodology **11**
1. CONTEXT AND PROBLEM: FIMI AS A CHALLENGE TO MEDIA INTEGRITY AND DEMOCRATIC PROCESSES **12**
1.1. FIMI Exposure Matrix: A Framework for Mapping Channels 15

2. EUROPEAN REGULATORY AND STRATEGIC CONTEXT FOR FIMI IN THE MEDIA AND DIGITAL ECOSYSTEM **17**
2.1. Regulatory instruments: platform accountability, transparency and protection of media pluralism 18
2.2. The Council of Europe and the security perspective: human rights, design and resilience 19
2.3. Implications for North Macedonia: obligations and opportunities in the context of EU integration 19

3. PERCEPTIONS AND NEEDS RELATED TO FIMI IN THE MEDIA ECOSYSTEM IN A NATIONAL CONTEXT **21**
3.1. Media and electoral legislation: normative basis, without an integrated approach for FIMI 24
3.2. Digital regulation and the online environment: limited regulatory scope beyond traditional media 24
3.3. National Security and Hybrid Threats: Risk Recognition Without Media Operationalization 25
3.4. Cybersecurity and legislation: a strong foundation for incident management, but not a substitute for a FIMI approach 26
3.5. Education and media literacy: prevention and long-term resilience 27
3.6. Synthesis: what is missing in the system and why it matters 28

4. APPLICATION OF THE FIMI EXPOSURE MATRIX IN THE CONTEXT OF NORTH MACEDONIA **30**
4.1. How and why do we use the Matrix? 31
4.2. What this means in practice: recurring scenarios relevant to North Macedonia 32

5. EXISTING MECHANISMS AND GAPS IN THE RESPONSE OF THE STATE AND THE MEDIA SECTOR **34**

5.1. State mechanisms: relevant elements exist, but a unified framework is lacking 35
5.2. Self-regulation and media practices: a strong foundation, but with limitations in the online environment 36
5.3. The role of civil society and international partners: pivotal role, but without a permanent coordination platform 37
5.4. Key gaps through the prism of the FIMI Exposure Matrix 37

6. CONCLUSION AND PROPOSED POLICY MEASURES 39
6.1. Conclusion 40
6.2. Proposed policy measures 41

EXECUTIVE SUMMARY

Foreign Information Manipulation and Interference (FIMI) is a complex systemic risk to democratic societies that is particularly manifested and amplified through the media. FIMI operates through the coordinated activities of foreign state and non-state actors, their proxies and coordinated channels, which, among other things, exploit the economic, institutional and digital vulnerabilities of the media to influence public debate, trust in institutions and democratic processes.

This policy paper analyses this phenomenon in the context of North Macedonia, focusing on the media ecosystem, the regulatory framework and institutional mechanisms, and proposes measures to reduce the risks, while fully upholding freedom of expression and in line with European regulatory frameworks. Instead of attribution to specific operations, the paper applies an analytical framework - the European FIMI Exposure Matrix, to identify techniques, channels and actors that enable manipulation and interference.

The analysis shows that **in the national context, FIMI is not regulated as a separate and integrated area**, and its relevant aspects are dispersed across media and electoral legislation, digital regulation, cyber and national security frameworks, and educational policies. This fragmented approach allows for **partial detection, but not systemic risk management**. Media and electoral regulation provide important democratic guarantees, however, they remain predominantly reactive and content-specific. Digital regulation and cyber legislation establish a solid foundation for managing technical risks and incidents, but do not treat FIMI as a media problem.

The findings point to **systemic factors that increase the media's susceptibility to manipulative influence**. Physical and online attacks, legal threats and insufficient institutional protection diminish the capacity for research, verification and critical reporting, which are crucial to recognizing and exposing coordinated information influences. The limited media market, financial pressures and incomplete transparency increase the vulnerability of some media outlets to pressures and influences and narrow editorial autonomy. On platforms, algorithms often reward content that prompts strong reactions, so manipulative messages gain greater reach and verified sources get less visibility. FIMI, however, rarely occurs as a single technique and most often manifests itself through combinations of selective presentation of facts, disinformation, coordinated amplification, manipulative narratives and abuse of influencers and pseudo-media sites. Risks increase during election cycles, security and geopolitical crises, and high-profile public interest cases, when the pressure for rapid information accelerates the spread of unverified content.

At the same time, **gaps in coordination** are noted, **i.e. insufficiently clear protocols for rapid response and information exchange** between institutions, regulators, media and civil society, and **a lack of systemic support for media and information literacy** as a long-term and preventive pillar of resilience.

Based on the analysis, the recommendations of this policy paper are aimed at measures that can be implemented in parallel, with a clear priority on transparency, institutional communication and strengthening professional and public capacities. This includes:

- enhancing the **transparency of media financing and ownership** and the public visibility of political/paid online advertising;
- establishing **protocols for rapid, accurate and consistent communication in crisis situations**, with clearly assigned roles and responsibilities, without interfering with editorial autonomy;
- continuous **training in editorial offices** on verification, digital security, editorial standards and working with open sources (OSINT), with a special focus on the local level;
- **cooperation with platform**s through transparency of moderation, access to data for research and public interest, and better visibility of credible sources, without censorship and while upholding freedom of expression;
- strengthening public resilience through **media and information literacy programs** and promoting fact-checking; and
- establishing **cross-sectoral coordination** between institutions, media organizations, civil society and the academic community to monitor trends, provide early warning and assess the effects of the measures.

Such measures will ensure strengthening the resilience of the media and digital ecosystem and will protect freedom of expression and the public interest in the face of foreign information influences.

INTRODUCTION

Foreign Information Manipulation and Interference (FIMI) represents a complex and long-term threat to democratic societies, which is increasingly manifested through media systems and public communication. Unlike classical forms of propaganda or individual cases of disinformation, FIMI encompasses coordinated and intentional activities by foreign state and non-state actors (including their proxies) aimed at reducing trust in the media, institutions and democratic processes, through the systemic misuse of traditional media and digital channels (EEAS, 2023).

Modern European approaches to FIMI, developed by the European External Action Service (EEAS), indicate that FIMI is, above all, a structural problem (EEAS, 2023). Rather than focusing solely on identifying "misinformation", these approaches analyse the infrastructure of influence, i.e. networks of official channels, state-controlled media, formally independent but de facto aligned actors, and broader ecosystems of channels that support each other and jointly create a manipulative effect on the public (EEAS, 2025).

In this context, the media are not just "victims" or "intermediaries" of foreign influence, but part of the system in which FIMI operations can be embedded, reproduced or contested. The economic vulnerability of the media market, the lack of transparency of ownership structures and financial revenues, the dependence on online platforms and algorithm-driven content distribution create an environment in which manipulative influences can occur even without the direct or conscious cooperation of media actors. These structural weaknesses are also consistently noted in assessments of the sustainability of the media sector in North Macedonia, where financial constraints and insufficient resources are associated with reduced quality of information and greater vulnerability to pressures (IREX, 2024). Hence, FIMI poses a challenge not only for journalism, but also for media regulation, self-regulation and institutional coordination.

The Republic of North Macedonia, as a NATO member state and candidate for membership in the European Union, faces such risks in the context of additional structural weaknesses. Political polarization, limited trust in institutions, economic pressures on the media, and relatively low levels of media and digital literacy increase the exposure of the media ecosystem to foreign manipulative influences, especially in periods of political sensitivity, elections, or crises and they impede systemic responses (AJM, 2024). The European Commission's 2025 Report notes that media legislation is not yet fully aligned with the acquis, including new European legislation, such as the European Media Freedom Act (EMFA) (European Commission, 2024). Furthermore, the same report states that challenges remain around transparency of ownership and that the framework for state advertising poses risks of abuse and market disruption.

At the same time, the response to FIMI must not be based on restrictive measures or ad hoc content restrictions, as this poses a serious risk to freedom of expression and media pluralism. European regulatory instruments, in particular the Digital Services Act (DSA) (European Union, 2022) and the Media Freedom Act (EMFA) emphasize the need for systemic risk management, greater transparency, responsibility and accountability, but without interfering with editorial autonomy and legitimate public discourse.

In this sense, **this policy paper aims to contribute to the development of a media-oriented and regulatory-aligned approach to FIMI in North Macedonia. The focus is on the role of the media ecosystem and relevant stakeholders, as well as**

the regulatory and institutional frameworks that shape their operations, in order to identify key gaps and offer applicable policy options. The ultimate goal is to strengthen media resilience and improve coordination between media, regulators, institutions and civil society, in line with European standards and principles of freedom of expression and the public interest.

This paper is prepared as a policy analysis, with the aim of contributing to a better understanding of FIMI as a systemic risk and to identifying realistic policy options to strengthen the resilience of the media and the digital ecosystem. It is part of the ongoing research and analytical work on Foreign Information Manipulation and Interference by the Institute of Communication Studies (ICS). It builds on the initial analysis of how FIMI manifests itself in the Republic of North Macedonia (Hadzi-Janev and Stoilkovski, 2025), continues the regulatory perspective and European context developed in the policy paper (Bleyer -Simon, 2025) and takes into account the findings and options for institutional response to FIMI in the country (Grizev and Poposka, 2025). In that sense, the document retains the already established definitions and analytical approach and develops them further with a focus on the media ecosystem: its structural vulnerabilities, the channels and mechanisms through which those vulnerabilities can be exploited, as well as measures that are proportionate, transparent and consistent with the protection of freedom of expression and media pluralism.

The approach is aligned with European frameworks that analyse the phenomenon through patterns of behaviour, networks and channels, rather than through isolated content. The paper does not assign responsibility for specific operations or "prescribe" operations to specific actors, nor does it aim to produce lists or "label" domestic media outlets, organizations or individuals. Instead, it focuses on structural vulnerabilities, institutional and regulatory gaps and ways to overcome them through measures that are proportionate and defensible from a human rights perspective. The guiding principles are: protecting freedom of expression and media pluralism; a risk-based approach with an emphasis on transparency and accountability; supporting quality journalism and self-regulation as a basis for public trust; and building societal resilience through media and information literacy and improved coordination among relevant stakeholders.

The paper begins with an introduction and methodological clarification of FIMI and the analytical matrix, then sets the problem in a national context and presents the exposure matrix as a tool for mapping channels and effects. This is followed by an overview of the European regulatory and strategic context, and then an analysis of perceptions and needs in the country and the relevant normative and institutional segments. The matrix is then applied to the Macedonian context to identify recurring scenarios and vulnerabilities, after which existing mechanisms and critical gaps are reviewed. The paper finishes with conclusions and proposed policy measures aimed at institutions, the media sector, civil society organizations and online platforms, in the spirit of proportionality, transparency and protection of freedom of expression.

Methodology

This document has been prepared as a policy analysis based on desk research and analytical synthesis of relevant European and national sources, in order to describe how FIMI manifests itself as a systemic risk in the media and digital ecosystem and to propose measures that strengthen resilience, without limiting freedom of expression and media pluralism.

The methodology relies on:

(a) (a) the European conceptual and analytical frameworks for FIMI of the European Media Freedom Act, including the FIMI Exposure Matrix (EEAS, 2025) as an approach to mapping channels and behavioural patterns,

(b) European regulatory instruments that set obligations for systemic risk management, transparency and protection of media freedom (Digital Services Act (DSA), Media Freedom Act (EMFA), political advertising regulation, Artificial Intelligence Act (AI Act) and related (co)regulatory mechanisms),

(c) relevant national legal and strategic documents on the media, the digital environment and security, and

(d) local and regional analyses of the media system, trust, information risks and the safety of journalists.

The selection of sources was guided by criteria of relevance to the purposes of the paper, institutional and expert authority (the EU and the Council of Europe take precedence), verifiability and applicability in Macedonian conditions.

The time frame of the review is November - December 2025. The paper does not use new field data (interviews, surveys or focus groups) and does not establish origin/responsibility for specific operations or actors. Due to the dynamics of the phenomenon, the analysis deliberately focuses on structural vulnerabilities, institutional capacities and sustainable policies, rather than on individual cases.

1.

Context and problem: FIMI as a challenge to media integrity and democratic processes

The European External Action Service (EEAS) defines FIMI as a "mostly non-illegal pattern of behaviour that 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 (EEAS, 2023). FIMI is not limited to classic propaganda or isolated cases of disinformation. It is an intentional and coordinated action in which different communication channels – from media and intermediary networks to anonymous social media profiles, influencers and synchronized web pages – reinforce each other to create a distorted image of events, institutions and international partners (EEAS, 2025). The key objective is often to reduce trust, weaken democratic processes, and not to "persuade" the audience about a single thesis (EEAS, 2023).

The consequences are twofold - concerning security and democracy. From a security perspective, foreign information influences can influence public perceptions and political decisions related to foreign policy, defence, or key geopolitical orientations of the state. From a democratic perspective, they disrupt informed participation of citizens in elections and public debates, fostering polarization, cynicism, and apathy (European Commission, 2024).

In North Macedonia, such risks are compounded by existing weaknesses in the media ecosystem and institutional trust. The European Commission, in its reports on candidate countries, notes limited progress on freedom of expression and points to unresolved issues, such as transparency of ownership and potential risks related to state advertising (European Commission, 2025). These conditions create space for external narratives to be more easily "localized" through local proxies, thematic communities, or targeting vulnerable groups.

In addition, digital transformation and the reliance on major online platforms means that much of public communication takes place in algorithmically driven and often non-transparent environments, which reduces the visibility of coordinated manipulative activities and hinders timely risk identification (EEAS, 2025). In this regard, the Digital Services Act (DSA) provides obligations, in particular for very large platforms, to assess and mitigate systemic risks related to fundamental rights, public debate and democratic processes (European Commission, 2025).

Hence, FIMI is a risk not only for foreign and security policy, but also for the fundamental values of the democratic order: pluralism, informed participation, accountability of institutions and free and independent media. Policies are needed that recognize the systemic nature of the threat, strengthen the media and journalists as guardians of public interest, and provide measures that are proportionate, transparent and in line with European standards on freedom of expression.

For the purposes of this document, FIMI refers to situations in which, cumulatively or predominantly, several interrelated elements are recognized.

- First, there is a foreign connection or interest, whereby activities are initiated, directed or carried out in the interest of foreign state or non-state actors [1], often through local proxies and intermediary structures (EEAS, 2023).
- Second, FIMI are characterized by intention in their actions and coordination, i.e. planned and coordinated action across multiple channels and formats, including networks of social media profiles and pages, online portals and media outlets, influencers, groups and paid communication tools (EEAS, 2024).
- Third, manipulative communication techniques are applied within the framework of FIMI, such as deception, source concealment, misrepresentation, selective framing, or the imposition of narratives through seemingly legitimate sources and platforms (Council of Europe, 2021).
- FIMI have a clear objective of influencing the public sphere, including electoral processes, public policies, trust in institutions and the media, social cohesion and international orientations, with a cumulative effect on democratic processes (EEAS, 2023).

In this approach, malinformation is an important, albeit not the only, element. Manipulative influence can also be achieved through accurate information presented in a manipulative context, if it is reinforced in a coordinated manner and with a clear goal of exerting influence (Council of Europe, 2021). It is crucial to keep in mind that much of the content that can be considered harmful (including disinformation) is often lawful communication, and as such is generally protected by freedom of expression and should be treated differently from unlawful content (Bleyer-Simon, 2025). The specificity of FIMI lies in the intention, coordination and potential harmful impact of organized activities. A manipulative effect can also be achieved with accurate information, if it is presented in a manipulative context and reinforced in a coordinated manner across multiple channels.

In practical terms, FIMI is most often recognized when several indicators coincide: there is a foreign interest; the action is coordinated through multiple channels; manipulative techniques are used (e.g., false contextualization, source concealment, imitation of credible media, abuse of mechanisms to amplify reach); and there is a clear goal of influencing the public sphere in another country.

For the purposes of analysis, it is useful to distinguish four basic forms:

(a) (a) long-term campaigns that gradually become normalized;

(b) operations around a specific event (elections, crises, protests) with the rapid imposition of an interpretation;

(c) operations targeting groups (ethnic/identity, youth, diaspora) with the aim of deepening divisions; and

[1] Non-state actors are powerful individuals or groups, such as non-governmental organizations, corporations, or armed groups that influence global or national processes, but are not part of formal state authority. They act independently and influence political, economic, and social processes at the national and global levels.

(d) hybrid operations that combine information manipulation with other instruments such as cyber activities or diplomatic pressure), with FIMI functioning as an integral part of a broader hybrid strategy (NATO, 2024).

This framework in the paper sheds light on how threats emerge in the media space and helps shape policies that reduce their impact, without jeopardizing freedom of expression, media pluralism, and the democratic character of public debate.

1.1. FIMI Exposure Matrix: A Framework for Mapping Channels

The European External Action Service's third report on FIMI threats introduces an analytical tool - the FIMI Exposure Matrix, for classifying information channels according to the degree and nature of their connection to foreign threat actors and networks of influence. The value of the Matrix is that it exposes the "architecture" of FIMI operations: in addition to the visible layer (official and publicly connected channels), it also maps the hidden infrastructure that allows infiltration into local audiences and amplification of manipulative narratives through networks of channels (EuvsDisinfo, 2025).

The matrix covers four categories of channels:

1. **Official state channels (Category 1)** - official profiles and websites of state institutions, ministries, embassies and other formal channels of state communication.
2. **State-controlled outlets (Category 2)** - media outlets that formally have their own legal entity, but are financed, managed or editorially controlled by the state.
3. **State-linked channels (Category 3)** - formally independent channels/media/profiles with structural ties to the state or state-linked actors (ownership, funding, coordination, recurring propaganda patterns).
4. **State-aligned channels (Category 4)** - sources that cannot formally be attributed to a state actor, but show systematic alignment and similar behavioural characteristics, thereby playing a significant role in FIMI activities.

Each category is recognized through a combination of technical and behavioural indicators, such as publicly declared affiliation or self-presentation, financial traces and sources of funding, shared infrastructure, as well as amplification practices (posting identical content, automated translations, mass reposting, coordinated messages, inauthentic profiles, and the like).

In this paper, we use the FIMI Exposure Matrix as a framework for mapping the channels and mechanisms through which information exerts influence. The goal is not to "hunt" for individual contentious posts, but to understand how manipulative influ-

ence is created and amplified, i.e. which channels produce it, which transmit it, how it "spills over" between platforms and media, and where it gains local visibility and legitimacy. This approach is particularly useful because FIMI almost never operates as an isolated incident, but rather builds a gradual effect through different channels, proxies, and formats.

Practically, the Matrix in this paper serves four purposes:

- First, to examine the types of channels relevant to FIMI risks in North Macedonia;
- Second, to compare that "channel map" with existing rules and mechanisms (laws, regulatory and self-regulatory instruments) and to identify systemic "blind spots";
- Third, to assess whether institutions and the sector have a clear division of roles and coordination, especially for channels where the impact is indirect; and
- Fourth, to formulate measures that are precise and proportionate: higher standards of transparency and accountability where justified, and preventive and long-term tools where the risk is indirect (media literacy, support for independent media, professional standards). Criteria that apply for all cases are compliance with European standards and a balance with freedom of expression and media pluralism.

It is important to highlight that the application of the Matrix here does not mean "labelling" specific domestic media outlets. It is used to better understand the risk points in the system and to develop recommendations that strengthen resilience without punitive logic and without restricting legitimate public debate.

2.

European regulatory and strategic context for fimi in the media and digital ecosystem

The European External Action Service (EEAS) defines FIMI as a mostly non-illegal pattern of behaviour, which can nevertheless have significant negative effects on values, democratic procedures and political processes. The focus is on the existence of clear intent, coordination, the manipulative nature and the use of proxies and networks, and not just the accuracy/inaccuracy of individual claims.

This logic is backed-up with empirical evidence: EEAS's second report is based on 750 investigated FIMI incidents between 1 December 2022 and 30 November 2023, confirming the need for analytics that recognise "patterns" and repetitive behaviours, rather than isolated incidents (EEAS, 2024). In parallel, the EEAS has institutionalised the framework through the development of a FIMI Toolbox and structures for systematic detection and exposure of operations, including the FIMI Information Sharing and Analysis Centre (FIMI-ISAC) as a mechanism for improved information exchange and shared situational awareness in line with the broader logic of European "network defence".

EEAS's third report goes a step further, focusing on digital infrastructure (channels, domains, networks of pages/profiles, distribution methods) and presents the FIMI Exposure Matrix as a tool for mapping the architecture and indicators of operations (EEAS, 2025). This is particularly important for this policy paper as it shifts the debate from the question of "which story is false" to the question of "which channels and mechanisms create a cumulative effect on the public sphere and where are the systemic vulnerabilities".

2.1. Regulatory instruments: platform accountability, transparency and protection of media pluralism

The European Union is building its regulatory framework on the premise that the online space must not remain a space without accountability when it comes to systemic risks to public debate and democratic processes. In this regard, risk management and transparency are being strengthened, through a combination of regulatory and co-regulatory mechanisms.

A practical example of this logic is the transformation of the Code of Practice on Disinformation into a Code of Conduct under the Digital Services Act (DSA), with the European Commission and the European Board for Digital Services approving the integration (February 2025) as a benchmark for demonstrating risk reduction and transparency measures (European Commission, 2025).

In parallel, the new European regulatory package links the topic to media pluralism and independence and to the economy of political influence (transparency of political advertising and limitation of risky targeting/amplification practices). These instruments are relevant for FIMI because they are not limited to "harmful content", but address the infrastructure of influence, i.e. who pays, how is targeting done, how is reach amplified and what transparent traces must exist (IviR, 2025).

Finally, the EU AI Act (European Union, 2024) introduces standards that become directly relevant to FIMI due to the increasing use of synthetic content, automated targeting and scalable manipulation techniques. In doing so, the European framework expands the policy from classic "information hygiene" to the management of technological risks affecting the public sphere.

2.2. The Council of Europe and the security perspective: human rights, design and resilience

In addition to the EU, the Council of Europe is developing the topic from the perspective of human rights and democratic culture. The direction of the Steering Committee on Media and Information Society (CDMSI) and the Committee of Experts on the Integrity of Online Information (MSI-INF) explicitly structures the fight against online (dis)information around three pillars: (1) fact-checking, (2) platform design solutions, and (3) user empowerment, with a clear orientation towards a human rights - compliant approach, i.e. measures that focus on ranking/distribution processes and information requirements, rather than arbitrary "content judgment" (Council of Europe, 2023).

From a security perspective, the topic is linked to hybrid risks and cyberspace. The EU Agency for Cybersecurity (ENISA) makes threat and trend assessments, including an intersection of cyber risks and FIMI in hybrid scenarios (ENISA, 2022). In this context, the Agency points out that a common situational awareness and coordinated response between institutions, platforms and society is needed, as information manipulation is increasingly linked to technological infrastructure, automation and misuse of digital services.

In this paper, the European context serves as a reference framework for: (a) a clear distinction between legitimate public debate and coordinated manipulation; (b) building proportionate measures that protect freedom of expression; and (c) setting up a system of responsibilities – institutional, media and platform – with a focus on prevention, transparency and resilience, rather than ad hoc reactions.

2.3. Implications for North Macedonia: obligations and opportunities in the context of EU integration

Although North Macedonia is not yet a member of the EU, as a candidate country it has a clear direction of gradual alignment with the acquis and with European standards governing the media sphere and the digital public. In the context of the FIMI, this means that, when preparing or amending relevant laws and policies, European ap-

proaches should be taken into account that treat the problem as a systemic risk, and not as a matter of "contentious content" (EEAS, 2023).

Practically, this opens up three priorities:

1. alignment with the principles of the European framework for platform liability, transparency and risk management, including by adopting good practices from co-regulatory mechanisms (such as the Code of Conduct on Disinformation);
2. embedding the FIMI logic (indicators, techniques, network practices) into national strategies and action plans, to avoid a fragmented and exclusively reactive response;
3. stimulating coordination among institutions, regulators, the media sector and civil society, as FIMI is a network phenomenon that by definition requires a multi-sectoral approach.

From a policy perspective, it is essential to avoid two extremes: ignoring risks (leaving the media space without a systemic response) and disproportionate measures that may restrict freedom of expression or open up space for political abuse. The European frameworks and standards of the Council of Europe offer a practical reference line for policies that simultaneously protect the public interest, security and media freedom.

3.

Perceptions and needs related to FIMI in the media ecosystem in a national context

In North Macedonia, Foreign Information Manipulation and Interference is not regulated as a separate policy area. Instead, relevant aspects are incorporated indirectly into multiple laws, strategies, and institutional mandates that regulate the media system, electoral processes, the digital environment, and national security. This dispersed normative approach allows for partial addressing of individual symptoms, but not systemic risk management.

Resilience to FIMI depends not only on formal strategies and legal frameworks, but also on the real conditions in which newsrooms and the journalistic profession operate. Analyses of media freedoms and the safety of journalists indicate that structural pressures on newsrooms - physical and online attacks, legal threats and insufficiently effective institutional protection - create a "chilling effect" on journalists' work and reduce the capacity for investigation, verification and critical reporting (AJM, 2025). This effect directly reduces the capacity for research, verification and critical reporting, especially in conditions of complex and coordinated information influences.

Additionally, analyses of the media market and trust in the media show that the small media market, low levels of trust, politically motivated channels and sources with foreign influence complicate the public space and facilitate the normalization of manipulative content (MIM, 2023). The audience rarely makes a clear distinction between these sources, which makes manipulative content easier to normalize, and foreign information interference more difficult to recognize as a systemic problem (SEENPM, 2024).

Hence, from the perspective of the media community, public policies are needed that are not limited to restrictive measures or measures focused solely on security, but they should at the same time strengthen the role of trade union organizations, the safety of journalists, the economic and editorial independence of the media, self-regulation and ethical standards, as well as capacities for investigative journalism. It is these elements that determine the boundary between resilience and vulnerability of the media space and represent a necessary starting point for developing effective, proportionate and media-sensitive policies for dealing with FIMI, elaborated subsequently herein.

In 2025, the Institute of Communication Studies (ICS), through a series of public interviews and analyses of its online media outlets Res Publica and Samo Prasaj, provided additional insights into how the media and expert community recognizes the risks and gaps related to FIMI - from institutional responses and electoral vulnerabilities, to cyber capacities and the role of new online actors.

The following points summarize the most frequently repeated observations from these consultations and public debates. They are presented here as a diagnosis of systemic gaps, and are elaborated below, through the analysis of frameworks, mechanisms and measures.

- **Coordination and a clear mechanism for response are lacking.** The practical problem is not only "which law is relevant", but also that there is no clearly systematized approach and institutional mechanism for a rapid and coordinated response to FIMI, which leaves the state vulnerable to hybrid threats and manipulative narratives (ICS, 2025). This points to the need for a clear allocation

of roles, protocols for information exchange and proportionate measures that will protect freedom of expression, while still allowing for an effective response when there is coordinated and intentional harmful influence.

- **There are vulnerabilities in the regulation and financing of online media in electoral processes.** The risks most clearly surface in electoral cycles, especially around paid political advertising and the status/treatment of online media. In the public debate, it was pointed out that online media registered outside the country also appear in electoral registers, which opens up space for abuse and potential influences. In such a context, the discussion most often boils down to the need for more precise and sustained changes in electoral regulations, both in terms of the conditions for participation and in terms of the transparency of financing and advertising (SamoPrasaj, 2025).
- **Cyber Security and capacities are a "bottleneck" for resilience.** In the domain of digital security, institutional capacities remain one of the most critical vulnerabilities. The National Computer Incident Response Centre (MKD-CIRT) provides technical support and coordination for over 150 institutions, but has limited human resources (six people). This further highlights the need for structural strengthening, for example, by establishing a national contact point/"SOS" line and 24/7 monitoring, as well as a stronger connection between security measures and public communication policies (ResPublica, 2025).
- **There are influences through social media and proxies.** In the broader institutional context, foreign influences and manipulations are most often associated with the Internet and social media as key channels for putting pressure, discrediting or indirectly influencing internal processes. This highlights the need for systematic analysis and a coordinated response, but without resorting to excessive restrictions on speech (ResPublica, 2025).
- **FIMI often functions as a "foreign policy instrument".** Case studies show that FIMI rarely operates in isolation; it is most often "attached" to existing social and political tensions. Analyses of Russian interference, for example, suggest that vulnerabilities such as bilateral disputes and low trust in institutions can be used to reinforce certain narratives and create destabilizing effects. This is important because it suggests that the response should not be fragmented, but rather existing policies and mechanisms should be linked into a more coherent system of resilience (ICS, 2025).

In summary, the views indicate that the FIMI is recognized across multiple policies and institutions, but that a common framework that would ensure a timely, coordinated and proportionate response is lacking. Therefore, it is necessary to link existing measures into a more consistent approach, with clear competencies, a minimum set of common protocols and stable capacities, without violating freedom of expression.

3.1. Media and electoral legislation: normative basis, without an integrated approach for FIMI

The basic regulatory framework governing the media space and election reporting in North Macedonia - the Law on Audio and Audiovisual Media Services, the Law on Media and the Electoral Code - is built around key democratic principles such as media pluralism, professional and ethical standards, protection against hate speech and ensuring fair and equal media coverage during elections. These laws represent an important normative basis for the quality of public debate and electoral integrity, but their analytical and regulatory focus remains limited to traditional media roles and individual content.

None of the above laws explicitly recognize Foreign Information Manipulation and Interference as a coordinated, intentional, and often transnational risk, nor do they provide mechanisms for analysing networks of influence, intermediary channels, or synchronized manipulative behaviour that takes place through a combination of media, online platforms, and informal communication actors. The regulatory approach remains predominantly reactive and content-oriented, which makes it difficult to identify systemic patterns of influence early on.

In the electoral context, the Electoral Code (State Election Commission, 2024) establishes detailed rules for media coverage, political advertising and equal access of electoral participants to the media, as well as the competences of regulatory bodies to monitor compliance with these rules. However, the focus is primarily on the formal legality, equality and transparency of the electoral campaign, and not on detecting and addressing coordinated external information influences that act indirectly, through the online ecosystem, social media and so-called "grey" media channels.

As a result, **the existing media and election regulation provides basic guarantees for fair competition and professional reporting, but is not conceptually and instrumentally adapted to deal with FIMI as a systemic phenomenon that operates through networks, proxies and digital infrastructure. This gap limits the ability of institutions and regulators to timely recognize and address manipulative influences that do not formally violate the rules, but have a cumulative effect on the public sphere and trust in democratic processes.**

3.2. Digital regulation and the online environment: limited regulatory scope beyond traditional media

The digital and online environment in North Macedonia is still regulated in a fragmented manner, through general laws that are not primarily aimed at the media sphere and information risks. The Law on Electronic Communications, the Law on

Personal Data Protection and the Law on Cybersecurity establish basic rules for the functioning of the digital infrastructure, the protection of privacy and the security of networks, but do not treat foreign manipulation and interference with information as a specific democratic and media risk.

In this normative context, online platforms, social media, influencer channels and digital portals that are not registered as media within the meaning of the Law on Media remain outside of systematic regulatory and analytical oversight. Although these actors have a significant influence on public opinion and electoral processes, the existing regulation does not provide for obligations for transparency of editorial structures, financing or coordinated behaviour in the online environment. This creates a space in which manipulative activities can take place in a "grey zone", formally legal, but potentially harmful to the public interest.

From a cybersecurity perspective, the National Cybersecurity Strategy (Ministry of Digital Transformation, 2025) and the relevant legal framework recognize the possibility of hybrid threats, but predominantly treat them through a technical and infrastructure prism (system protection, incidents, networks), without a clear connection to information operations, media channels and public communication. In the absence of such a connection, FIMI remains an indirectly mentioned phenomenon, without operationalized indicators and without a clearly defined institutional competence for monitoring the information influence in the online space.

Compared to European regulatory trends, this approach creates a gap. The Digital Services Regulation introduces obligations to assess and manage systemic risks related to elections, public debate and media pluralism, especially for very large online platforms. The absence of national mechanisms that follow this logic limits the state's ability to timely recognize and address coordinated informational influences that unfold through digital ecosystems.

As a result, **digital regulation in North Macedonia provides basic protection of infrastructure and personal data, but does not offer sufficient tools for a systematic understanding and management of the risks of FIMI online. This gap is particularly relevant during election and crisis periods, when manipulative campaigns are most often activated through a combination of platforms, informal channels and proxy networks, beyond the reach of traditional media regulation.**

3.3. National Security and Hybrid Threats: Risk Recognition Without Media Operationalization

In the national security and strategic framework of North Macedonia, foreign influence and hybrid threats are recognized as relevant risks to the stability of the state and democratic institutions. The National Security Strategy (Ministry of Digital Transformation, 2024-2029), the National Cyber Security Strategy (Ministry of Digital Transformation 2025-2028), as well as the Law on Security of Network and Infor-

mation Systems (Parliament of RNM, 2023) point to the existence of complex and combined threats that can endanger institutional resilience and public trust, including through the misuse of news and information channels.

However, despite this formal recognition, the approach to these risks remains predominantly security and infrastructure-oriented. Hybrid threats are treated primarily through the prism of protecting critical infrastructure, state systems and institutions, while the media sphere, public communication and digital platforms are covered indirectly and without clear operationalization. There is no normative or strategic framework that systematically connects security assessments with the dynamics of media reporting, the online ecosystem and the communication networks through which information influence takes place.

As a result, FIMI is not defined as a specific media and democratic risk with precisely defined indicators, institutional roles and monitoring mechanisms. There are no publicly available established procedures for coordination and information exchange among security institutions, media regulators and other relevant actors, as well as early-warning mechanisms and analysis of coordinated information campaigns operating below the threshold of classic security incidents, as also elaborated in the European framework for FIMI (EEAS, 2022). In this context, the cyber dimension emerges as part of a broader security understanding of hybrid threats, while the specific legal and operational aspects of cybersecurity are discussed below.

In this institutional context, **the media are left without clear guidance, support or protective mechanisms to deal with complex forms of foreign information influence, while the security sector has limited analytical insight into the media and digital processes through which these influences manifest. This gap between strategic recognition of the threat and its practical management in the media and public spheres limits overall institutional resilience and reduces the state's ability to respond in a timely and proportionate manner to FIMI as a complex, cross-sectoral phenomenon.**

3.4. Cybersecurity and legislation: a strong foundation for incident management, but not a substitute for a FIMI approach

With the adoption of the new Law on the Security of Network and Information Systems, applicable from January 2026, the management of cyber risks and institutional coordination are strengthened, in line with Directive (EU) 2022/2555 (NIS2). The Law establishes clear rules for the protection of network and information systems and is important for national digital resilience. Under this Law, the National Computer Incident Response Center (MKD-CIRT) is designated as the competent authority for all important and essential entities in the country, as well as for entities without sectoral computer security incident response teams.

However, despite its relevance to broader hybrid scenarios in which cyber incidents and information influence can be intertwined, the law is not designed to reg-

ulate Foreign Information Manipulation and Interference as a media and democratic issue. Its focus remains on incidents, technical risks and institutional responses, without covering aspects related to editorial practices, transparency of information channels or analysis of narratives and networks of influence. Cyber legislation therefore constitutes an important "layer of defence", but does not replace the need for a separate and integrated approach to FIMI that links media policies, professional standards and public communication.

Following that same direction, the Cyber Security Strategy 2025-2028 (Government of RNM, 2025) develops the national vision for a secure digital transformation and recognizes that modern risks overlap with hybrid threats and information impacts. Additionally, the Cyber Defense Strategy (Ministry of Defence, 2021) treats the cyber dimension in a security-defense context. Despite this, **the national "package" still lacks a document/mechanism that would clearly position FIMI as a separate subject of action in the media ecosystem with precisely defined roles, protocols, response thresholds, protective measures and guarantees for freedom of expression.**

3.5. Education and media literacy: prevention and long-term resilience

Foreign Information Manipulation and Interference do not rely solely on normative gaps or institutional weaknesses, but also on limited capacities in society to recognize and critically assess manipulative techniques, coordinated campaigns, false contextualization and abuse of digital amplification mechanisms. Hence, education and media literacy represent a key preventive layer in national resilience. They are not aimed at "pursuing content", but at strengthening the ability of citizens to make informed assessments and participate in public debate with less vulnerability to manipulative influences.

In this context, the Framework for Media Literacy in Primary Education (2023) (Bureau for the Development of Education, 2023) represents an important step towards the systematic incorporation of media literacy into formal education. The document sets out media literacy as a system of competencies that are developed across different subjects and age levels, with a particular emphasis on critical thinking, understanding media messages, recognizing manipulative techniques and responsible content creation and sharing. The fact that the Framework was developed through cooperation between institutional and professional stakeholders - the Bureau for the Development of Education, IREX and the Macedonian Institute for Media, increases its practical applicability, but at the same time emphasizes the need for continuous support in its implementation, especially through teacher training, development of teaching materials and systematic monitoring of its implementation.

In addition to primary and secondary education, it is important to treat media literacy as a continuum that continues in higher education, especially since it is there that future teachers, journalists, communicators and public servants are formed. In this regard, within the framework of initiatives and partnerships for media literacy, ICS has contributed to

opening up the topic in higher education and to practical steps for its institutionalization, including by introducing media literacy courses/modules at eight faculties from six universities (ICS, 2024).

An additional value for an "ecosystem" approach is the Media Literacy Network [2], established to facilitate communication and consultation among different actors working to improve media literacy. In the logic of this paper, such platforms are important because they create space for harmonization of approaches and standards among institutions, regulators, media, academia and civil society, a condition that is essential for long-term resilience to FIMI as a network phenomenon, and not as a series of isolated incidents. As a practical support for the standardization of terminology and easier application in teaching and public policies, the Media Literacy Dictionary is also available - an online platform with terms and explanations in Macedonian and Albanian[3]. Such tools are important because they reduce terminological inconsistencies between stakeholders and facilitate the development of materials, training and public interventions that are mutually compatible.

As a final point, this field is also relevant because independent assessments indicate **the need for an accelerated strengthening of media literacy in response to vulnerability to disinformation and manipulative influences** (YouthWiki, European Commission/EACEA, 2025). Therefore, **the existing educational and coordination steps should be read as a foundation that already exists in national policies and as a part that can be strengthened and linked to other institutional and regulatory measures** in the following chapters.

3.6. Synthesis: what is missing in the system and why it matters

Despite the visible progress in adopting strategies and new legal solutions in the domain of cyber security and hybrid threats, FIMI in national frameworks most often appears as an implicit category, dispensed through multiple documents, institutional competencies and sectoral policies, without a unified and clearly articulated position that treats foreign information interference as a specific security and democratic challenge for the media system. Domestic analyses (ResPublica, 2025) indicate that the institutional response is often activated reactively, especially in sensitive periods (such as elections or regional crises), coordination and information exchange are not sufficiently continuous and visible, and stronger capacities for monitoring and analysis are needed, as well as formalized partnerships with the academic community and the civil society sector, complemented by systemic programs for media and digital literacy in the public sector.

[2] Media Literacy Network (2023) "About Us / What is the Media Literacy Network?". Online platform.
[3] Media Literacy Glossary "About the Glossary", https://recnik.medium.edu.mk/za-recnikot/

Existing analyses (MIM, 2021) show that, although hate speech is addressed through multiple legal and institutional mechanisms, disinformation - as in most democratic countries - most often remains within the domain of self-regulation and fact-checking, which reinforces the need for a coordinated, strategic and proportionate approach rather than ad hoc interventions.

In parallel, there are significant positive foundations for long-term resilience (particularly through media literacy and network initiatives), but these will only have the greatest impact if coupled with clearer institutional roles, protocols and mechanisms for continuous monitoring and early warning. In this regard, the following sections of the paper identify key gaps and develop policy options that strengthen resilience to FIMI, while fully respecting standards of freedom of expression, media pluralism and editorial autonomy.

4.

Application of the FIMI exposure matrix in the context of North Macedonia

4.1. How and why do we use the Matrix?

After reviewing the European frameworks and domestic policies, the next step is to set an operational logic, i.e. how to talk about FIMI in a way that is precise enough for public policies, but without the risk of arbitrary assessments, stigmatization or limiting legitimate public discourse. Here we use the FIMI Exposure Matrix as an analytical framework for mapping channels and roles in information influence, not for evaluating individual posts, but for understanding the architecture through which manipulative narratives are created, legitimized, amplified, and localized.

In the Third Report of the European External Action Service (EEAS) on the Threats of FIMI (EEAS, 2025), the Matrix is part of the methodology that makes the infrastructure of operations visible. FIMI is treated as an ecosystem in which different channels, proxies and practices can be activated in synchrony and reinforce each other, with a cumulative effect on the public. This is crucial for a policy paper, i.e. the debate shifts from "whether a statement/post is accurate/inaccurate" to "which mechanisms create systemic risk and which measures are justified".

In a national context, the reason for using such a framework is both practical and protective at the same time. It ensures proportionality – it is not the same when there is misrepresentation as an institution through a fake or cloned profile, when there is uncritical downloading and mass reposting of content, and when there is coordinated repackaging and legitimization of narratives through networks of proxies in order to give them the appearance of credibility and a wider reach (EUvsDisinfo, 2025). Therefore, in this document the Matrix is read as a mapping and orientation tool (policy mapping), and not as a mechanism for formally labelling specific domestic media outlets. The goal is to identify:

(a) which types of channels are used most often;
(b) where the most realistic early warning "spots" are; and
(c) which measures are most effective without violating freedom of expression and media pluralism.

According to that logic, **the four categories of the Matrix are understood as follows:**

Category 1 - Official state channels. This includes official websites and profiles of state institutions (including diplomatic missions often presented as official pages of foreign embassies on social media). The risk is not in the "content" per se, but in the fact that these channels often function as a reference point for the public, and therefore are a target for imitation, misrepresentation and manipulated "statements". Therefore, the measures are mostly institutional and preventive, i.e. clear verification and visual identification of official channels, crisis communication protocols and rapid correction/rebuttal when a false "official" source appears.

Category 2 - State-controlled outlets. In European analyses, this category is a typical instrument in authoritarian contexts, but for North Macedonia The most relevant point is preventive. This means that domestic media (including the public service broadcaster and media outlets that receive significant amounts of public funds) must have real guarantees of editorial independence and clear professional standards that prevent the uncritical transmission and amplification of external manipulative narratives, especially in crisis and election periods. (This is not a "classification" of domestic entities, but a rule of resilience. The public interest requires a higher threshold of transparency, scrutiny and editorial autonomy when the role of the outlet is systemically important).

Category 3 - State-linked channels and the "grey zone". This is the space where risk is often created through non-transparent ownership and financing structures, dependence on public funds, proxy networks and repetitive patterns of coordinated reinforcement. Here, measures are mostly in the domain of transparency and accountability: publicly visible ownership and financing, clearer rules for the allocation of public funds and monitoring that focuses on behavioural practices and networks, rather than isolated contributions, because it is precisely repetitiveness and coordination that are the key signals of systemic influence.

Category 4 - State-aligned channels. This includes web portals, pages, profiles and influencer systems that do not have a formal institutional connection with a foreign state actor or, alternatively, this cannot be proven, but show persistent alignment within certain frameworks, timing and behaviour, often activated at "critical moments". This is the most sensitive space for policies, as an incorrectly positioned response can easily produce polarization and stigmatization. Therefore, the priority instruments here are long-term and democratically defensible - media and information literacy, support for independent journalism and strengthening the professional standards of the journalistic profession.

In summary, the Matrix in this document serves as a compass for public policies, i.e. to show where the risky "entry points" and "bridges" in the ecosystem are and to help ensure that measures are precise, proportionate and in line with European standards, without punitive logic and without limiting legitimate public debate (EEAS, 2025).

4.2. Practical implications: recurring scenarios relevant to North Macedonia

In the context of public policies, the scenarios below do not serve to list specific cases or actors, but rather to explain the practical logic of exposure to FIMI. They indicate where pressure on the public is most often generated, which narratives are relatively "easy to activate," and which combinations of channels and proxies have the greatest potential to produce a systemic effect.

During election periods, a recurring risk is delegitimization of the process through claims of "rigged elections," attacks on the credibility of the election administration, and cultivation of apathy or radicalization. International IDEA's analysis of election-related FIMI in North Macedonia suggests that foreign and proxy influences often "build on" existing vulnerabilities (polarization, distrust, sensitive identity issues) and amplify them through coordinated strategies in an electoral context (International IDEA, 2025).

In times of geopolitical crises (wars, sanctions, regional tensions), frames that portray the West as weak or hostile, relativize the responsibility of authoritarian regimes, and activate fears and historical traumas are common. The EEAS notes that the digital infrastructure of the FIMI is often spread across multiple layers and actors, with a mix of visible and "proxy" channels. This is why national media systems can become unwitting "reproducers" if they lack context, scrutiny, and editorial discipline (EEAS, 2025).

A particularly sensitive point for North Macedonia are ethnic and identity issues, where manipulations are most often aimed at deepening mistrust between communities or creating the impression that Euro-integration means "loss of identity." Analyses indicate that such narratives rely on domestic weaknesses (declining standards, political turbulence, fragmented media space) to gain real influence, including over issues such as interethnic relations (Trojachanec, Rizaov, 2024).

Finally, there is a recurring pattern of campaigns targeting civil society and independent media through discrediting and labelling them as "foreign paid operatives/agents." The risk here is systemic. When trust in actors who fact-check, monitor power, and represent the public interest is undermined, societal resilience is diminished, and manipulative narratives are more easily normalized. Regional vulnerability assessments in the Western Balkans explicitly note this pattern as a factor that increases exposure to information manipulation (NATO StratCom Centre of Excellence, 2020).

5.

Existing mechanisms and gaps in the response of the state and the media sector

After identifying typical scenarios in which foreign interference and information manipulation are activated and applying the FIMI Exposure Matrix as a framework for mapping channels and patterns of influence (Chapters 3 and 4), the next step is to assess how well the existing mechanisms in the state and the media sector are prepared to respond to these risks. The assessment focuses in particular on aspects of prevention, early recognition and a coordinated institutional and media response.

This chapter examines the situation through the "prism" of the FIMI Exposure Matrix, but from a systemic resilience perspective: clarity of roles, existence of practical protocols, and real coordination between institutions, regulators, media organizations, civil society, and online platforms.

5.1. State mechanisms: relevant elements exist, but a unified framework is lacking

The state response to disinformation and related threats in North Macedonia has so far developed in a fragmented manner, through multiple laws and strategies that touch upon the issue, but without a single and explicit framework that treats FIMI as a specific risk to democratic processes and the media ecosystem. In a normative sense, relevant issues exist in media regulation, especially in the Law on Audio and Audiovisual Media Services and the Law on Media (Assembly of RNM, 2025), which set rules for the accountability of the media, especially traditional ones. In parallel, certain forms of speech that incite discrimination or violence are also addressed through criminal law provisions, and the electoral legislation sets rules for media coverage during the election period and restrictions on propaganda practices.

However, the key practical problem is that, in the absence of a clear FIMI policy, institutional responses often appear as ad hoc responses. These include individual rebuttals, informal coordination in crisis situations and information campaigns that are not supported by continuous monitoring, clear indicators and formalized protocols for cooperation with the media sector. This gap becomes more apparent when compared with the European approach, which insists on risk management, transparency and structured mechanisms to reduce systemic risks in the digital sphere, including through the Digital Services Directive (DSA) and its accompanying codes and guidelines.

Although strategic documents on cyber security and resilience to hybrid threats recognize disinformation and propaganda as part of the broader spectrum of risks, this recognition is still insufficiently "translated" into operational architecture. Regular trend analysis, clearly allocated responsibilities, mechanisms for sharing relevant data, and a consistent line of public communication during sensitive periods are lacking, which limits the ability to respond in a timely and proportionate manner.

5.2. Self-regulation and media practices: a strong foundation, but with limitations in the online environment

Self-regulation is one of the strengths of the media ecosystem. The Council of Media Ethics, as well as the Council of Honor of the Association of Journalists of Macedonia (AJM), provide an established mechanism for complaints and deciding on violations of professional and ethical standards, which is an important public resource when manipulative or unethical content appears. AJM has long-term activities related to the protection of journalists, advancement of the profession and promotion of ethical standards, including the Code of Journalists. The Institute of Communication Studies (ICS) and the Macedonian Institute for Media (MIM) develop media literacy programs, research and training on dealing with disinformation and hate speech. In 2025, the ICS initiated and supported activities aimed at recognizing and responding to Foreign Information Manipulation and Interference, including public events and consultations on a systemic approach (ICS, 2025).

These mechanisms contribute to the development of a culture of accountability and professional self-reflection, but their reach in the context of FIMI is limited by several structural factors.

First, **self-regulation by its nature does not encompass all actors in the digital environment**, especially anonymous channels, non-transparent portals, and networks that operate exclusively through social platforms, where manipulative narratives are often amplified and recycled.

Second, although there is a certain level of **communication between self-regulatory bodies and institutions**, this cooperation often remains **ad hoc and informal**. In situations where manipulation has a pronounced foreign or coordinated component, this creates gaps in the timely coordination of public clarifications and institutional responses, without calling into question the autonomy of self-regulatory mechanisms.

Third, **limited and unstable resources** make it difficult to systematically and continuously monitor the online ecosystem in the logic of the matrix, i.e., monitor categories, proxy roles, and recurring patterns, which is a prerequisite for early warning and timely recognition of risks.

In the same vein, **fact-checking initiatives and media literacy programs** also represent an important part of the broader "social immunity" to disinformation and manipulative influences. However, they often **operate as project-oriented activities**, with time interruptions and dependence on donor cycles, rather than as a stable and institutionally supported component of public policies. In the context of FIMI, such instability limits their ability to contribute to long-term, systemic resilience.

5.3. The role of civil society and international partners: pivotal role, yet lacking a permanent coordination platform

Civil society and international partners have a significant and recognizable role in strengthening resilience to Foreign Information Manipulation and Interference, particularly in three interrelated areas: (1) researching and documenting trends and practices of information influence, (2) building capacity in the media community and the wider public, and (3) supporting independent media and advocating for better regulatory and institutional solutions. In many cases, it is civil society organizations and research initiatives that are among the first to detect structural vulnerabilities and coordinated campaigns, before they are systematically addressed in official institutional analyses.

However, this pillar of resilience also has limitations that are directly related to the logic and dynamics of the FIMI.

First, **civil society organizations often become targets of discrediting campaigns and labelling as "foreign agents" or "paid operatives"**, which functionally fits into strategies aimed at weakening trust in the corrective mechanisms of democracy and independent sources of verification.

Second, the **dominant project logic and dependence on donor cycles** make it difficult to sustain expertise and continuity of activities, even though continuity is a key prerequisite for systematic trend monitoring, early warning, and building institutional memory.

Third, **there is a lack of a formal and stable coordination platform** that would enable regular and structured exchange of information, indicators and analyses between state institutions, regulators, media organizations, civil society and international partners, as well as agreed protocols for joint action in sensitive periods.

In the absence of such a platform, the contribution of civil society and international partners remains significant but insufficiently integrated into the broader national architecture for FIMI response. This limits the possibility of timely recognition of systemic risks and a coordinated, proportionate and democratically defensible response, further highlighting the need for clearer mechanisms for institutional cooperation, discussed in the next chapter.

5.4. Key gaps through the prism of the FIMI Exposure Matrix

When existing mechanisms are reviewed across the categories of the FIMI Exposure Matrix, gaps clearly emerge that are most critical precisely where FIMI typically receives "support," i.e. in proxy and state-aligned channels (categories 3 and 4).

First, in a national context, **transparency of ownership and financing in part of the online media market remains limited, and this is particularly pronounced in the**

election campaign in which the Election Law foresees a significant amount for paid political programming and in those media outlets of dubious origin. Although there are initiatives and public discussions to increase the visibility and accountability of online media, including through the potential role of the regulator, a systemic mechanism that would provide a consistent, verifiable and comparable picture of ownership structures and financial flows is still lacking. **This is directly relevant for state-linked channels, i.e. formally independent channels/outlets/profiles with structural links to the state (ownership, financing, coordination), where non-transparency creates space for influence without public accountability**.

Second, the state still **does not have sufficiently developed tools for the so-called "soft management" of the risks arising from state-aligned channels, i.e. sources that cannot formally relate to a state actor, but show systematic alignment and similar behavioural characteristics**. In this zone, repressive measures are often either ineffective or counterproductive. Therefore, **the focus should be on transparency, platform accountability, media literacy and strengthening quality journalism**, i.e. policies that build resilience rather than create new lines of polarization.

Third, **there is insufficient coordination and information sharing between security institutions, regulators, media organizations, and civil society** on trends, indicators, and risk narratives. This is not just an organizational issue, but a prerequisite for early warning and public communication that will prevent "gaps" where manipulation is most easily embedded.

Fourth, **European standards, including the Digital Services Act (DSA), the European Media Freedom Act (EMFA) and the Code of Practice on Disinformation**, have not yet **been systematically "translated" into domestic media laws**, then into **national policies, procedures and clear expectations towards key actors**, especially in the areas of transparency, systemic risk assessment, accountability and independent oversight.

Fifth, **capacities for continuous monitoring and research are limited**. While there are quality individual reports, there is a lack of a sustainable national system that would provide regular data on trends, patterns and channels, which is a prerequisite for evidence-based policies, not just reactive ones.

This analysis shows that North Macedonia has relevant elements (legal grounds, strategies, active self-regulation and civil society capacities), but that it lacks the "glue", i.e. a unified framework, clear roles, coordination protocols and sustainable monitoring and early warning capacities.

The following chapter, based on these gaps, proposes policy options that are proportionate, enforceable, and in line with human rights and European standards.

6.

Conclusion and proposed policy measures

6.1. Conclusion

This policy paper shows that North Macedonia is realistically exposed to FIMI risks that manifest through multiple channels and practices in the domestic media and digital environment. These risks are not limited to individual disinformation, but have a cumulative effect on trust, democratic debate and the resilience of institutions.

The paper uses the FIMI Exposure Matrix to shift the analysis from reactive "content fixing" to a systemic understanding of exposure: which channels are most vulnerable, where amplification points are repeated, and what "blind spots" exist in existing mechanisms. In a national context, this is particularly relevant due to the combination of factors that increase vulnerability – political polarization, limited financial sustainability of the media, low trust in institutions, and underdeveloped media and digital literacy.

At the national level, three weaknesses stand out that directly reduce resilience to FIMI. First, the phenomenon is rarely clearly named and operationalized as a separate risk in strategic and normative documents. Second, the institutional response is fragmented and often ad hoc, without a stable mechanism for coordination and information exchange. Third, the vulnerability of the media market and the lack of transparency in part of the online ecosystem facilitate "local legitimization" and the circulation of manipulative narratives.

At the same time, there are capacities that can serve as a basis for upgrading, namely a self-regulatory system, active civil society organizations with expertise, and growing institutional awareness of hybrid risks.

The proposed measures in this document are designed to strike a balance between two equally important goals:

(a) **protecting democratic processes and the public interest** through clearer integration of FIMI into relevant policies, improved coordination and enhanced transparency in the media sector; and

(b) **promoting freedom of expression and media pluralism** by prioritizing media literacy, self-regulation, and support for independent media, rather than broad repressive measures that may be counterproductive or open to abuse. The key message is that resilience is not built by restricting freedoms, but by strengthening the quality and trust in the public sphere.

For the recommendations to have a real impact, implementation needs to be politically accountable and institutionally sustainable, with clear roles and responsibilities, transparency and oversight, as well as an inclusive process in which media organizations, civil society and academia are true partners. Due to the rapid evolution of the digital ecosystem, continuous monitoring and periodic revision of the measures is also necessary.

6.2. Proposed policy measures

Based on the identified types and practices of threats (Chapter 4) and the identified institutional and sectoral gaps (Chapter 5), this chapter proposes measures with a common goal, which is **to increase North Macedonia's resilience to Foreign Information Manipulation and Interference without undermining democratic standards, freedom of expression, media freedoms and pluralism.** The measures are grouped by key actors and, where relevant, linked to the categories of the FIMI Exposure Matrix, as an analytical tool for proportionality – from official institutional channels, through media with a public role and potential dependence on public resources, to the broader online ecosystem.

Additionally, it is necessary the term **FIMI should be more clearly defined and incorporated into relevant policies and regulations** as a common basis for risk recognition and coordinated response. In parallel, **systematic capacity building of journalists is necessary** (training and awareness-raising for detecting coordinated campaigns, encouragement for analytical stories and networking with research centers). In support of these measures, it is important **to develop and centralize resources and tools for journalists and institutions** - a process that is already beginning in our country, but is still in its infancy (ResPublica, 2025).

State institutions and official channels

To reduce the space for manipulation, official institutional channels should function as a stable source of verifiable information, especially in periods of elections, geopolitical tensions, and security crises, i.e. moments when FIMI most easily "take root." This requires a shift from ad hoc reactions to a system of early warning and coordinated public communication.

- The approach to preventing and tackling **FIMI** should **be explicitly embedded in relevant national strategies and policies** (national security, cyber security, strategic communication and public communications), with a harmonised definition of the term and clearly defined risks, objectives and division of responsibilities. Alignment with European approaches (including the EEAS framework and methodologies for election-related manipulation) is important as a common language and comparability, but not as a mechanical "replicating" of solutions.
- **A small but functional coordination structure** (unit or interdepartmental working group) with a clear mandate to monitor trends, assess risks, agree on institutional messages and support rapid and verifiable repudiations is needed. In this regard, an inter-institutional coordination group for dealing with FIMI was initiated and established in 2025 (ICS, 2025). The structure must operate transparently, with clear limitations on its role (no "truth assessment" in public debate) and

with respect for freedom of expression, so that it is perceived as a mechanism for public interest, not a political instrument.

- The state should develop and test **standard operating procedures for information incidents** - who responds, within what timeframe, on what basis (evidence/sources), through which channels and with what rules to mitigate the situation and avoid escalation. These procedures should be accompanied by training for spokespersons and officials on language that is precise, verifiable and non-polarizing, especially when the goal of manipulation is panic and conflict.
- **Proactive transparency** is necessary, i.e. thematic briefings on areas that are often the target of manipulation (European integration, foreign policy, defence), improved access for journalists to timely official information, and expansion of open data practices. This is not a communication "luxury", but prevention, because when institutions are late, the gap is filled by speculation and manipulative frameworks.

Public service broadcaster and media with structural risks related to public resources and connections

In media with a public role or with potential dependence on public resources, the risk of FIMI most often does not appear as "direct propaganda", but as an uncritical sharing, legitimization or reinforcement of other people's frames, especially in crisis and geopolitical contexts. Therefore, measures here are aimed at protecting editorial autonomy, transparency and professional standards that reduce vulnerability.

- Additional systemic **strengthening of the public service broadcaster (Macedonian Radio Television) is needed, through real guarantees of independence** with transparent and non-partisan procedures for the selection of management and supervisory bodies, clear criteria for integrity and public accountability of the management. One option for this measure is to separate MRT from the Law on Audio and Audiovisual Media Services (LAAVMS) and draft a separate law for the public service broadcaster. This is in line with the principles of the Council of Europe and EMFA's logic for protection from political influence and strengthening the public interest.
- **The public service broadcaster should incorporate the FIMI issue into its own strategic documents and internal mechanisms**, i.e. protocols for checking and contextualizing foreign sources, clear rules for covering geopolitical topics during sensitive periods, and upgrading internal ethical standards to prevent manipulative "rebroadcasting".
- In the segment of **channels with structural risks** (non-transparent ownership, dependence on public funds, opaque financial flows), the key response is **transparency**, i.e. public, easily searchable information **on ownership and financing**,

as well **as clear rules for public funds** (including state advertising) with clear criteria, procedures, accountability and independent oversight. These measures reduce the "grey zone" in which influence can be exercised without public visibility.

- The role of **the regulator** should **be strengthened** not in the direction of sanctioning politically inappropriate content, but **as a public resource for monitoring trends**, with periodic reports with indicators of recurring manipulative practices and exposure structures in broadcasting, which will serve as a basis for policies and professional correction mechanisms.
- With **regard to foreign state-controlled propaganda channels, any measure affecting distribution must be strictly based on legality and proportionality**, with clear guarantees (legal basis, transparent decision, possibility of legal protection) and, where applicable, aligned with European restrictive measures, in order to avoid counter-effects and risk of abuse.

Transparency, media literacy and support for independent media

Given that state-regulated channels, i.e. sources that cannot formally be attributed to a state actor, but show systematic coherence and similar behavioural characteristics, encompass the zone in which manipulative frameworks are most often presented as "organic" public sentiment, the key response cannot be repressive. The most effective measures here are long-term, i.e. critically informed citizens, professional media and sustainable corrective mechanisms.

- **Media and information literacy** should **be positioned as a systemic policy**, not a project activity. It should be integrated as a horizontal competence in education (with outcomes and materials) and complemented by programs aimed at adults conducted through local institutions and public campaigns. This is the foundation of resilience, as it reduces vulnerability to emotional and identity manipulations.
- Transparent mechanisms to **support public interest journalism, especially investigative journalism and network/narrative analytics are necessary**. A key requirement is that the instruments are designed with strong protection from political influence (public calls, independent commissions, accountability), so that they do not become an instrument of control. Additionally, **specialized training and mentoring for journalists** on reporting and research on FIMI, development and use of existing tools for verification and analysis, as well as cooperation with analytical centres and international journalist associations are needed - activities that are starting in our country, but need to be made systematic and continuous (ICS, 2025).
- **Self-regulation** (the Ethics Council, the Council of Honor, as well as journalist and media associations) should **be strengthened as a public resource**, through stable support, greater visibility and a clear role in professional debates on standards,

including standards for the use of foreign sources, unverified claims and sensitive geopolitical narratives. Self-regulation offers legitimate correction without state pressure.

- **Transparency in political communication and advertising, especially online, should be increased** through clear watermarking of political advertisements and sponsored content, information about the client and funding, and stronger oversight during election periods in coordination with the SEC, the regulator, and citizen observers. This reduces the possibility of FIMI being "disguised" as a legitimate internal campaign. Additionally, the labelling of texts, photos, and videos that are created by public institutions **and** then sent to the media in the form of press releases or public information should also contain a clear logo from the specific institution. In this way, the audience will more clearly distinguish between government communication materials and authentic media content.

Multi-sectoral coordination: connecting the security sector, media and civil society

One of the most consistent findings is that North Macedonia has individual capacities, but lacks a permanent coordination platform. Therefore, the following is recommended:

- **Establish a national platform/council on FIMI and hybrid threats that will connect relevant institutions, AVMS, SEC, media organizations, self-regulatory bodies, fact-checking initiatives and research centres.** This body should not be a so-called "truth commission", but a practical mechanism for exchanging indicators, harmonizing protocols and improving public communication in crisis situations.
- **joint training and simulation exercises** for election-related manipulation scenarios are recommended, as well as the development of standard operating procedures that define steps for monitoring, verification, institutional response, media information, and cooperation with corrective actors (media self-regulation).
- Measures should rely on **regional and international cooperation** (methodologies and good practices of the EEAS, the Council of Europe, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki, as FIMI is usually a cross-border phenomenon and requires comparability of data and early warning mechanisms.

Online platforms, synthetic content and electoral integrity (intersectional priority)

Given that a significant portion of exposure to Foreign Information Manipulation and Interference occurs through online platforms and algorithmic distribution, it is necessary **to establish a clear national "election protocol" for the digital sphere**. The goal of such a protocol is not to control content, but to strengthen transparency, timely information, and trust in the electoral process.

This protocol should be based on coordination between the State Election Commission, the regulator, relevant state institutions and civil society observers, with clearly defined roles and procedures regarding the transparency of political advertising, timely identification of coordinated inauthentic networks and public information in cases of systemic manipulation. It is particularly important that these mechanisms function without restricting legitimate political speech and with full respect for freedom of expression.

In this context, special attention should be paid to synthetic and manipulated content (including audio and video materials), which pose a growing risk to electoral integrity and trust in institutions. This is expected to become an increasingly significant problem in the future, given the availability of applications based on artificial intelligence and the potential to generate content that can then be misused. Clear rules are needed for marking such content, public guidelines for its recognition, and established procedures for rapid and verifiable clarifications by institutions, especially in cases where an "official" source is imitated or misrepresented. Such an approach has a preventive function and reduces the possibility of manipulation spreading before it is publicly exposed.

List of abbreviations

AVMS - Agency for Audio and Audiovisual Media Services
AEC - Agency for Electronic Communications
BDE - Bureau for Development and Education
CSO - Civil Society Organizations
SEC - State Election Commission
LAAVMS – Law on Audio and Audiovisual Media Services
AJM - Association of Journalists of Macedonia
ICT - Information and Communication Technologies
ICS - Institute of Communication Studies
MIM - Macedonian Institute for Media
MIL - Media and Information Literacy
NIS - Networks and Information Systems (in the context of the Law on Security of Network and Information Systems)
MoD - Ministry of Defence
MFA - Ministry of Foreign Affairs
MoI - Ministry of Interior
MRT - Macedonian Radio and Television
CMEM - Council of Media Ethics of Macedonia
FIMI - Foreign Information Manipulation and Interference
EU - European Union
AI Act – EU Artificial Intelligence Act
CoE - Council of Europe
CDMSI – Steering Committee on Media and Information Society (Council of Europe)
MSI-INF – Committee of Experts on the Information Environment (Council of Europe)
DSA - Digital Services Act
EEAS - European External Action Service
EMFA - European Media Freedom Act
ENISA - European Union Agency for Cybersecurity
EUvsDisinfo - EEAS/EU platform for monitoring and debunking disinformation
FIMI - Foreign Information Manipulation and Interference
FIMI-ISAC - (FIMI) Information Sharing and Analysis Center
International IDEA - International Institute for Democracy and Electoral Assistance
NATO - North Atlantic Treaty Organization
OSCE - Organization for Security and Co-operation in Europe
OSINT - the process of collecting and analysing publicly available information to assess threats, make decisions, or answer specific questions.
UNDP - United Nations Development Program

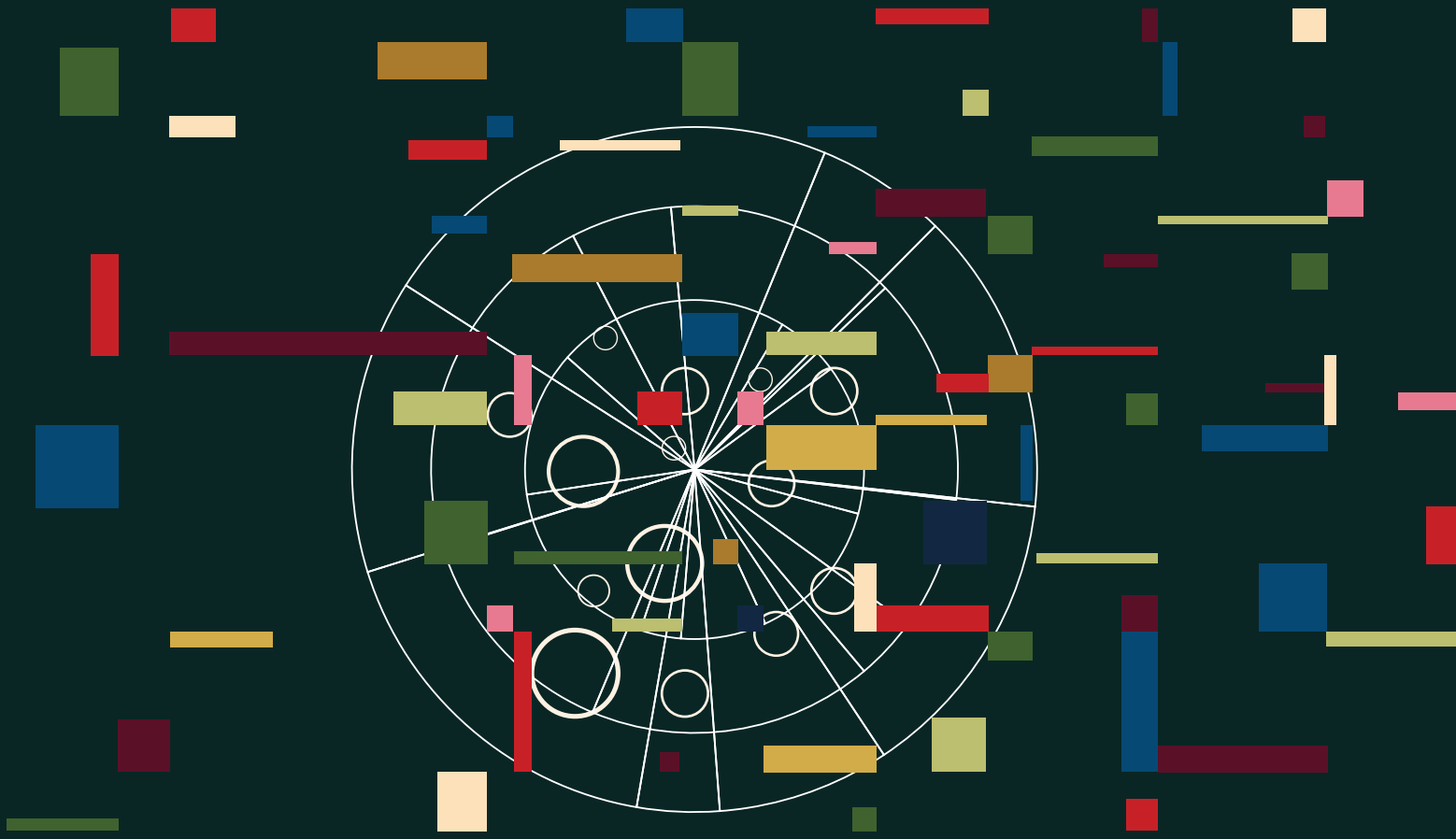
References:

1. Association of Journalists of Macedonia (AJM) and SafeJournalists Network (2025) North Macedonia: Indicators on the Level of Media Freedom and Journalists ' Safety Index 2024. Skopje: AJM/ SafeJournalists Network.
2. Council of Europe (2023) Guidance Note on countering the spread of online mis - and disinformation through fact-checking and platform design solutions in a human rights compliant manner (adopted by CDMSI, 15.12.2023). Strasbourg: Council of Europe.
3. Council of Europe (2021) Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Strasbourg: Council of Europe.
4. Delov, V. (2025) "ICS initiates institutional coordination in dealing with foreign influence and disinformation". Institute of Communication Studies, 16.07.2025.
5. European Commission (2025) "Commission endorses the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act" (Press release, 12.02.2025). Brussels: European Commission.
6. European Commission (2025) North Macedonia Report 2025. Brussels: European Commission.
7. European Commission (2025) "The Digital Services Act". Shaping Europe's digital future (policy page). Brussels: European Commission.
8. European External Action Service (EEAS) (2025) "Inside the infrastructure of Foreign Information Manipulation and Interference (FIMI) operations". Brussels: EEAS.
9. European External Action Service (EEAS) (2025) 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats: Exposing the architecture of FIMI operations (March 2025). Brussels: EEAS.
10. European Commission (2024) Commission Guidelines for providers of Very Large Online Platforms and of Very Large Online Search Engines on the mitigation of systemic risks for electoral processes, pursuant to Article 35(3) of Regulation (EU) 2022/2065 (OJ C 2024/3014, 08.02.2024). Brussels: European Commission.
11. European Union Agency for Cybersecurity (ENISA) (2022) Foreign Information Manipulation and Interference and Cybersecurity: Building a common situational awareness. Luxembourg: Publications Office of the European Union.
12. European External Action Service (EEAS) (2022) A Framework for a Joint EU Response to Foreign Information Manipulation and Interference (FIMI). Brussels: EEAS.

13. European External Action Service (EEAS) (2023) Foreign Information Manipulation and Interference (FIMI): A Framework for Analysis. Brussels: EEAS.
14. European External Action Service (EEAS) (2023) 1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats: Towards a Framework for Networked Defense (February 2023). Brussels: EEAS.
15. European External Action Service (EEAS) (2024) Second EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats (January 2024). Brussels: EEAS.
16. EUvsDisinfo (2025a) "Behind the curtain: a novel analytical approach to FIMI exposure". EUvsDisinfo, 19.03.2025.
17. EUvsDisinfo (2025b) "Enter the galaxy: a network analysis of influence operations". EUvsDisinfo, 09.04.2025.
18. European Union (2024) Regulation (EU) 2024/1083 (European Media Freedom Act). Official Journal of the European Union.
19. European Union (2022) Regulation (EU) 2022/2065 (Digital Services Act). Official Journal of the European Union.
20. European Union (2024) Regulation (EU) 2024/1689 (Artificial Intelligence Act). Official Journal of the European Union.
21. International IDEA (2025) Enablers and Incentives of Election-Related Foreign Information Manipulation and Interference in North Macedonia. Stockholm: International IDEA.
22. IREX (2024) Vibrant Information Barometer (VIBE): North Macedonia 2024. Washington, DC: IREX.
23. IViR (2025) European regulatory frameworks on election disinformation. Amsterdam: Institute for Information Law (IViR).
24. Macedonian Institute for Media (2023) Deprived media market, low ethical standards and the need for effective legislation: The future of media in North Macedonia. Skopje: MIM.
25. Macedonian Institute for Media (2021) Regulatory and self-regulatory framework against hate speech and disinformation in North Macedonia. Skopje: MIM.
26. Metamorphosis Foundation (2024) Disinformation and Civil Society Mapping Report: Western Balkans Region. Skopje: Metamorphosis Foundation.
27. NATO (2024) "Countering hybrid threats". NATO (web resource).
28. NATO StratCom Centre of Excellence (2020) Risks and Vulnerabilities in the Western Balkans. Riga: NATO StratCom COE.
29. ResPublica (2025) Национален систем за отпорност на СММИ. Skopje: ResPublica.

30. ResPublica (2025) "Selmani: Six people are 'defending' 150 institutions from cyber attacks". ResPublica (interview), 21.08.2025.
31. ResPublica (2025) "Trajanov: Macedonia is exposed to attempts to influence internal affairs". ResPublica (interview), 29.07.2025.
32. ResPublica (n.d.) "Tools for Dealing with Foreign Information Manipulation and Interference". ResPublica.
33. South East European Network for Media Professionalization (SEENPM) and OurMedia (2024) Trust in media and vulnerability to disinformation in South East Europe – Country findings for North Macedonia. Ljubljana: SEENPM/ OurMedia.
34. Trojachanec, M. and Rizaov, G. (2024) Stability Under Threat: FIMI in North Macedonia (September 2024). Skopje: Metamorphosis Foundation.
35. YouthWiki (European) Commission /EACEA) (2025) "6.8 Media literacy and safe use of new media – Republic of North Macedonia". YouthWiki.
36. Bureau for the Development of Education (2023) Рамка за медиумска писменост во основното образование. Скопје: Биро за развој на образованието.
37. Bleyer -Simon, K. (2025) Policy Paper: Addressing Foreign Information Manipulation and Interference in the Context of European Regulations. Skopje: Institute of Communication Studies (ResPublica).
38. Grizhev, A. and Poposka, V. (2025) Institutional Response to FIMI in North Macedonia: Models and Policy Options. Skopje: Institute of Communication Studies (ResPublica).
39. State Election Commission (2024) Electoral Code – consolidated text (April 2024). Skopje: State Election Commission.
40. Association of Journalists of Macedonia (2025). Annual Report on Media Freedom and Safety of Journalists – 2024. Skopje: AJM
41. Institute of Communication Studies (2025) "Second Meeting of the Coordinating Body for Dealing with Foreign Information Manipulation and Interference (FIMI)". Institute of Communication Studies, 20.11.2025.
42. Institute of Communication Studies (2025) "Training for Journalists on Reporting on Foreign Information Manipulation and Interference (FIMI)". Institute of Communication Studies, 25.08.2025.
43. Institute of Communication Studies (2024) "Workshop: Media Literacy Competencies". Institute of Communication Studies, 05.11.2024.
44. Kramarska, S. (2025). Дали порталите од странство повторно ќе оживеат во предизборието?. SamoPrasaj, 16.09.2025.
45. Ministry of Digital Transformation (2025) Cyber Security Strategy 2025 - 2028. Skopje: Ministry of Digital Transformation.
46. Ministry of Digital Transformation (n.d.) National Security Strategy of the Republic of North Macedonia. Skopje: Ministry of Digital Transformation.

47. Ministry of Defence of the Republic of North Macedonia (2021) Cyber Defence Strategy. Skopje: Ministry of Defence.
48. Media Literacy Network (2023) "About Us / What is the Media Literacy Network?". Online platform.
49. Media Literacy Glossary (n.d.) "About the Glossary". Online platform.
50. Parliament of the Republic of North Macedonia (2025) "Law on Amendments to the Law on Media", Official Gazette of the Republic of North Macedonia, No. 87/2025 (29.04.2025).
51. Parliament of the Republic of North Macedonia (2024) "Law on Amendments to the Law on Audio and Audiovisual Media Services", Official Gazette of the Republic of North Macedonia, No. 193/2024 (18.09.2024).
52. Parliament of the Republic of North Macedonia (2023) Law on Security of Network and Information Systems. Skopje: Parliament of the Republic of North Macedonia.
53. Hadzi-Janev, M. and Stoilkovski, M. (2025) Foreign Information Manipulation and Interference in the Republic of North Macedonia - Baseline analysis. Skopje: Institute of Communication Studies (ResPublica).



Institute of Communication Studies

www.iks.edu.mk
info@iks.edu.mk

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This product has been prepared as part of the UK Government-funded project "Tracking, Exposing, and Countering Hidden Foreign Manipulations and Interferences", supported by the British Embassy in Skopje. The opinions and views expressed herein do not necessarily reflect the opinions and views of the British Government.