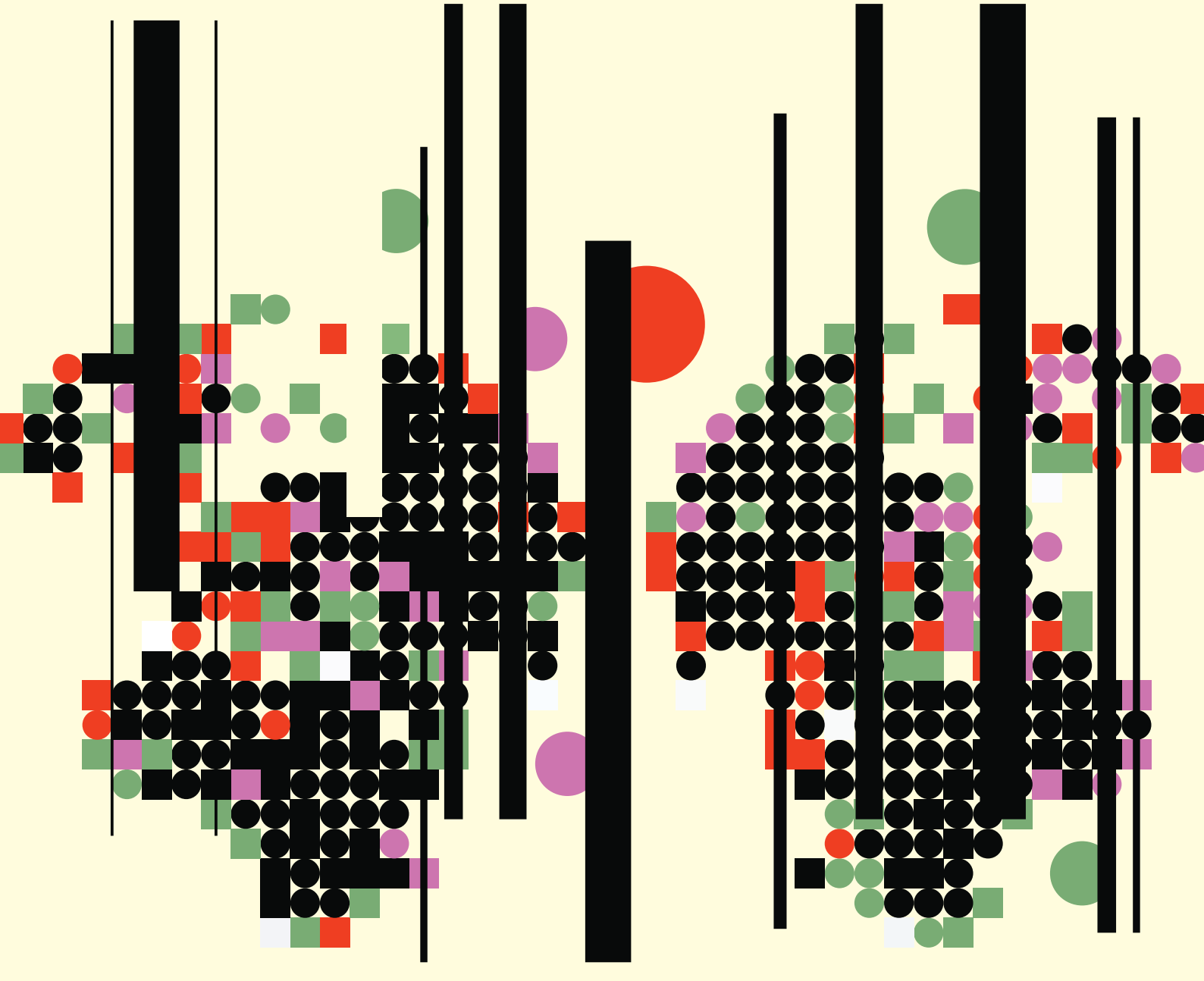
Institute of
Communication Studies

Foreign Information Manipulation and Interference (FIMI) in North Macedonia: Baseline Assessment of Institutional Readiness, Coordination Frameworks, and Response Capacities



Skopje, 2026

Institute of Communication Studies

respublica

Original title (Macedonian):

Странско мешање и манипулирање со информации (СММИ) во Северна Македонија: Основна проценка на институционалната подготвеност, рамките за координација и капацитетите за одговор

Title:

Foreign Information Manipulation and Interference (FIMI) in North Macedonia:
Baseline Assessment of Institutional Readiness, Coordination Frameworks, and Response Capacities

Publisher:

Institute of Communication Studies (ICS), Skopje

Authors:

Vladimir Delov, Bojan Georgievski, Prof. Dr. Zaneta Trajkoska

Expert review:

Joe McCaron-Shipman, UK Government Communication Service International
Francesca Boggeri, OSCE/ODIHR
Federico Giulio Sicurella, Independent FIMI researcher and consultant
Vesna Poposka, PhD, Assoc. Prof.
Aleksandar Grizev, PhD, Assoc. Prof.

For the publisher:

Prof. Dr. Zaneta Trajkoska

Layout:

Zoran Kardula

Graphic editing:

Dejan Joveski

Translation (Macedonian to English language):

Gordan Tanaskov

Edition:

ResPublica

Place and year:

Skopje, 2026

CIP - Каталогизација во публикација
Национална и универзитетска библиотека “Св. Климент Охридски”, Скопје

342.5:[316.776.23:327.8](497.7)(047.31)
[316.776.23:327.8]:34(4-672ЕУ:497.7)(047.31)

DELOV, Vladimir
Foreign Information Manipulation and Interference (FIMI) in North Macedonia [Електронски извор] : Baseline Assessment of Institutional Readiness, Coordination Frameworks, and Response Capacities / [Vladimir Delov, Bojan Georgievski, Zaneta Trajkoska ; translation (Macedonian to English language) Gordan Tanaskov]. - Текст во PDF формат, содржи 24 стр.,. - Skopje : Institute of Communication Studies, 2026. - (Edition ResPublica)

Начин на пристапување (URL):
https://respublica.edu.mk/wp-content/uploads/2026/04/fimi-in-macedonia-baseline-assessment-of-institutional-readiness-en.pdf
(Слободен пристап). - Наслов преземен од екранот. - Опис на изворот на ден 26.05.2026. - Фусноти кон текстот. - Превод на делото:Странско мешање и манипулирање со информации (СММИ) во Северна Македонија:
Основна проценка на институционалната подготвеност, рамките за координација и капацитетите за одговор. - Библиографија: стр. 24

ISBN 978-608-4805-86-1

1. Georgievski, Bojan [автор] 2. Trajkoska, Zaneta [автор]
а) Дезинформации -- Странски влијанија -- Институционален одговор -- Македонија -- Истражувања б) Дезинформации -- Странски влијанија -- Законско регулирање -- Европска Унија -- Македонија -- Истражувања

COBISS.MK-ID 68848389

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This document is prepared within the programme Strengthening the Operational Readiness for Government Response to FIMI in North Macedonia funded by the UK Government with the support of the British Embassy Skopje. The content of this publication does not necessarily reflect the position or the opinions of the UK Government.

Contents

Glossary 3
Introduction..... 5
1. North Macedonia's legal and strategic framework for responding to FIMI..... 8
2. Analysis of the legal mandates of key institutions in North Macedonia..... 11
2.1. Intelligence Agency..... 11
2.2. National Security Agency..... 11
2.3. Ministry of Defence and the Law on Defence..... 11
3. Findings from the qualitative research..... 13
Summary of findings for North Macedonia..... 16
4. European Union: Building a common framework to counter FIMI..... 17
4.1. Analytical foundations for understanding FIMI: the ABCDE..... 19
4.2. The analysis cycle..... 20
4.3. DISARM Framework..... 22
4.4. The FIMI Exposure Matrix..... 23
5. RESIST 3: The UK Approach to Countering FIMI..... 24
5.1. The six steps of RESIST 3..... 25
6. Next Steps..... 27
Bibliography..... 30

Glossary

FIMI	Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character and is conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.
Incident	A FIMI incident is an action perpetrated by one or more threat actor(s) pursuing specific objectives and carried out with the intent to deceive. It is composed of a combination of observables and TTPs. Multiple related incidents can be part of a campaign.
Campaign	A coherent set of FIMI incidents launched, over a certain period of time, against one or more targets with a unified objective and a potential narrative arc. One or more campaigns can be attributed to an IMS.
DIMI	Domestic information manipulation and interference (DIMI) involves intentional, domestically coordinated campaigns, often by utilizing bots, trolls, and local proxies to distort public opinion, weaken trust in democratic institutions, and sway elections. Like FIMI in technique and intent (manipulation of the information space to undermine democratic processes), but executed by domestic actors, such as local political parties, organizations, or individuals, against their own population.
IMO	Information Manipulation Operations - deliberate, coordinated campaigns designed to deceive audiences, distort reality, and influence perceptions, behavior, or decisions to serve a specific agenda. These operations utilize techniques like spreading disinformation, propaganda, and using fake accounts to polarize societies and erode trust, often executed by foreign actors, but not exclusively.
Grey zone	'Grey zone' refers to hostile activity below the threshold of direct, state-on-state conflict, designed to coerce governments or simply erode their ability to function.
TTPs	Tactics, Techniques, and Procedures (TTPs) used by threat actors, to uncover how FIMI campaigns are structured, executed, and adapted over time
Attribution	Process of identifying responsible parties: It seeks to answer "who" (state, state-linked, or proxy) is behind a coordinated, deceptive information campaign, which is often difficult due to the intentional use of proxies and masking techniques to evade detection.
Online trolling	Online trolling is the act of deliberately posting inflammatory, insincere, or off-topic messages in online communities to provoke, upset, or humiliate others. Trolls seek emotional responses or disruption for entertainment, often acting under anonymity to harass users.

Introduction

The evolution of the modern information landscape has placed North Macedonia at a critical juncture. While hybrid threats, disinformation campaigns, or Foreign Information Manipulation and Interference (FIMI) are increasingly identified in national strategies as a primary threat to security and democratic stability, the transition from general recognition toward concrete operational readiness remains a significant challenge. Current institutional responses are often fragmented, partly because they struggle to reconcile high-level policy definitions with the messy, "actor-agnostic" reality of the digital environment.

To address this, the document acknowledges that while FIMI is the primary strategic concern, the operational entry point must be the broader concept of Information Manipulation Operations (IMOs). This shift recognizes a fundamental reality of the information gray zone: in the early stages of an incident, the distinction between foreign and domestic (DIMI) actors is rarely provable without deep forensic or intelligence data. By adopting an IMO-first lens, institutions can avoid the risk of narrowing investigations prematurely or being paralyzed by a lack of immediate attribution. In this framework, identifying the source is treated as a vital subsequent analytical stage rather than a qualifying entry point for defensive action. By focusing on the how - the tactics, techniques, and procedures (TTPs)-rather than the who, institutions can initiate response protocols without being paralyzed by the forensic delays of definitive attribution. In this context, attribution is treated as a vital subsequent intelligence stage rather than a prerequisite for defensive action.

However, the specific focus of this research remains firmly on FIMI, reflecting North Macedonia's commitment to aligning with Euro-Atlantic security frameworks. While the boundaries between FIMI, DIMI, and general disinformation campaigns are inherently porous, foreign interference represents a unique threat to national sovereignty that requires specialized diplomatic and strategic counters. This research treats FIMI as the "strategic endpoint" of a funnel-a specific subset of manipulation that demands a targeted institutional response once the manipulative behaviour has been identified and mitigated.

The objective of this baseline document is to bridge the gap between strategic policy and tactical execution. By providing a shared analytical foundation that recognizes the operational fluidity of information threats, it offers a roadmap for developing standardized coordination mechanisms, robust Standard Operating Procedures (SOPs), and specialized incident-response tools. This ensures that North Macedonian institutions are equipped to act decisively against manipulative patterns while maintaining the analytical depth required to isolate and counter foreign interference.

This baseline builds directly on three previous publications by the Institute of Communication Studies (ICS), which together establish the evidence base for why a more operational approach is needed. First, the policy paper "Institutional Response to Foreign Information Manipulation and Interference in North Macedonia: Models and Policy Options"[1] provides qualitative insight into how institutions currently understand FIMI and how they respond in practice. It highlights that understanding of FIMI varies across the public sector, that it is more developed within the security and intelligence community, and that there is still no shared, harmonised institutional understanding across government. Most importantly, it concludes that despite the existence of relevant institutions and individual capacities, North Macedonia still lacks a formalised and coordinated model for inter-institutional cooperation in relation to FIMI incidents, resulting in reactions that are often ad hoc and dependent on individual initiative.

[1] Institute of Communication Studies (ICS) (2025) Institutional Response to Foreign Information Manipulation and Interference in North Macedonia: Models and Policy Options. Skopje: ICS. Available at: https://respublica.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf

Second, the policy paper "Addressing FIMI in the Context of EU Regulations"[2] situates this institutional challenge within the evolving European policy and regulatory environment, clarifying why EU approaches matter for candidate countries and why compatibility with EU standards is increasingly relevant for cooperation and preparedness. Third, the study "Foreign Information Manipulation and Interference in North Macedonia"[3] provides a wider picture of the national FIMI landscape and reinforces the assessment that preparedness and coordination gaps remain central constraints. Taken together, these documents show a consistent pattern: the problem is not only limited capacity, but the absence of a predictable operational "route" for how a FIMI incident moves from detection to assessment, to decision-making, to public communication, and to learning.

The baseline is guided by the following core questions: How do internationally established analytical and response frameworks for FIMI function in practice, particularly within the European Union and the United Kingdom? Which elements of these frameworks are most relevant and applicable to the institutional context of North Macedonia? Where are the main gaps between existing national strategies and the day-to-day operational reality of institutions when responding to FIMI incidents? How can current institutional mandates and capacities be connected into a clearer, more predictable coordination and response model?

The baseline is based on qualitative research and document analysis. It draws on a review of key EU and UK analytical and operational frameworks for addressing FIMI, including ABCDE, the EEAS analysis cycle, DISARM, the FIMI Exposure Matrix, and RESIST 3, examining these frameworks as institutional tools rather than abstract models. In parallel, ICS conducted semi-structured interviews with former and current senior public officials, members of parliament, and civil servants from relevant institutions. These interviews were complemented by consultative discussions within an ICS-initiated Coordination Body on FIMI. This process enabled the exchange of practical experience and perspectives on existing coordination practices, limitations, and institutional bottlenecks. While contemporary European frameworks emphasize a "Whole-of-Society" approach involving civil society organizations (CSOs), media actors, and private technology companies, this research purposefully narrows its focus to state and government capacity. This delineation is based on the premise that a robust "Whole-of-Government" foundation is a functional prerequisite for any broader societal mobilization. In the context of North Macedonia, institutional fragmentation remains the primary hurdle; therefore, this study prioritizes the internal coordination mechanisms, legal mandates, and operational readiness of state institutions.

While the vital role of non-state actors and the necessity of engaging technology company focal points are recognized as essential long-term assets, they remain outside the immediate scope of this analysis. The objective here is to evaluate the institutional backbone of the state—the "first responder" in the face of hybrid threats—before these broader multi-stakeholder architectures can be effectively integrated. Consequently, the semi-structured interviews conducted for this study were localized to senior public officials and civil servants to specifically diagnose the internal structural gaps within the state apparatus.

This baseline is not a policy strategy and does not replace national strategic documents. Instead, it serves as a technical and analytical bridge between strategy and practice. Its intended outcome is to support the development of realistic coordination flows, SOPs, and incident-response templates that align with EU and partner standards while remaining grounded in the current capacities and mandates of North Macedonian institutions.

---

[2] Institute of Communication Studies (ICS) (2025) Addressing FIMI in the Context of EU Regulations. Skopje: ICS. Available at: https://respublica.edu.mk/wp-content/uploads/2025/06/policy-paper-addressing-fimi-in-context-of-eu-regulations-en.pdf

[3] Institute of Communication Studies (ICS) (2025) Foreign Information Manipulation and Interference in North Macedonia (Baseline study). Skopje: ICS. Available at: https://respublica.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf

1. North Macedonia's legal and strategic framework for responding to FIMI

North Macedonia has formally acknowledged hybrid threats and information operations as part of its national security environment. In the 2021 Strategy for Building Resilience and Tackling Hybrid Threats, as well as in the 2018 Strategic Defence Review, hybrid threats are defined as the coordinated use of conventional and unconventional methods by state or non-state actors to achieve strategic objectives. These threats combine asymmetric, psychological, and cyber elements, exploit societal vulnerabilities, and ultimately aim to undermine trust in democratic institutions.

North Macedonia's key strategic reference point is the Strategy for Building Resilience and Tackling Hybrid Threats 2021–2025, which clearly recognises information operations as a serious threat. The strategy explicitly mentions the use of media manipulation, coordinated networks of bots and trolls on social platforms, and the spread of false news and disinformation as instruments of hybrid activity.

This strategic framing provides an important policy foundation for FIMI preparedness. It confirms that information manipulation is not treated as an isolated communication issue, but as part of a broader national resilience challenge. At the same time, the practical limitation remains that strategies often describe what should exist, such as early warning, coordination, and resilience-building, without establishing a single operational workflow for how institutions detect, assess, escalate, and respond to concrete incidents in practice.

North Macedonia's legal framework does not use the term "FIMI" directly (which is normal, because the concept is newer than many laws). Instead, the legal basis usually appears through broader mandates such as protecting sovereignty, constitutional order, national security, countering foreign subversion, addressing cyber threats, and coordinating the security-intelligence community. In the current North Macedonian policy landscape, Information Operations and FIMI are not treated as standalone silos, rather they are viewed as tactical instruments within the broader strategic toolbox of hybrid warfare.

To make this approach operational, the strategy defines several priority areas. Three are especially relevant for this baseline. First, it foresees the development of an early warning and reporting system to protect against information operations, drawing on EU and NATO expertise. Second, it highlights the role of civil society in strengthening media literacy and critical thinking through education. Third, it sets objectives in the information sector, including the ability to detect disinformation and psychological operations and to address coordinated online trolling.

The strategy also outlines three core methods: early detection of threats, resilience-building to reduce harm, and an effective strategic-level response process led through the national security-intelligence coordination structures. Importantly, it notes that early recognition should not rest only with security services, but that all ministries should develop basic preparedness.

The most recent national document addressing information operations in North Macedonia is the National Security Strategy 2024–2029. This strategy identifies information manipulation and foreign influence as some of the most serious challenges to national sovereignty and democratic processes.

The strategy provides a comprehensive assessment of the security environment and, across several sections, directly or indirectly treats FIMI-related activities as a high-intensity security risk. In the

section on espionage and the activity of foreign intelligence services (II.1.7), such actions are described as a real and serious threat. These activities are framed as part of a broader hybrid approach aimed at influencing internal stability through political confrontation, deepening intra- and inter-ethnic or religious polarisation, and systematically promoting Eurosceptic narratives that weaken trust in NATO and Euro-Atlantic integration. Particular attention is given to the targeting of organisations, political actors, and individuals linked to extremist ideologies, who may serve as channels for shaping public opinion.

Hybrid threats are further identified as one of the fastest-growing challenges at both regional and global level. The strategy notes that such threats are carried out through synchronised and coordinated activities by both state and non-state actors. These activities often involve a wide range of intermediary structures, including NGOs, political organisations, religious groups, and public figures.

The analysis emphasises that these operations are designed for long-term influence over strategic orientation and social cohesion. Key methods include political subversion and economic pressure, as well as information operations that involve the financing and instrumentalization of media, the spread of disinformation, and the systematic misuse of digital platforms and online portals. The strategic objective of these activities is to increase social divisions, encourage ethnic nationalism, create public anxiety, and undermine trust in democratic institutions (II.1.8).

The strategy also explicitly addresses foreign malign influence (II.1.9) by naming specific state actors and their strategic directions. In the context of North Macedonia, it highlights that Russian influence is pursued through interference in democratic processes, large-scale disinformation campaigns, malicious cyber activity, and illegal intelligence operations. It also stresses the use of domestic intermediaries, including political parties, civil society actors, and media outlets, to slow down or undermine Euro-Atlantic integration and influence the country's strategic choices.

Within the main policy objectives supporting national security interests, the Strategy defines the Council for Coordination of the Security-Intelligence Community as the key responsible body for providing strategic guidance, adopting conclusions, and proposing response measures against hybrid threats (III.1.4). Its role includes overseeing the implementation of the national resilience strategy and the accompanying action plan, in line with NATO and EU standards.

In addition, under the policy objective III.4.2 ("Countering disinformation and developing media literacy"), the Strategy highlights that addressing disinformation is a core element of the broader response to hybrid threats. A particularly important provision is the planned establishment of a central coordination body composed of institutional communicators from key sectors, including government, defence, foreign affairs, internal affairs, education, health, and others. This body would be mandated to coordinate institutional activities related to disinformation and to support a national approach to countering foreign information manipulation and interference, recognising disinformation as one of its central instruments.

The EU–North Macedonia Security and Defence Partnership creates a clear alignment incentive

A major recent development is the EU–North Macedonia Security and Defence Partnership, which includes cooperation areas that are directly relevant to information threats, resilience, and strategic communication. This partnership strengthens the case for aligning national operational practice with EU approaches, terminology, and coordination expectations.

This baseline supports alignment with partner expectations and makes future cooperation easier because it uses the same logic that EU partners increasingly expect: shared concepts, repeatable processes, and documented incident handling.

2. Analysis of the legal mandates of key institutions in North Macedonia

Effective national responses to Foreign Information Manipulation and Interference (FIMI) depend not only on analytical capacity and situational awareness, but also on clear institutional mandates.

This section provides an overview of the mandates of the key institutions whose responsibilities are relevant for the detection, assessment, and response to foreign influence operations. The purpose is to identify the existing legal foundations that can support an institutional model for coordinated FIMI incident management.

2.1. Intelligence Agency

The Intelligence Agency is mandated to collect intelligence related to threats originating from abroad and to protect the national security and strategic interests of the state. Although the law does not explicitly refer to FIMI, the concept of "threats and risks from foreign sources" provides a clear legal basis for engagement in cases of coordinated foreign influence activity.

Foreign information manipulation campaigns often involve cross-border infrastructure, external coordination, and proxy actors. The Agency's mandate is therefore relevant for supporting attribution efforts, monitoring foreign threat ecosystems, and contributing intelligence assessments that inform national decision-making.

At the same time, intelligence collection alone cannot ensure an effective response unless embedded within a wider coordination process that enables timely institutional escalation, information-sharing, and operational decision-making.

2.1. National Security Agency

The National Security Agency has a broad mandate to protect the constitutional order, sovereignty, and fundamental rights and freedoms of the state.

Established in 2019 as part of wider reforms of the security-intelligence sector, ANB is positioned as a central national security institution capable of functioning as a key coordination node in hybrid threat contexts. In practice, the Agency's mandate allows engagement with complex information incidents that intersect security, public trust, and institutional stability. Within a national FIMI response model, ANB is frequently identified as a potential focal point for early warning, institutional alerting, and cross-sector coordination, not as the sole actor responsible for response, but as a convening institution capable of integrating inputs from multiple domains.

2.2. Ministry of Defence and the Law on Defence

Although the Law on Defence does not explicitly address FIMI, it contains provisions related to intelligence and counterintelligence activities, including the prevention of foreign subversive actions against the defence sector.

Information manipulation campaigns often include narratives designed to undermine trust in defence institutions, weaken alliance cohesion, or distort security-related decision-making. The defence domain is therefore relevant for specific categories of incidents, particularly those involving NATO-related messaging, military legitimacy, or strategic security crises.

However, the Ministry of Defence mandate remains primarily sector-specific. While essential for certain incident types, it cannot serve as the sole institutional lead for national FIMI response, which requires a whole-of-government and whole-of-society coordination model.

3. Findings from the qualitative research

The baseline analysis was complemented by qualitative research conducted by the Institute of Communication Studies (ICS). This phase utilized semi-structured interviews and expert consultations to diagnose the internal structural and operational gaps within the Macedonian state apparatus. To ensure a high-level diagnostic of the state's readiness, the research team approached 10 key state institutions specifically selected for their mandates in national security, foreign policy, and crisis communication. The outreach targeted a strategic cross-section of the state's security and policy architecture, including current and former high public officials. Out of the 10 institutions approached, 6 in-depth interviews were successfully conducted. These participants provided the granular, "behind-the-scenes" insights necessary to understand how information manipulation signals are currently processed, identify where inter-institutional coordination breaks down, and analyze why current responses remain largely ad hoc.

It is important to clarify that this methodology intentionally prioritizes state and government capacity. While European frameworks typically advocate for a "Whole-of-Society" approach, incorporating civil society, media, and tech platforms, this research treats the "Whole-of-Government" response as the foundational layer of national resilience.

The decision to focus on these institutional perspectives, rather than a broader multi-stakeholder sample, was driven by the need to evaluate the institutional backbone of the state. Establishing clear internal SOPs, mandates, and coordination bodies is a functional prerequisite: until the state's "first responders" are synchronized, broader societal mobilization remains premature. Therefore, these interviews serve as a specialized assessment of the state's sovereign responsibility to defend the democratic information space.

The objective of this research was to assess whether institutions in North Macedonia possess practical protocols and coordinated procedures for responding to FIMI incidents, beyond the existence of general mandates and strategic recognition of hybrid threats.

Overall, the findings confirm that while awareness of the threat is increasing, institutional response remains largely fragmented and insufficiently formalised.

A consistent finding across interviews is that the initial identification of potential FIMI incidents is most often expected to originate within the security-intelligence community.

Respondents emphasised that foreign influence operations are still primarily perceived through a national security lens, particularly when they involve suspected external actors, geopolitical objectives, or coordinated manipulation campaigns.

As a result, the first point of alerting and risk assessment is commonly associated with institutions such as the National Security Agency (ANB) or the Intelligence Agency (AR), rather than with civilian ministries or communication departments.

This reflects an institutional logic in which FIMI is treated as a specialised security concern, rather than a cross-government operational challenge.

Coordination remains ad hoc and dependent on informal institutional initiative

Despite the existence of relevant institutions and potential coordination structures, the research confirms that North Macedonia does not yet have a harmonised and formalised model for inter-institutional response to FIMI incidents. This institutional friction is rooted in a dual deficiency that creates a disconnect between intelligence and action. While specialized capacities and technical expertise exist within the security sector, there is a marked absence of dedicated coordination structures within the civilian ministries.

Furthermore, this is compounded by a systemic absence of operational procedures within the existing frameworks. Without these internal "playbooks," even institutions with relevant legal mandates are unable to translate strategic recognition into a predictable and synchronized response. This leaves the state dependent on individual initiative and informal networks rather than institutionalized resilience, significantly hindering the ability to mount a unified defence against sophisticated information threats.

Instead, responses tend to occur through:

- informal communication channels,
- case-by-case institutional judgement,
- and reactive engagement based on individual initiative.

This creates a system in which institutional action is not guided by standard procedures, but by situational improvisation. The absence of clear operational pathways means that similar incidents may be handled differently depending on the institution involved, the individuals in leadership positions, or the perceived political sensitivity of the case.

Lack of clearly defined roles, responsibilities, and escalation procedures

Interviewees repeatedly highlighted that institutional responsibilities in the context of FIMI remain insufficiently defined.

Key procedural questions do not currently have standardised answers, including: which institution is responsible for receiving the first signal, who conducts initial triage and prioritisation, when an incident should be escalated beyond the originating institution, how evidence should be documented and shared, and which actor leads public communication when manipulation affects societal trust.

In practice, institutions operate largely within their own legal boundaries, without an agreed operational process that connects mandates into a coherent response chain.

This reinforces fragmentation and increases the risk of delayed or inconsistent action.

Limited institutional awareness outside the security sector

While awareness of information manipulation threats is relatively higher within security-related institutions, respondents noted that other sectors of government often lack sufficient understanding of FIMI as a structural risk.

In many ministries and public bodies, manipulation campaigns are still interpreted narrowly as:

- media misinformation,
- isolated disinformation cases,
- or communication challenges rather than coordinated influence operations.

This gap in awareness limits the ability of civilian institutions to recognise early signals, assess risks, and contribute to national situational insight.

It also reduces the effectiveness of whole-of-government preparedness, which is a core principle of both EEAS and UK approaches.

Absence of standardised analytical methodology and risk thresholds

The research indicates that although institutions may informally assess the seriousness of manipulation incidents, these assessments are rarely based on shared criteria or structured analytical frameworks.

Risk levels are often described in general terms (low, medium, high), but such judgements remain subjective rather than methodologically grounded.

The lack of common analytical standards limits the ability to:

- compare incidents across sectors,
- prioritise resources consistently,
- and build interoperable institutional knowledge over time.

This highlights the relevance of frameworks such as ABCDE and DISARM, which provide shared analytical language and classification tools.

Need for a central coordination role, combined with distributed institutional readiness

Respondents expressed broad support for the establishment of a more centralised coordination mechanism, rather than the current situation in which multiple institutions may have overlapping or unclear competence.

The National Security Agency (ANB) was frequently identified as the institution best positioned to serve as a central alerting and coordination node, due to its mandate and cross-sector relevance.

However, interviewees also stressed that central coordination does not imply that responsibility should rest exclusively with one institution. Effective response requires shared institutional ownership, structured cooperation across sectors, and clear communication roles for civilian bodies.

This is precisely where the analytical frameworks presented earlier in this baseline document become operationally significant. ABCDE supports structured incident understanding, DISARM enables classification of hostile tactics and techniques, and the EEAS analysis cycle provides a model for repeatable institutional processes. Together, these tools can be translated into national SOPs, escalation pathways, and incident response templates.

International practice, including the EEAS Analysis Cycle and the UK RESIST model, highlights that successful response requires:

- a shared situational picture across institutions and partners,
- clear escalation pathways,

- defined roles for analysis and communication,
- and standardised procedures for information-sharing and documentation.

Without these elements, institutional reactions remain ad hoc, dependent on informal networks, and vulnerable to delay or duplication.

Summary of findings for North Macedonia

The qualitative research confirms several core conclusions:

- North Macedonia possesses foundational legal mandates and strategic recognition of FIMI-related threats.
- However, institutional response remains fragmented, informal, and insufficiently operationalised.
- Clear SOPs, escalation pathways, and shared analytical standards are currently missing.
- Awareness and capacity remain uneven across government sectors.
- A coordinated national model requires both central leadership and whole-of-government readiness.

These findings provide the basis for the development of the TRACE operational outputs, which aim to translate existing institutional infrastructure into practical, repeatable procedures for incident handling and coordination.

4. European Union: Building a common framework to counter FIMI

In the European Union, dealing with Foreign Information Manipulation and Interference (FIMI) has become a serious and growing priority. The reason is simple: these influence operations do not stop at borders. They spread across countries, platforms, and institutions, and they are designed to exploit weak points in democratic systems over time.

Because of this, the EU has been working in recent years to build a common approach for understanding, analysing, and responding to FIMI. This is still a developing field, but the direction is clear: institutions cannot rely only on fact-checking or on reacting to individual false stories. Instead, they need tools that help them recognise coordinated operations, understand who is behind them, how they work, and what kind of damage they can cause.

The leading EU institution in this area is the European External Action Service (EEAS), the EU's diplomatic and foreign policy service, created in 2011. Over time, the EEAS has taken a central role in protecting the EU and its partners from FIMI. Its work includes monitoring influence campaigns, analysing patterns of manipulation, supporting coordination between institutions, and helping build resilience against information threats. Within the EEAS, the EU has also created Strategic Communication Task Forces. These teams work with partners in different regions, including the Western Balkans, to support EU communication[4] and strengthen resistance to foreign manipulation. Their role is not only to communicate EU messages, but also to understand how hostile influence campaigns operate and how societies can respond.

[4] European External Action Service (EEAS), EEAS Strategic Communication Task Forces. Available at: https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en

A key part of the EU's modern approach is the recognition that FIMI is not mainly about one false post or one misleading article. The real issue is that harmful actors often run long-term, coordinated operations. These operations use many channels at once, target specific groups, repeat certain narratives, and aim to create deeper effects, such as weakening trust in institutions, increasing polarisation, or influencing political decisions.

The EEAS defines FIMI as a *"mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character and is conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory."*[5] These activities are intentional, coordinated, and can be carried out by states, non-state actors, or proxies, both inside and outside the target country.

Since this is a relatively new area of work, the EU's tools and methods have developed quickly over the past few years. One of the most important developments is the effort to create a shared analytical language across institutions and countries. Without common standards, cooperation becomes difficult, because different actors describe the same threat in different ways.

The EU uses several tools and frameworks that work together, each serving a different purpose. They provide a structured way to classify the tactics, techniques, and procedures used in influence operations and help analysts document incidents in a consistent format, making it easier to share findings across institutions, countries, and partners.

As a candidate country and a close partner of the EU, North Macedonia faces similar information pressures and needs compatible institutional methods. Understanding these frameworks is therefore not only useful for analysis, but also necessary for building national SOPs, coordination channels, and operational response tools that match European standards and allow effective cooperation with partners.

Therefore, it is necessary to understand these frameworks, such as ABCDE, the EEAS analysis cycle, DISARM, and the FIMI Exposure Matrix, in order to assess how they can be practically useful for North Macedonia and how they can inform the development of national coordination procedures, SOPs, and institutional response tools.

4.1. Analytical foundations for understanding FIMI: the ABCDE

Before institutions can respond to Foreign Information Manipulation and Interference (FIMI), they first need a clear way to understand what they are looking at. In practice, this is one of the biggest challenges. Many actors still treat FIMI as "false news" or isolated disinformation posts. But modern influence operations are more complex: they involve coordination, repeated narratives, amplification networks, and strategic intent.

For this reason, analysts need a simple but structured way to break down a FIMI incident into its key components. One of the most useful starting tools is the ABCDE framework.[6] ABCDE has been applied directly in EU-linked analytical work to structure early assessments of coordinated influence campaigns, such as cases documented through EEAS reporting on pro-Kremlin manipulation efforts during

[5] European External Action Service (EEAS), 2025 EEAS Threat Report, March 2025, https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

[6] European External Action Service (EEAS) (2023) EEAS Threat Report 2023. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

major political moments. ABCDE does not replace deeper investigation. Instead, it provides a basic logic for understanding what makes an incident part of a broader influence operation. When applied consistently across multiple cases, it helps identify patterns, recurring actors, and typical methods.

The framework is built around five core elements:

Actor (A)

The first question is always: who is behind the activity?

The "actor" refers to the potential source of the threat. This can include foreign state actors, intelligence-linked networks, organised proxy groups, or coordinated online communities. In many cases, attribution is difficult because FIMI actors often hide behind anonymous accounts, intermediaries, or misleading branding.

Still, distinguishing between the actor and the channels they use is essential. Even when full attribution is not possible, identifying likely actor types helps institutions understand motivation, strategic goals, and the level of risk.

Behaviour (B)

The second element focuses on how the actor operates.

"Behaviour" refers to the methods used to influence the information environment. This includes coordinated inauthentic behaviour, the use of bots, troll networks, artificial amplification, harassment campaigns, or manipulation of platform algorithms.

This element is especially important because FIMI is defined not only by content, but by patterns of coordinated behaviour. Behavioural indicators often provide stronger evidence than narrative similarity alone.

Frameworks like DISARM, discussed later in this document, are particularly useful here because they allow analysts to classify tactics and techniques in a standardised way.

Content (C)

The third element is the message itself.

"Content" refers to the narratives, formats, and types of information used in the operation. This can include fabricated stories, manipulated media, misleading framing, selective truth, or emotionally charged messaging designed to provoke fear, anger, or distrust.

Content analysis helps institutions understand what kind of information threat they are dealing with, whether it is misinformation, disinformation, or malicious information, and whether it connects to known influence narratives or emerging themes.

Degree (D)

The fourth element looks at scale and spread.

"Degree" refers to how widely the content is circulating and how strongly it is being amplified. This includes the size of the audience reached, the speed of dissemination, the platforms involved, and the presence of coordinated boosting.

This element is critical for prioritisation. Not every incident requires the same level of response. Understanding the degree of exposure helps institutions decide whether an issue is minor noise or part of a larger campaign.

Tools like the FIMI Exposure Matrix, developed by the EEAS, support this kind of assessment by mapping channels and levels of linkage to hostile actors.

Effect (E)

The final element focuses on impact.

"Effect" refers to the outcome the operation is trying to achieve and the influence it is having on the target environment. The goal may not be to convince people of one false claim, but to weaken trust, create confusion, delegitimise institutions, discourage participation, or intensify polarisation.

Effect analysis helps institutions assess how dangerous an operation is and what kind of response is proportional and necessary.

The ABCDE framework is particularly useful for institutional settings because it creates a shared language. It allows different actors, from security services to government communicators, to describe the same incident using comparable categories.

4.2. The analysis cycle

The ABCDE framework helps institutions understand what a FIMI incident consists of: who is behind it, how it works, what content is used, how far it spreads, and what effect it aims to achieve. However, institutions also need a practical process for what to do once such an incident is detected.

This is why the European External Action Service (EEAS) developed the analysis cycle.[7] Unlike ABCDE, which is a conceptual lens, the analysis cycle is an operational workflow. It explains how institutions should monitor, prioritise, investigate, document, and share information about FIMI incidents in a structured and repeatable way.

The purpose of the cycle is to move away from ad hoc reactions and toward a consistent institutional process that builds knowledge over time. It provides the foundation for coordinated analysis and response, which is essential for developing national SOPs and incident-handling procedures. The EEAS analysis cycle translates the understanding of FIMI into a practical step-by-step process. While ABCDE helps describe an incident, the analysis cycle explains how institutions should work through it in an organised way, from early detection to long-term situational awareness.

The cycle consists of five sequential phases:

Phase 1: Strategic monitoring

This phase involves continuous and organised observation of known channels, actors, and infrastructures used for foreign information manipulation. This includes websites, social media accounts, media outlets, and other platforms that have previously been linked to influence activity. The goal is early detection of signals before they escalate.

[7] European External Action Service (EEAS), 2023 EEAS Threat Report, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

Phase 2: Prioritisation and triage

Not every suspicious message requires the same level of attention. This phase serves as a filter, helping institutions focus resources on cases that are more serious, more coordinated, or more likely to cause harm. It separates low-level noise from higher-risk incidents.

Phase 3: Incident analysis and evidence collection

This is the core analytical phase. Analysts conduct deeper investigation using open sources and available data. They examine how content spreads, where it first appeared, which networks amplify it, and what tactics, techniques, and procedures are being used. This is where structured tools such as DISARM become especially important.

Phase 4: Knowledge sharing and coordination

Analysis is only useful if it reaches the actors who can respond. In this phase, findings are shared with relevant stakeholders and partners. In the longer term, incidents are documented in standardised formats so that they can be compared, stored, and used for future learning.

Phase 5: Situational awareness

The final phase focuses on building deeper understanding of the threat environment. Over time, repeated use of the cycle helps institutions identify patterns, emerging actors, and evolving tactics. Monitoring is expanded based on new findings, and institutional response becomes more informed and proactive.

4.3. DISARM Framework

Once institutions can recognise a FIMI incident and follow a basic analysis process, the next challenge is how do we describe what the hostile actor is actually doing in a precise and comparable way?

Unlike ABCDE, which helps explain the overall structure of an incident, and unlike the analysis cycle, which explains the workflow of institutional analysis, DISARM[8] focuses on the operational behaviour of the threat actor.

DISARM (Disinformation Analysis and Risk Management) is an open-source framework developed by the DISARM Foundation and widely used by FIMI analysts across the EU, NATO-related structures, and partner countries. Its purpose is to provide a shared taxonomy, meaning a common language for documenting and classifying the tactics and techniques used in manipulation campaigns.

FIMI operations are rarely isolated events. The same actor often repeats similar methods across different countries, platforms, and time periods. Without a standard way of describing these methods, institutions cannot easily share findings, compare cases, or build early-warning systems. DISARM is built around the idea of a "disinformation kill chain", meaning that manipulation campaigns follow a logical sequence of steps, from planning to execution and assessment. The framework organises these steps into phases, and within each phase it identifies specific tactics and techniques.

[8] DisARM Foundation, DisARM Navigator. Available at: https://disarmfoundation.github.io/disarm-navigator/

The four main phases of DISARM are:

Planning: The actor defines the strategic goal of the operation, selects target audiences, and designs the intended outcome.

Preparation: The actor builds the infrastructure needed for the campaign, such as fake accounts, proxy outlets, coordinated networks, and tailored narratives.

Execution: The campaign is launched through content distribution, amplification, coordination across platforms, and sometimes offline mobilisation.

Assessment: The actor measures impact, adjusts messaging, and decides whether to escalate, repeat, or shift tactics.

The key value of DISARM is that it allows institutions to identify patterns of behaviour, not just individual false claims. By tracking tactics and techniques, analysts can recognise the "signature" of a hostile actor and intervene earlier in the operation, before it produces wider societal effects.

4.4. The FIMI Exposure Matrix

After DISARM helps institutions understand what hostile actors do, the next question is through which channels do they do it?

FIMI operations spread through layered networks of accounts, websites, influencers, proxy media, and coordinated amplification. This is why identifying the full infrastructure of influence is often more important than focusing only on the original message.

To support this type of structured mapping, the European External Action Service (EEAS) developed the FIMI Exposure Matrix in its 3rd EEAS Report.

Unlike ABCDE, which breaks down the incident, and unlike DISARM, which classifies tactics and techniques, the Exposure Matrix focuses on attribution and exposure. Its role is to help analysts and institutions categorise different sources based on how directly they are connected to a hostile actor. It provides clear terminology for describing these channels and their level of connection to a foreign actor. This makes it easier for institutions to build evidence-based responses and to coordinate effectively with partners when exposing and countering FIMI operations. This is essential because in many cases, the most impactful channels are not openly linked to a foreign state. Instead, they operate through indirect or hidden connections, making institutional response more difficult.

The matrix serves four main purposes. First, it supports infrastructure mapping. It helps analysts see beyond the most visible sources and include the wider network that amplifies manipulation. Second, it strengthens evidence-based attribution. The matrix encourages institutions to rely on behavioural and technical indicators, not only narrative similarity, reducing the risk of over-attribution. Third, it supports multi-source analysis. Effective assessment requires combining open-source information with institutional, commercial, or partner data. Fourth, it improves proportional response. By understanding the type of channel involved, institutions can apply more targeted countermeasures and avoid unnecessary escalation.

The Exposure Matrix is built on two key axes.

The first axis is attributed versus unattributed. Attributed channels are those where strong evidence links them directly to a state actor. Unattributed channels show alignment or coordination but lack sufficient proof for formal attribution.

The second axis is overt versus covert. Overt channels openly present their state affiliation. Covert channels hide their origin, ownership, or coordination, operating through proxies or disguised networks. By combining these axes, institutions can classify influence channels into categories that reflect different levels of exposure and responsibility.

5. RESIST 3: The UK Approach to Countering FIMI

If the EU's approach is mostly about building a shared analytical language (how to describe FIMI clearly and consistently), the UK RESIST model is about what institutions should actually do when manipulation starts spreading.

RESIST 3[9] is a structured framework for government communicators. It was developed by Dr James Pamment (who also contributed heavily to ABCDE) and is used as a practical approach for building resilience against information threats. It is not an intelligence framework, and it is not a military doctrine. It is closer to an institutional "playbook" for public-sector communicators, press offices, and decision-makers who need to respond quickly but responsibly. RESIST is now in its third version because the UK has updated the model over time, based on real experience with disinformation campaigns and new changes in the information environment. The first versions focused mainly on basic communication response. The third version is the most developed and practical one, because it includes stronger guidance on building long-term resilience, working across institutions, and responding in a more structured way, including in the context of new technologies like AI.

It proposes realistic communication channels, an operational flow, and an incident-response template that can work across ministries and institutions. RESIST is one of the clearest international examples of how to translate FIMI thinking into a day-to-day institutional routine.

This is why RESIST 3 is especially relevant for North Macedonia. Many institutions in the country are not intelligence agencies, but ministries, public communicators, and officials who need clear and simple procedures when manipulation spreads online. RESIST 3 provides exactly that.

RESIST's approach is not only to "fight disinformation," but to strengthen trust and reduce vulnerability over time. It also takes into account newer technologies, including AI, and improves how institutions assess threats and vulnerabilities. This is critical for these baseline findings, because one of the repeated problems is that risk assessments are often informal, inconsistent, and not shared.

At the core of RESIST is the concept of resilience. In this context, resilience means the ability to withstand an information attack, adapt during the incident, and recover after it. This includes adapted messaging, preparation, coordination, trust-building, and learning from past incidents.

RESIST also assumes a whole-of-society approach. The government cannot do everything alone, and it should not try. The framework treats collaboration with other institutions, media, civil society, and trusted messengers as part of the solution.

[9] Department for Science, Innovation and Technology (DSIT) (2025) RESIST 3: A Framework for Building Government Communication Resilience. Available at: https://www.communications.gov.uk/wp-content/uploads/2025/10/RESIST-FINAL.pdf

That said, RESIST is very clear about one thing: government communication is a critical frontline in FIMI. If institutions communicate poorly, late, or inconsistently, they create space for manipulation to grow.

5.1. The six steps of RESIST 3

RESIST is structured around six linked steps. They are meant to be used as a cycle, not as a one-time checklist. Institutions can enter the cycle at different points depending on the situation, but the logic remains the same: detect early, understand what is happening, decide whether intervention is needed, respond proportionally, and learn.

Recognise

The primary goal of Recognise is to ensure that all government communicators possess a baseline understanding of the mechanics of mis-, dis-, and malinformation, the nature of algorithmic amplification, and the strategic aims of hostile actors. By treating "Recognise" as a pillar of professional development rather than a reactive operational trigger, institutions can build a more resilient and informed frontline against information interference. This foundational, peacetime educational programme ensures that communicators are capable of early identification—the essential "spot it before it spreads" stage—allowing them to detect suspicious narratives or synthetic content without requiring a full intelligence assessment first.

In practice, this is where basic indicators and structured frameworks, such as FIRST (Fabrication, Identity, Rhetoric, Symbolism, and Technology), become vital. Rather than turning every communicator into a professional analyst, these tools reduce guesswork and provide a common language so that when an incident is flagged, the rationale behind it is clear and defensible. This process links directly to the ABCDE framework and the broader analysis cycle by providing the initial data points required for deeper investigation. Ultimately, "Recognise" serves as the moment where triage begins; if this educational foundation is weak, every subsequent institutional response becomes reactive.Early Warning

Instead of monitoring everything, institutions define priorities. They identify which risks matter most (for example, elections, security crises, ethnic tensions, foreign policy decisions, major incidents). They also identify which audiences are most vulnerable or most important in that context.

Early warning becomes realistic when institutions have clear monitoring responsibilities and clear escalation rules. A key theme here is that early warning is not only a technical function. It also depends on institutional discipline: who watches what, who reports, and how fast.

How this builds on earlier parts: this step directly links to the analysis cycle's first two phases (strategic monitoring and prioritisation/triage), but translated into an institutional setting.

Situational Insight

Situational insight means summarising what is happening in a way that is short, clear, and actionable. It is not a long report. It is not a press statement. It is a brief that answers what is happening, who is behind it (if known), who is being targeted, how it is spreading, and what could happen next.

Why it matters for North Macedonia: our baseline repeatedly shows that institutions often do not share a common situational picture. Even when individuals notice the issue, the understanding

stays inside one office or one institution. Situational insight is the bridge between "someone noticed something" and "the system reacts."

Impact Analysis

This step is about deciding whether to intervene, and if yes, how strongly. RESIST does not suggest that the state should declare what is true in every case. Instead, the key question is: what is the likely harm?

Impact analysis looks at possible damage to public safety, institutional trust, democratic processes, social cohesion, or policy implementation. It also considers timing: sometimes the same narrative is minor in one moment and high-risk in another.

A practical feature of this step is the idea of thresholds. Institutions should define what "low," "medium," and "high" risk means in practice, and what types of response match each level.

Without this, response becomes political, inconsistent, or delayed.

Strategic Communication

Strategic communication can include a range of measures, depending on the risk and the type of incident.

It can mean proactive communication that pre-empts likely manipulation. It can mean factual clarification when misinformation spreads. It can mean exposing manipulation tactics when attribution is strong. It can mean working with trusted external messengers instead of using only government voices. It can also mean internal coordination: making sure institutions do not contradict each other.

The core principle is proportionality and credibility. A weak response can amplify the story. An aggressive response without evidence can create backlash. RESIST pushes institutions to respond in ways that protect trust over the long term, not only to "win the day."

How this connects to our next deliverables: the Operational Flow Framework will need to show who drafts messages, who clears them, who coordinates across institutions, and how speed and accuracy are balanced. The template will need space for message objectives, audiences, channels, and risk level.

Tracking Effectiveness

This step is what most institutions skip, and then they repeat the same mistakes forever.

Tracking effectiveness means measuring whether the response worked, and whether the internal process worked.

That includes questions like: did we respond fast enough, did we coordinate properly, did we reduce harm, did we avoid escalating the narrative, did we reach the right audiences, and did we learn anything actionable for next time?

This does not require perfect metrics. It requires simple routines: short after-action reviews, documented lessons, and updates to protocols.

When responses are ad hoc, learning is also ad hoc. Tracking effectiveness is how institutions can turn experience into an institutional memory, instead of relying on the same few individuals who "know how it works."

6. Next Steps

This baseline confirms that North Macedonia does not lack institutions, nor the legal mandates to respond to FIMI in a coordinated manner. It lacks a shared way of working when a FIMI incident appears. Three gaps stand out across the interviews and document review. First, there is no agreed coordination model that clearly answers "who leads, who supports, and when." Second, there are no repeatable incident-handling procedures that move an incident from initial signal to assessment, decision, and public communication in a predictable way. Third, institutional understanding of FIMI remains uneven, which means that the same incident can be treated as a communications nuisance in one place, and a security concern in another.

Frameworks such as ABCDE, the EEAS analysis cycle, DISARM, and the Exposure Matrix each solve a different part of that problem. ABCDE helps break down an incident early and prevents teams from focusing only on "what was said" while missing who is behind it, how it spreads, and what impact it is aiming for. The EEAS analysis cycle shows how professional teams turn constant monitoring into prioritised cases, deeper investigation, shared outputs, and long-term situational awareness. DISARM standardises the behavioural layer, allowing institutions to record tactics and techniques in the same format, which is essential for recognising patterns and collaborating with partners. The Exposure Matrix adds a practical model for mapping channels and infrastructure, which matters when a campaign uses a mix of open outlets, proxy networks, and hidden amplification.

The UK RESIST is relevant for North Macedonia because it was designed for the people who often carry the public-facing burden during an incident: government communicators, press offices, and policy teams that must respond fast, without improvising and without escalating panic.

It provides a simple, repeatable routine for recognising manipulation signals, running early warning, producing situational insight for decision-makers, deciding whether intervention is needed based on harm, executing strategic communication measures, and then checking what worked. If communicators do not have a basic playbook, responses default to ad-hoc reactions, delayed corrections, inconsistent messaging, or silence.

EU frameworks help institutions define and classify the threat in a way that supports evidence-based attribution, shared terminology, and cross-partner cooperation. RESIST helps institutions manage the incident in real time through an operational routine that can be applied across ministries. In other words, EU frameworks build the "common language," while RESIST helps turn that language into institutional action.

Based on the findings of this baseline, the following outputs are proposed to move North Macedonia from strategic intent to functional operationalization:

- A capacity building program for government communicators: A specialized training curriculum designed for press officers, PR specialists, and civil servants across ministries. This program focuses on moving beyond traditional PR toward a security-conscious communication model, specifically targeting:
    - Advanced Media monitoring: Training on tools and techniques to scan the information environment for emerging narratives.
    - Identification and assessment of information threats: Developing the ability to distinguish between organic domestic debate and coordinated manipulation (IMOs/FIMI).
    - Risk and impact assessment: Establishing a methodology to evaluate the potential for public harm, social polarization, or security risks posed by a specific campaign.

    - Strategic communications and evaluation: Mastering the art of proactive and reactive messaging, followed by rigorous evaluation to determine the effectiveness of the intervention.
    - Ethical standards and democratic safeguards: Ensuring every action is grounded in transparency, accuracy, and the "Do No Harm" principle.

- The Central Government Coordination Body (CGCB) Protocol: In alignment with the National Strategy for Security 2024-2029, this output will define the operationalization of a central body to synchronize government efforts. This body will act as the vital link between political communication and national security:

- An Operational Flow Framework that should define the institutional route of a FIMI incident from first detection to shared assessment, escalation, decision, public response, and review. It should clarify who convenes whom, which channels are used for urgent coordination, what triggers escalation, and how information is shared across institutions without confusion or duplication.

- An Incident Response Template that should standardise documentation so that institutions do not lose time debating what to record and how. It should capture the minimum fields needed to support EU-compatible analysis and partner cooperation, and a clear statement of assessed impact and confidence level. Standardised templates are what makes cases comparable, what enables institutional memory, and what allows lessons learned to turn into faster and better decisions next time.

Expansion toward a "Whole-of-Society" resilience framework

A structured mechanism for multi-stakeholder collaboration that bridges the gap between government operations and external expertise. This output focuses on moving beyond internal capacity to leverage the diverse strengths of non-state actors through:

- CSO and academic partnerships: Formalizing pathways for Civil Society Organizations (CSOs) and researchers to provide independent monitoring, data analysis, and pedagogical support for media literacy initiatives.
- Expert-led red teaming: Engaging digital experts, OSINT (Open-Source Intelligence) specialists, and cybersecurity professionals to simulate information attacks and stress-test existing government response protocols.
- Public-private information sharing: Establishing secure channels for real-time communication with digital platforms and tech experts to identify and mitigate the spread of Foreign Information Manipulation and Interference (FIMI) at the source.
- Co-designed public awareness: Developing joint communication campaigns with academia and CSOs to build civic "cognitive immunity," ensuring that messaging is trusted, inclusive, and reaches marginalized communities.
- Shared knowledge repository: Creating a centralized, non-classified database of emerging narratives and tactics accessible to both government communicators and authorized research partners to ensure a common operating picture.

This baseline shows that North Macedonia's strategic documents increasingly recognise hybrid threats, information operations, and foreign influence as serious risks. That is aligned with European practice and provides an enabling policy environment. The weak point is the operational bridge between strategy and daily response. The next phase therefore needs to focus on operationalisation: taking what exists on paper and making it work the same way every time, regardless of which institution sees the signal first.

Bibliography

1. DISARM Foundation, DISARM Navigator. Available at: https://disarmfoundation.github.io/disarm-navigator/
2. European External Action Service (EEAS), EEAS Strategic Communication Task Forces. Available at: https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en
3. European External Action Service (EEAS) (2023) EEAS Data Team Threat Report 2023 [PDF]. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf
4. European External Action Service (EEAS) (2025) EEAS 3rd Threat Report (March 2025) [PDF]. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
5. Institute of Communication Studies (ICS) (2025) Addressing FIMI in the Context of EU Regulations [Policy paper]. ResPublica. Available at: https://respublica.edu.mk/wp-content/uploads/2025/06/policy-paper-addressing-fimi-in-context-of-eu-regulations-en.pdf
6. Institute of Communication Studies (ICS) (2025) Foreign Information Manipulation and Interference in North Macedonia [Study]. ResPublica. Available at: https://respublica.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf
7. Institute of Communication Studies (ICS) (2025) Institutional Response to Foreign Information Manipulation and Interference in North Macedonia: Models and Policy Options [Policy paper]. ResPublica. Available at: https://respublica.edu.mk/wp-content/uploads/2025/12/institutional-response-to-fimi_en.pdf
8. UK Government Communication Service, RESIST [PDF]. Available at: https://www.communications.gov.uk/wp-content/uploads/2025/10/RESIST-FINAL.pdf

Institute of
Communication
Studies

