FOREIGN INFORMATION MANIPULATION AND INTERFERENCE IN THE REPUBLIC OF NORTH MACEDONIA

Baseline study

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE IN THE REPUBLIC OF NORTH MACEDONIA

Baseline study

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

About the publisher:
Assoc. Prof. Dr. Zhaneta Trajkoska

Edition:
ResPublica

Authors:
Assoc. Prof. Dr. Metodi Hadzi-Janev
Marijan Stoilkovski, PhD

Editor:
Dejan Andonov, MA

Translation from Macedonian:
Olivera Celeska

Original title:
Странско мешање и манипулирање со информации - појдовна анализа

Graphic design:
Igor Delov

Place and year:
Skopje, 2025

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

327.8(497.7)(047.31)
316.776.23(497.7)(047.31)
327.8(4-672ЕУ)(047.31)
316.776.23(4-672ЕУ)(047.31)

HADZI-Janev, Metodi
Foreign information manipulation and interference in the Republic of North Macedonia [Електронски извор] : baseline study / [authors Metodi Hadzi-Janev, Marijan Stoilkovski ; Translation from Macedonian Olivera Celeska]. - Skopje : Institute of Communication Studies, 2025. - (Edition ResPublica)

Начин на пристапување (URL):
http://respublica.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf.
- Превод на делото: Странско мешање и манипулирање со информации : појдовна анализа. - Текст во PDF формат, содржи 68 стр. - Наслов преземен од екранот. - Опис на изворот на ден 02.06.2025. - Фусноти кон текстот. - About the authors: стр. 63. - Библиографија: стр. 64-68

ISBN 978-608-4805-63-2

1. Stoilkovski, Marijan [автор]
а) Странски влијанија и дезинформации -- Справување -- Македонија -- Истражувања б) Странски влијанија и дезинформации -- Справување -- Европска Унија -- Истражувања

COBISS.MK-ID 66062341

CONTENTS

Executive summary 6

Introduction 7

Methodology 9

1. Foreign information manipulation and interference: concept and characteristics 11

1.1. Defining Foreign Information Manipulation and Interference 13

1.2. How does Foreign Information Manipulation and Interference manifest 14

2. Institutional capacity and vulnerabilities in North Macedonia in dealing with foreign information manipulation and interference 17

2.1. General overview of institutional capacity in North Macedonia to deal with Foreign Information Manipulation and Interference 19

2.2. Legal and regulatory framework 20

2.3. Critical Review: Institutional Challenges in North Macedonia in Dealing with Foreign Information Manipulation and Interference 23

2.3.1. Overview of the state capacity to respond to disinformation campaigns 27

2.4. Analysis and critical review of the role of the local community as a target of Foreign Information Manipulation and Interference 30

3. The role of the media and civil society in North Macedonia and the vulnerability to foreign information manipulation and interference 32

3.1. The role of the media in dealing with Foreign Information Manipulation and Interference 33

3.2. The role of civil society in addressing Foreign Information Manipulation and Interference 35

4. Cyber crime and social media as tools for foreign information manipulation and interference 39

4.1. How cyberattacks and manipulative disinformation are connected 41

4.2. Cybercrime and disinformation as a risk to the economic sector 44

4.3. Mechanisms for cybersecurity and protection against disinformation 45

4.4. Tips for protecting against cyber threats 46

5. A brief overview of european best practices in dealing with foreign information manipulation and interference 49

5.1. Successful practices in some EU countries 51

5.1.1. Strengthening the institutional response: successful models 51

5.1.2. Regulatory framework: how can the law protect democracy? 52

5.1.3. Public awareness and media literacy: a key line of defence 53

5.2. Brief overview of best practices and experiences of the EU and NATO in dealing with Foreign Information Manipulation and Interference 54

5.2.1. EU East StratCom Task Force 55

5.2.2. Hybrid Center of Excellence: hybrid defence through strategic analysis and coordination 56

5.2.3. EU Rapid Alert System: rapid response to information threats 57

Recommendations for creating policies to deal with foreign information manipulation and interference in North Macedonia 58

Conclusion 61

About the authors 63

References 64

EXECUTIVE SUMMARY

This study looks into the mechanisms, methods, and effects of Foreign Information Manipulation and Interference (FIMI) in the Republic of North Macedonia, with a special emphasis on national security, media diversity and social cohesion. As a country with a strategic position in the region, a member of NATO and a candidate for the European Union (EU), North Macedonia faces increased information threats coming from various state and non-state actors. These influences have the potential to disrupt democratic processes, weaken institutions and spur-on public distrust.

The study shows that Foreign Information Manipulation and Interference is not an isolated phenomenon, but part of broader hybrid strategies that combine disinformation, geopolitical narratives and cyber operations to shape public opinion and political decisions. The analysis covers multiple domains, including institutional readiness (with a focus on good governance), traditional media, digital space and social media, local communities and civil society organizations, identifying key methods and approaches used for political and ideological polarization.

Despite the existence of legal and institutional frameworks to address Foreign Information Manipulation and Interference, the nation's capacity for detection and counteraction remains limited and inconsistent. The analysis shows that a more comprehensive approach is needed, which will include better coordination between state institutions, civil society and the media community. Of particular importance is the promotion of good governance of state bodies, the improvement of regulatory mechanisms for transparency in the media, the strengthening of analytical capacities for monitoring digital threats and building public resilience through media literacy.

This study offers recommendations for improving strategies for dealing with Foreign Information Manipulation and Interference, with a focus on preventive and reactive measures that will enable the protection of the space i.e. the channels for information in North Macedonia. The recommendations include structural reforms, improving international cooperation and developing national mechanisms for detecting and neutralizing disinformation campaigns. The role of state institutions, the media and civil society is crucial in this fight, as only through a joint approach can the consequences of foreign information influences be minimized and the democratic values and security interests of the country be protected.

INTRODUCTION

In the modern globalized world, information is a powerful tool that can be used as an instrument to influence societies, political processes and security policies. Foreign Information Manipulation and Interference poses a serious challenge to national security, public trust and democratic institutions. FIMI encompasses a wide range of activities, including disinformation, cyber-attacks, media propaganda and coordinated influence campaigns that aim to undermine democratic processes, cause rifts in society and weaken state institutions.

In the context of North Macedonia, which is a NATO member and a candidate for EU membership, this threat takes on particular significance. As a strategically positioned country in the Balkans, North Macedonia is exposed to various forms of foreign influence that often involve the manipulation of information in order to undermine public trust in institutions, generate political instability, or hinder Euro-Atlantic integration. External actors, using advanced digital tools, social and traditional media, are increasingly conducting information operations targeting key sectors in the country.

This baseline study aims to define the nature, scope and methods of foreign information manipulation and interference in North Macedonia. In addition, to determine the level of exposure of North Macedonia to threats from FIMI, this Report analyses the vulnerabilities, risks and impacts on public institutions, the media and civil society.

To get a full understanding of the country's vulnerability to Foreign Information Manipulation and Interference and the effects that can be caused by such actions, the analysis focuses on several key aspects. First, it addresses how public institutions deal with FIMI, and in that context, whether there are structural or human weaknesses. This section reviews the legal and regulatory framework, institutional capacity, and the approach and ability to respond to disinformation campaigns. Then, the analysis focuses on the media and social networks, as well as on the role of the local community (a seemingly overlooked segment) as a target of influence and in dealing with these challenges. The analysis also provides an overview of how cybercrime and disinformation are combined, especially through social media.

By mapping existing NATO and EU policies and frameworks, as well as mechanisms available to national institutions, the study identifies crucial capacities of the Macedonian society to counter foreign information manipulation and interference.

Based on the findings, the study proposes best practices and recommendations to help strengthen resilience in the societal, media and cyber spheres, and ultimately - the national security and democratic stability of North Macedonia.

METHODOLOGY

This study is based on a desktop analysis as the primary methodological approach for examining the phenomenon of Foreign Information Manipulation and Interference in North Macedonia. This approach involves the collection, processing and synthesis of existing information from relevant sources in order to gain a comprehensive insight into the nature, methods and impact of FIMI on national security and social stability. This data was then processed thanks to the professional and academic experience of the authors.

The research is based on an analysis of official documents, reports and regulatory frameworks, which include government strategies for dealing with hybrid threats, cybersecurity, media literacy and national security. In addition, the analysis includes documents from relevant security institutions in North Macedonia, NATO and the EU, as well as legal regulations related to countering disinformation and foreign influence. For a deeper understanding of the problem, the study includes research conducted by international think tanks, research centres and organizations working on issues related to hybrid threats and disinformation, such as the NATO StratCom Center of Excellence, the EU-NATO Hybrid Center of Excellence and the EU East StratCom Task Force, including, no less importantly, the authors' experience in collaborating with these institutions on the given topic and problem.

In addition to academic and institutional sources, the analysis includes media publications and reports from non-governmental organizations dealing with media transparency and monitoring the information space. Special attention is paid to the role that media and social media platforms play in the spread of disinformation.

Methodologically, the study employs qualitative content analysis to identify key narratives, methods, and actors involved in foreign information manipulation and interference. This approach allows for a systematic categorization of techniques used in information operations, including disinformation, media manipulation, news fabrication, cyber-attacks, and geopolitical propaganda strategies. In addition, comparative analysis is used to compare the Macedonian context with similar experiences from other countries in the region, which allows for a better understanding of the patterns and dynamics of the FIMI threat.

Additionally, the research analyses factors that increase North Macedonia's vulnerability to foreign information manipulation and interference, such as weaknesses in media literacy, institutional capacity, and political polarization. The political and regulatory analysis, in turn, allows for an assessment of existing mechanisms for dealing with these threats, as well as their effectiveness in relation to the country's national interests and security priorities.

While this research provides an in-depth analysis of Foreign Information Manipulation and Interference in North Macedonia, certain limitations should be considered. The lack of transparent data, the confidentiality of intelligence, and the dynamic nature of disinformation campaigns pose challenges to a full and objective assessment of the problem. Despite these limitations, this study aims to provide a systematic overview of the nature, methods, and impact of FIMI in the country. It aims to map existing policies and mechanisms to counter threats and propose recommendations for strengthening national resilience.

1.

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE: CONCEPT AND CHARACTERISTICS

In the contemporary global information space, Foreign Information Manipulation and Interference represents one of the most sophisticated and destructive threats to democratic processes, national security and social cohesion. This phenomenon is based on the strategic and deliberate manipulation of information to sway decisions of citizens, institutions and governments, most often to the benefit of foreign actors.

Foreign Information Manipulation and Interference is not just classic disinformation. It is a complex mechanism that combines tactics of propaganda, media manipulation, destabilization through social media, economic and political pressures, and even cyber activities. Its essence is in the controlled distortion of the information landscape in order to achieve long-term geopolitical influence.

1.1 DEFINING FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

In its simplest terms, foreign information manipulation and interference is an organized, intentional, and often covert activity by state or non-state actors aimed at manipulating the information environment in order to achieve a political, military, economic, or social advantage *(EEA, 2023)*. The key characteristics of foreign information manipulation and interference include *(Diplomatic Service of EU, 2025):*

- **a manipulative approach** – through fabricated, manipulated or selectively presented information to create a false picture of reality;
- **such activities have a strategic goal** – the goal is not only to disinform, but also to influence the public, institutions or decision-makers and to corrupt democratic processes;
- **application of different tactics and channels** – the use of FIMI involves combining methods of classical propaganda, digital manipulation, cyber-attacks, and even economic and diplomatic instruments (for example, through Multitrack Diplomacy, i.e. Track -II Diplomacy) *(Diamond L., McDonald J., 1996)*.
- **complex to detect and monitor** – unlike conventional disinformation, FIMI is often conducted at multiple levels, with complex narratives and coordinated networks of actors, often skilfully hidden between legitimate democratic processes.

Foreign Information Manipulation and Interference is designed to act multidimensionally. They attack institutions, but not directly, instead they use the approach through citizens, thanks to the misuse of modern information and communication technologies, and recently through the so-called transformative or disruptive technologies that are on the rise. This allows them to influence by controlling or imposing control over the content with which they (dis)inform citizens, collect and process data including through cyberattacks, manipulating web search engines and algorithms. FIMI is therefore not only a threat to individual information users, but a threat to institutions through creation of information chaos, social and political divisions.

1.2 HOW DOES FOREIGN INFORMATION MANIPULATION AND INTERFERENCE MANIFEST

FIMI is not limited to one form of manipulation. It manifests itself through various tactics adapted to the target country and the specific context. The most common forms of Foreign Information Manipulation and Interference include: disinformation and propaganda, abuse and manipulation of media and social media space, cyberattacks, influence and manipulation through economic and diplomatic sectors.

FIMI also uses advanced methods of classical propaganda and the dissemination of disinformation and propaganda. They involve deliberate dissemination of false, distorted or manipulated information to undermine the credibility of institutions, media outlets or individuals *(Boulianne Sh., Humprecht E, 2023)*. To create divisions in society, FIMI also involves creation of false narratives that discredit political opponents or advance a particular agenda, typically by exploiting historical, ethnic and religious tensions *(Miguel R., 2024)*.

Media and social media manipulation is a technique that is common with these practices *(Kelly S at all, 2017)*. It often includes control or infiltration into local media, through various forms, donations, sponsorships of projects or, alternatively, full takeover and installation of editorial boards prone to the proliferation of false information and manipulation of information intended to shape public discourse. Media manipulation also includes the practice of creating fake media platforms that imitate relevant sources but spread propaganda content *(CISA, 2023)*. The use of bots, trolls and coordinated campaigns for the mass dissemination of manipulative content are an additional multiplier in the manipulations (Walker Sh., Simeone M., 2020).

FIMI often attacks sectors of society that do not prioritize their tasks, missions, resources and capacities to deal with foreign influence. This increases vulnerabilities across society and requires cross society engagement and coordination.

Cyber-attacks are an integral part of FIMI strategies. These include:

- **hacking and exfiltrating sensitive data,** including ransomware attacks, to compromise political figures or institutions;

- **conducting attacks through Distributed Denial of Services DDoS** on media websites or government websites to reduce their availability;

- **false reports or information** that creates panic aiming to paralyze or test, i.e. shift the system and create cumulative intolerance towards the government/leadership;

- **manipulating social media algorithms** to promote or suppress certain narratives (to redirect traffic, block, reduce or speed up or overcrowd).

Although seldom addressed in North Macedonia, FIMI often happens through economic and diplomatic channels. This can include, among other things:

- **using strategic investments, economic aid and loans, as well as market freedom** to gain influence over media, academic institutions or political elites, through third (usually partner) countries;

- **using energy dependence or trade ties** to impose a political agenda;

- **diplomatic pressure** through media propaganda funded by foreign governments (for example, "Russia Today ", "Sputnik" and others).

The use of a synchronized campaign indicates that FIMI does not happen sporadically (although the intensity may vary) and is not implemented randomly. On the contrary, behind all actions lie strategic goals often aiming to (EUEA, 2023):

- **delegitimize democracy and institutions** – undermining citizens' trust in their governments and creating perceptions of inefficiency and corruption;

- **political polarization** – inciting conflicts between different groups in society in order to weaken social cohesion;

- **manipulation of electoral processes** – influencing public opinion through disinformation campaigns, especially during elections;

- **undermining security alliances (NATO, EU)** – creating a perception that Western institutions are weak, divided, or unable to provide stability.

- **strengthening the influence of authoritarian states** – promoting narratives that present the authoritarian model as more efficient and desirable than liberal democracy *(EUEA, 2025)*.

However, although FIMI is not a simple phenomenon, its impact can be significantly reduced through strategic approach and strong institutional preparedness.

2.

INSTITUTIONAL CAPACITY AND VULNERABILITIES IN NORTH MACEDONIA IN DEALING WITH FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

The manipulation of information by foreign services directly or via proxy poses a serious challenge for institutions in North Macedonia. In conditions of intensified geopolitical competition and digitalization, strong institutional capacity to deal with FIMI is truly necessary. Understanding of institutional vulnerabilities and gaps is therefore required to design recommendations.

2.1. GENERAL OVERVIEW OF INSTITUTIONAL CAPACITY IN NORTH MACEDONIA TO DEAL WITH FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

This is the first analysis on the preparedness of North Macedonia institutions to deal with FIMI. It focuses on the existing legal and regulatory framework, institutional capacity (government Agencies and their approach – reactive/proactive, inter-institutional coordination and communication) and the approach to disinformation campaigns.

The findings – in summary - are that Macedonian institutions are still at an early stage in terms of fully understanding and effectively dealing with FIMI. Awareness among political representatives of the threat from FIMI is only declarative. Institutional representatives recognize the threat, often as part of hybrid threats. Unfortunately, in practice, there is very little that could be used to realistically measure if awareness of the threat is at an adequate level (EU Commission, 2023). For instance, while in their speeches at public events, political representatives rightly recognize the threat (MIA, 2022), very little action to counter it can be seen in practice. For example, there is no data on funds allocated from the State budget for capacity building to deal with this challenge. Instead, all training and capacity building actions take place with donor funding.

The Strategy for Dealing with Hybrid Threats is the only document that closely addresses the problem of Foreign Information Manipulation and Interference. The document is on the website of the Ministry of Defence that led on its development. While the Government has tasked the Security and Intelligence Community Coordination Council to delegate the implementation of the tasks from the Strategy and the Action Plan, in practice this Council it is not operational.

This existence of the Strategy is a good start, but more needs to be done to operationalise it.

2.2. LEGAL AND REGULATORY FRAMEWORK

In North Macedonia, the legislation lacks specialized measures for FIMI. Whilst provisions targeting topics related to FIMI exist in some laws including the Criminal Code, the Law on Personal Data Protection and the Law on Amendments to the Law on Personal Data Protection, it is evident that these provisions alone are not sufficient to directly deal with FIMI. The absence of specific laws or by-laws directly targeting foreign influence on the information space only confirms that the legal and regulatory framework in the country for dealing with FIMI needs further development.

Relevant legislation that should serve as a foundation in tackling Foreign Information Manipulation and Interference include: the Law on Criminal Procedure, the Criminal Code, the Law on Interception of Communications and the Law on Electronic Communications, which, among other things, regulate the security of personal data and define terms that play an important role in online communication of Macedonian citizens. In addition, laws that should be taken into account are: the Law on Media, the Law on Audio and Audiovisual Media Services, the Law on Prevention of Money Laundering and Financing of Terrorism, the Law on Civil Liability for Insult and Defamation[1], the Law on Child Protection (which regulates the child protection system and organization) and the Law on Justice for Children. Taking into account the complexity of Foreign Information Manipulation and Interference, it could be said that this list of legal acts does not end here. For example, in addition to disinformation and propaganda, the scope of FIMI includes influence operations through cyber-attacks, with the aim of either changing official information and creating uncertainty and disinformation or exploiting the under-preparedness of the reaction system and based on that, manipulating and disinforming. Hence, this points to the need for additional legal solutions.

During the preparation of this study, the Law on Security of Networks and Information Systems had gone through Governmental procedure and it was submitted to the Parliament of RNM. Networks and information systems, primarily the Internet, play a crucial role in facilitating malicious actions and the use of Foreign Information Manipulation and Interference. Due to their transnational nature, significant disruptions

1 Which refers to Article 8 of the European Convention on Human Rights (ECHR) on the protection of private life, reputation and honour

to these systems, whether intentional or unintentional and regardless of where they occur, can also affect North Macedonia. In addition, this law transposes Directive (EU) 2016/1148 of the European Parliament and of the European Council of 6 July 2016 concerning measures for a high general level of security of network and information systems across the Union, i.e. the Directive on the Security of Network and Information Systems, known as the *NIS Directive*.[2] A more in-depth focus on some of the pieces of legislation as follows:

A BRIEF OVERVIEW OF THE PROVISIONS OF THE CRIMINAL CODE (CC) OF THE REPUBLIC OF NORTH MACEDONIA

There are several articles in the Criminal Code that can be indirectly linked to Foreign Information Manipulation and Interference. For example, Article 137 of the Criminal Code criminalizes “incitement of national, racial and religious hatred, discord and intolerance” and speech that causes hatred and discord. However, this article does not cover the influence of foreign actors or organized disinformation campaigns.

Furthermore, Article 274, which refers to unauthorized interception of communication and wiretapping, refers to illegal activities that may be part of FIMI, but does not cover digital disinformation or foreign interference through the media.

Also interesting is Article 394-d - Terrorist Threat, which refers to acts that are a threat to security but does not cover psychological manipulation through information. The Criminal Code will need to evolve to address Foreign Information Manipulation and Interference including by:

- clear definition of “foreign information manipulation”;
- foreseeing sanctions for organized disinformation campaigns sponsored by foreign states;
- adapting to the existence of digital threats and cyberspace.

2 Во оваа директива меѓу другото се инсистира земјите членки да ги подобрат своите способности за сајбер-безбедност, истовремено воведувајќи мерки за справување со ризик и барања за известување на субјекти од повеќе сектори и воспоставување правила за соработка, споделување информации, надзор и спроведување мерки за сајбер-безбедност.

BRIEF OVERVIEW OF THE MEDIA LAW AND THE LAW ON AUDIO AND AUDIOVISUAL MEDIA SERVICES

The Law on Media (2013) regulates media entities and transparency of ownership. The Law on Audio and Audiovisual Media Services (2018, amended 2023) regulates the operation of broadcasters and obliges media to transparency in financing. These laws however:

- lack mechanisms for preventing foreign propaganda through national, regional and local media;
- lack measures to address instances of media knowingly spreading Foreign Information Manipulation and Interference;

A BRIEF OVERVIEW OF THE LAW ON THE PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

This law, among other things, regulates monitoring of financing organizations and media. However, given that there is no clearly adopted definition of Foreign Information Manipulation and Interference through a strategic document on this matter, the law does not explicitly target the application of FIMI. The main shortcomings with respect to FIMI of the Law on the Prevention of Money Laundering and Financing of Terrorism are the following:

- there is no system for monitoring foreign funding of news websites;
- the financing of online platforms, which can serve for Foreign Information Manipulation and Interference, is not regulated.

A BRIEF OVERVIEW OF THE LAW ON PERSONAL DATA PROTECTION

In general, this law regulates the use and protection of personal data. However, the law does not regulate the misuse of data for “targeted disinformation” or “psychological operations”, i.e. influence operations. With that in mind, main shortfalls of the Law in addressing FIMI are:

- lack of mechanisms to protect against foreign digital manipulation (like a Cambridge Analytica-type scenario) or manipulation by so-called “platform companies”)[3]
- lack of clear procedures for responding to mass psychological operations, i.e. influence operations based on data misuse.

2.3. CRITICAL REVIEW: INSTITUTIONAL CHALLENGES IN NORTH MACEDONIA IN DEALING WITH FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

The fight against Foreign Information Manipulation and Interference in North Macedonia is hampered by institutional weaknesses, limited resources, and inconsistent strategies. Although there are formal mechanisms and institutions that, according to laws and other regulations, are responsible for protecting against such threats, their real capacity to counter coordinated disinformation campaigns remains worryingly low. An additional problem is the lack of merit-based appointments in the public sector.

In essence, Macedonian institutions, such as the National Security Agency (NSA), the Ministry of Interior (MoI), the Intelligence Agency (IA), the Military Service - Security and Intelligence Sector (MSSI) under the Ministry of Defence (MoD), and the National Center for Computer Incident Response (MKD-CIRT), respond to foreign information manipulation and interference on an ad hoc basis, without a single, centralized strategy that would enable an efficient, coordinated response.

The National Security Agency (NSA), which has a mandate for counterintelligence operations, in practice does not have a specialized team that deals with digital disinformation and hybrid threats. Instead, it mostly relies on traditional intelligence methods. These methods, in the context of modern information warfare, which also

3 These are companies that, rather than producing products or services directly, provide the infrastructure that enables third parties to create value. “Platform companies” are transforming the economy and the way people access services, often challenging traditional industries. They are businesses that operate as digital ecosystems, connecting diverse groups of users (e.g., buyers and sellers, drivers and passengers, content creators and consumers).

includes influence operations, abuse of cyberspace, and so-called attacks below the "threshold of classical use of force" that are conducted with the use of technology, are no longer sufficient. A greater challenge is that the NSA does not have clear authorizations to deal with online manipulation of public opinion, especially when they are not the direct result of foreign intelligence services, but of parastate or "grey" networks of players who use local media and social networks as tools for influence. With no public document on building the NSA's capacity in this direction, it is not clear whether the situation is being addressed.

The Ministry of Interior (MoI) Cybercrime Department mainly deals with classic cybercrimes such as financial fraud and hacking. For a structured analysis of disinformation networks, the Sector would benefit from more professionally trained staff, digital forensics experts, sophisticated tools for monitoring digital campaigns, as well as deeper cooperation with global technology companies like Meta, Google, and X.

The Intelligence Agency (IA) similarly requires additional human and technical capacities. Although there are efforts to build capacity through bilateral or multilateral cooperation, these efforts are not planned or funded by the agency itself but are provided through donor-funded projects.

The Military Service's Security and Intelligence Sector within the Ministry of defence – faces similar challenges. The Ministry and the Army of the Republic of North Macedonia (ARNM) need a doctrine for reducing FIMI risk to members of the military and civilian personnel in the armed forces, the ministry and their families in the country, as well as for soldiers and civilian personnel deployed abroad in pre-war missions by NATO, EU or UN. Although there is a military authority for cyber defence, it is mainly focused on protecting critical infrastructure, and less on analysing hybrid threats that include information warfare and influence operations. This is of concern as contemporary military doctrines of Russia, China, but also terrorist groups with a global agenda, rely heavily on information operations as part of their power projection strategy. Although psychological operations are addressed to some extent within the Army, the entire approach is at a basic level with a focus on the army's expeditionary operations, and not in the context of the constitutional duty to defend territorial integrity and sovereignty. With the legal limitation on the Army's operations on the territory of the state, this capacity is inadequate for the threat of FIMI.

Given that within the EU disinformation in 2023 is considered an integral part of cyber threats (CERT–EU, 2024), the National Computer Incident Response Center (MKD-CIRT), operating within the Agency for Electronic Communications, should

continuously strengthen its human and other capacities in order to fulfill its core function – responding to cyber incidents and monitoring EU and NATO trends in this context. Namely, the EU sees disinformation as an integral part of cybersecurity, and since 2015 NATO has considered cyberspace to be a separate domain of warfare, and hence when planning cybersecurity, responses and operations to deal with influence operations should be planned *(Hubervic A., Prudent Y., STO)*. Additionally, cybersecurity, and thus the threats from disinformation and manipulation through influence, are part of national security.[4]

Another critical aspect in this context is that the Agency for Audio and Audiovisual Media Services (AVMS) has jurisdiction over social platforms only if they are registered in the country *(Law on Audio and Audiovisual Media Services, 2014)*. Foreign and domestic disinformation centres can use this legal loophole to create and maintain websites that do not have clearly defined ownership and that can disappear and reappear under a different name in just a few hours.

Foreign influence through disinformation, as in any other country, has a particular weight on electoral processes. Therefore, the State Election Commission (SEC), which is responsible for the transparency of the electoral process, needs to strengthen its capacity to monitor digital interference in elections. Otherwise, in the worst-case scenario, foreign actors could spread false information about the electoral processes with impunity, use bot networks to discredit certain candidates, and even influence the election results through campaigns aimed at discouraging voters. In this context, it is also worth mentioning that online portals registered abroad can receive funds for political campaigns in the country.

Institutional weaknesses are not only a reflection of the challenges that come from the lack of technical or human resources. The core problem lies in the lack of coordination and political will for a comprehensive approach to solving this issue. North Macedonia does not have a separate national centre for combating disinformation. The existing bodies that should cover this area often lack clear mechanisms for exchanging data and intelligence information or are dysfunctional. For example, the Security and Intelligence Community Coordination Council, which is responsible for combating hybrid threats, is nonfunctional and does not enable information exchange at the institutional level. In addition, there is no digital connection between institutions, so in the event of a problem, often due to the organisational setup and different positions

4 For example, the Cyber Defence Strategy, which has expired, recognizes that Article 5 can be a legal basis for conducting physical military operations and the use of force in response to cyber-attacks.

of subsidiarity (which is good for decentralization and avoiding the accumulation of power), it is not clear which institution is failing or has jurisdiction over a given problem. This creates a dangerous vacuum, which foreign actors can exploit to unimpededly spread narratives and other forms of influence that undermine democratic processes and national security.

Another weakness is the fact that institutional initiatives to increase public awareness of Foreign Information Manipulation and Interference and the information and media literacy of the population are few. An institution that has a legal mandate to promote media literacy through cooperation with civil society organizations, educational institutions, media and institutions is the AAVMS. In 2017, it established the Media Literacy Network, now with over 80 members (ministries, state institutions, educational institutions, civil society associations and organizations and media), and once a year it conducts a public interest campaign in cooperation with the media, dedicated to media literacy and safety when using the internet and social media[5]. However, a large part of Macedonian citizens lack the knowledge, skills and tools to recognize manipulative narratives, which makes them vulnerable to influence from various propaganda sources. This situation is exacerbated by the fact that some domestic political elites use disinformation as a tool for political calculation, contributing, consciously or unconsciously, to the intensification of Foreign Information Manipulation and Interference. The proximity of languages (Serbo-Croatian and Albanian) is an additional problem that in an era of open societies and free markets also requires a careful approach.[6]

Faced with this reality, institutions in North Macedonia must take decisive steps to improve capacities and establish a strategy for national resilience to foreign information manipulation and interference. This includes:

- a comprehensive approach to combating disinformation and deciding on a body that will coordinate all state actors in this regard;

5 See more at: https://mediumskapismenost.mk/

6 Foreign actors or local disinformers who are occupied, bribed or bought can quickly adapt narratives from one language to another, or even market them only in Serbo-Croatian or Albanian. In this way, from one centre (Belgrade, Tirana, etc.) they can influence the entire region. This allows for the coordinated spread of false information in different ethnic communities, especially if we also know the fact that a large number of local media outlets, due to their limited capacities, often take information from these centres. This linguistic similarity can also be used to create false translations, disinformation campaigns with manipulated quotes or fabricated news that sound authentic to multiple groups, but are also understood by a larger audience. This is especially dangerous in sensitive contexts such as political crises, elections or interethnic tensions, where manipulated messages can incite distrust, division and destabilization.

- strengthening the capacities of the National Security Agency, the Armed Forces, the Ministry of Interior, the Ministry of Defence and the Armed Forces of the Republic of Macedonia to monitor and neutralize FIMI;
- increased cooperation with NATO, the EU and technology companies to tackle cyber disinformation;
- promoting media and information literacy in the education system as a long-term strategy for building resilience.

If these measures are not timely implemented, the country will remain vulnerable to foreign information manipulation, which in the long term could undermine not only democracy, but also national security.

2.3.1. OVERVIEW OF THE STATE CAPACITY TO RESPOND TO DISINFORMATION CAMPAIGNS

The state capacity to respond to disinformation campaigns, as the most important part of dealing with Foreign Information Manipulation and Interference is limited to monitoring and analysis. Additionally, North Macedonia has weak institutional capacity to provide a comprehensive, thorough and timely response by implementing strategic communications of government. This institutional weakness is accompanied by distrust in institutions due to poor governance. The following section provides a review of the capacity of the state to respond to disinformation campaigns. We will analyse three parameters - capacity to monitor and analyse disinformation, strategic communication of government and formation of a counter-narrative, and citizen trust in institutions.

A BRIEF OVERVIEW OF THE STATE'S CAPACITY FOR MONITORING AND ANALYSING DISINFORMATION

In the modern information space, disinformation spreads at an unprecedented speed. Social media algorithms fuel polarization, and foreign actors use local media, trolls, and botnets to amplify their narratives.

State institutions do not have sufficiently developed mechanisms for monitoring Foreign Information Manipulation and Interference, which is why they often rely on analyses from the non-governmental sector and international partners. Although these analyses are good and desirable, they are not sufficient in themselves and lack a state-led approach.

North Macedonia is a NATO member, and it receives significant assistance from the NATO StratCom Center of Excellence and, as an EU candidate, from the EU initiative to combat disinformation EUvsDisinfo, but these mechanisms have only a consultative role. Even when external partners raise the alarm about disinformation attacks targeting the state, the institutions must have an appropriate mechanism for response. Therefore, an institutional approach is needed that would narrow the room for manoeuvre of malicious, often proxy state and non-state actors.

REVIEW OF THE STRATEGIC COMMUNICATIONS OF GOVERNMENT CAPACITY

In North Macedonia, there is an evidently slow and ineffective counteraction to disinformation campaigns, which leaves room for their intensification. In addition to the lack of monitoring capacities, Macedonian institutions do not have a clear and convincing counter-narrative that would combat disinformation and often they neither respond quickly nor deny or explain disinformation. As a result, falsehoods spread in the public space with great speed. For example, when North Macedonia came under attack from disinformation campaigns about NATO membership, which promoted narratives of “stolen national resources” and “the country’s military involvement in conflicts”, the institutions failed to communicate with the public in a timely manner. Instead of a proactive approach with clear messages and evidence, the state’s reaction was limited to general statements, without strategically designed communication. Another example was the cyberattack on the Health Insurance Fund, for which there are serious concerns about the theft of a huge amount of citizens’ data.

An additional problem is that Macedonian government officials often use complicated bureaucratic language. This language is not adapted and is therefore ineffective in the digital age. Disinformation, on the other hand, is formulated in a simple way, aimed at stirring up emotions, which makes it more accessible and influential for the general public. It articulates emotions, promotes empathy, attacks values, undermines trust, is often stylistically well-crafted with hyperbole, inappropriate comparisons, neglects key moments that could give a different course to their argument-thesis, and emphasizes problematic aspects that serve their purposes. Even when there is no

direct connection, it implies ethnic issues, political disappointments and historically problematic topics, through self-proclaimed legitimacy or taken out of context and incompletely presented theses of scholars and experts.

Another key aspect is the lack of a unit, department or body for a rapid and coordinated response to disinformation attacks. In many countries, such bodies are part of the Prime Minister's office or the Foreign Ministry. Therefore, due to the complexity and diversity of the areas and topics through which disinformation is spread, very often, the giving of inadequate or incomplete statements by official government representatives can be an opportunity for manipulation and disinformation in itself. In practice, journalists often do not have the capacity to report adequately because they lack thematic and professional preparation, and therefore convey information that is partial, often poorly formulated and/or not entirely accurate. As a result, information chaos is established that further erodes the capacity of state bodies to deal with disinformation, and lack of public trust.

PUBLIC TRUST IN INSTITUTIONS AS AN ELEMENT FOR TACKLING DISINFORMATION

The public often believes that institutions themselves are a source of manipulation, which further complicates the fight against Foreign Information Manipulation and Interference. Some citizens see institutions as part of the problem, not as a solution *(Jakimova J., 2022)*. Such distrust generally stems from several factors, such as the political instrumentalization of information, corruption and abuse of political power, poorly organized and unsuccessful communication campaigns.[7] In this sense, the public often witnesses politically motivated interpretations of facts, which reduces the credibility of official sources. Many citizens believe that institutions do not work in their interest, which makes them susceptible to disinformation. This often translates into language such as "the West controls the country" or "North Macedonia is a puppet state." Finally, lack of transparency of institutions is a serious handicap that has been recognized in a series of reports by independent bodies, as well as the EU *(European Commission, 2021)*. Institutions often respond by denying or ignoring controversial topics, which only deepens the crisis of trust.

7 For example, expert opinion is that after the change of government as a result of the wiretapping scandal in 2017, the new (now opposition) leaders seem to have adopted the same strategy or public relations consulting service. Simply put, nothing has changed in this area. The 2023 EU report on North Macedonia notes all this on several occasions. See EU COMMISSION STAFF WORKING DOCUMENT, North Macedonia 2023 Report, available at: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf

2.4. ANALYSIS AND CRITICAL REVIEW OF THE ROLE OF THE LOCAL COMMUNITY AS A TARGET OF FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

Local communities in North Macedonia can play a crucial role in the complex web of disinformation and foreign influence. They are both a target of manipulation and a potential factor of resistance. Disinformation campaigns target local communities through national and local media, social media platforms and networks of informal actors, with the aim of causing distrust, division and destabilization.

Local communities are ideal targets for influence operations for the simple reason that the aim of influence and information operations is to exploit the gaps that exist in the effective management of local institutions in democratic societies. Hence, decentralization of governance and institutions opens up a large number of vulnerabilities for the security of the state. Namely, weaknesses in management of local institutions are exploited by manipulation operations., Most often, local communities are on the front lines of information warfare, as foreign actors exploit existing ethnic, political and economic differences, as well as the lucrative ambitions of local and political elites, to cause instability.

The fact that Macedonian society is multiethnic, in the context of the whole set of circumstances (local dynamics and geostrategic ambitions), the local community in the country is inevitably vulnerable to disinformation narratives that incite interethnic discord. Pro-Russian channels often spread disinformation that “the West is destroying traditional values” or that “NATO is suppressing Macedonian culture” *(Vistinomer (Truthfinder), 2023)*. These narratives follow up the EU integration processes *(Stanicek B. Caprile A., 2023)* and the US defocus from the region *(CSIS, 2021)* and, as a result, the “unfortunate feeling” of undesirability. Reinforcing this whole collage are the historical “problematic sentimental truths” that push part of the Macedonian ethnic citizenry towards so-called right-wing political narratives and the demand for a pure ethnic national identity. Albanian communities, at the same time, are targeted with stories that “the Macedonian state does not protect their rights”, which strengthens separatist sentiments *(Koldomasov A., Pylypenko A., 2024)*. When all this is added to the politicization of these issues to score political points and to cover up corruption, mismanagement, lack of transparency and lack of accountability, the trust gap in

institutions only intensifies and the space for foreign influence expands. Super amplifying this whole complex situation are the narratives that fuel the issue of Macedonian identity, using local media and influential figures to incite distrust towards official institutions *(Vatsov D. at all, 2023)*.

Local communities, especially in smaller cities, are vulnerable to false information related to the economy. Disinformation narratives often spread panic, claiming that "the EU is not bringing anything good to the country" or that "Chinese and Russian investments are more secure and profitable." When large projects (e.g. infrastructure investments) are announced, disinformation campaigns can portray them as "money laundering" or "selling out national interests." All of this, along with the weaknesses and vulnerabilities described above, undermines trust in legitimate economic reforms *("По патот на Македонија". January 11, 2025)*.

The instrumentalization of religion and traditional values is an additional complex phenomenon that, at the height of a democratic society and freedom of religion, is exploited for Foreign Information Manipulation and Interference. Religious institutions in local communities are often used as channels for the dissemination of certain disinformation, both for the purposes of certain state and certain non-state actors. This is particularly noticeable in narratives against the LGBT+ community, migrants or changes in the education system, which are presented as "Western influence destroying traditional values".

3.

THE ROLE OF THE MEDIA AND CIVIL SOCIETY IN NORTH MACEDONIA AND THE VULNERABILITY TO FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

3.1. THE ROLE OF THE MEDIA IN DEALING WITH FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

The media landscape in North Macedonia is complex and fraught with political, economic and external influences, making it extremely susceptible to foreign information manipulation and interference. Dominated by politically controlled media, dependent private television stations, online platforms with weak reporting standards and widespread disinformation on social media, the media space augments the vulnerability of the country. The media can be subject to serious political pressure, resulting in pressure which undermines their primary function as watchdog of society. At the same time, they cannot be an independent service to citizens that will provide a platform for different voices and opinions, enabling pluralism and active civic participation *(BIRN Macedonia, 2023)*.

The National Radio and Television (Macedonian Radio and Television - MRT), as the main public broadcasting service, has the potential to be an important pillar of professional and impartial journalism. However, political pressure and insufficient funding can undermine its role. Although nominally independent, MRT is often influenced by party elites *(Tuneva M., 2023)*. The lack of adequate resources is an additional challenge in the work of the public broadcaster, which limits the production of quality journalistic content and investigative journalism in the fight against disinformation *(Association of Journalists of Macedonia, 2023)*.

The dominance of political-economic interests is also present among private media. Various studies show that media outlets owned by business groups often maintain close relations with political elites. This results in media bias, self-censorship and limited space for critical journalism *(Tuneva M., 2023)*. The situation is difficult to change, and the media do not stimulate investigative and thematically oriented journalism that would strengthen professionalism and the approach, among other things, to the problem of Foreign Information Manipulation and Interference.

This setup is perfect for the strategies of anti-democratic malicious centres and proxy actors of the challengers of the Euro-Atlantic agenda. The fragmentation in regulations and the application of the laws and the intertwining of business and political interests leaves room for foreign influence through financially motivated narratives. Some

analyses indicate that it is highly likely that certain media outlets receive financial support from foreign power centres (Russia, Serbia, Bulgaria, Turkey, China), which is reflected in the aggressive promotion of their interests *(Association of Journalists of Macedonia, 2023; Pfeiffer H., 2024)*.

However, the main channel and source of disinformation is online media. The digital space and the possibility of acting remotely, in conditions of extremely problematic authenticity and the possibility of manipulation of digital identity and source, is perhaps the most vulnerable segment in the media structure. The owners and methods of financing websites are often unknown, which leaves room for easy manipulation. These websites are the largest source of sensationalist news, unconfirmed information and direct disinformation, without clear responsibilities for the published content. However, the unambiguous systematization and categorization of these media as a problem or their suppression in conditions of open markets and different interpretations of freedom of speech is extremely difficult. This can lead to errors and to incorrectly lumping media outlets in this network even when they are not. This situation increases the possibility of camouflage because their adaptation, among other things, is also aimed at feeding information chaos. In such conditions, these portals easily turn into bots and fake information factories, and through them campaigns are organized on social media (Facebook, Instagram, TikTok, X), significantly swaying public opinion through automated profiles and coordinated activities.

This leads us to another critical aspect in assessing the vulnerability of the media to Foreign Information Manipulation and Interference, i.e. the role of social media in the spread of FIMI. Social media is the largest zone of uncontrolled influence and functions as a catalyst for disinformation campaigns, as it bypasses traditional media standards and easily targets specific population groups. On Facebook, for example, there are groups that spread conspiracy theories successfully adapted to some social or geopolitical events, and they are adapted to domestic problems or the ignorance of political elites in dealing with disinformation. Thus, for example, during the time of COVID-19, anti-vaccine narratives were brought into a political context by glorifying alternative partnerships, and during the time when we became NATO members, they spread anti-NATO and anti-EU propaganda. Telegram groups, on the other hand, function as closed communities in which disinformation narratives are amplified without any control, creating the so-called echo-chamber effect of like-minded people in which any opposing opinion is rejected in advance, ideal for radicalization that can have extremist views and refer to or call to violence. This situation, combined with the politicization of every segment of society, stems from the low level of media and

information literacy. A large part of the population does not distinguish between credible sources and disinformation campaigns, which facilitates manipulation *(Institute of Communication Studies, 2024)*.

As a result of this media landscape, North Macedonia is highly vulnerable to foreign influence and disinformation campaigns. This is reflected in several key aspects:

1. polarization of society in which politically controlled media and disinformation on social media intensify social discord;

2. distrust in institutions, with citizens constantly exposed to false information and manipulative narratives, and their trust in the media and official sources declining;

3. In conditions of low awareness and capacity to deal with this form of influence, the political elites in the country have failed to build a systematic approach (no strategy or notable policy) to deal with disinformation in the past decade, which leaves the country vulnerable; and

4. unhindered promotion of foreign political and economic interests without a special state-regulated filter that would reflect the clear course of the Euro-Atlantic agenda. In this way, certain media outlets may promote agendas of third countries and directly undermine Macedonian foreign policy and the integration processes in the EU and NATO.

3.2. THE ROLE OF CIVIL SOCIETY IN ADDRESSING FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

Civil society in North Macedonia plays a critical role in the fight against Foreign Information Manipulation and Interference. However, perhaps due to an archaic approach to governance (specific to the former system of a dominant role of the state in civil society), civil society lacks the institutional support to exploit its potential to address disinformation. Non-governmental organizations, media associations, and individual experts are among the few actors that systematically analyse, expose, and

educate about disinformation. However, their impact is limited by several key challenges: low levels of media literacy, limited resources, insufficient state support, and, as previously explained, distrust in the institutions.

The low level of media and information literacy makes the public susceptible to manipulation, especially in the digital space *(Institute of Communication Studies, 2023),* which in turn deepens the vulnerability to Foreign Information Manipulation and Interference. In a time of convergence of the digital and physical worlds, education has so far failed to catch up in preparing and adapting the population to the digital space (not even the youth who are the largest users of electronic information). Although there are initiatives for media literacy, formal education should introduce more intensive education for fact-checking, digital literacy and recognition of propaganda. The habits and assumptions for consuming information from traditional media, which had built up professional authority in the past, primarily in terms of the legitimacy and reliability of the content and were taken “for granted”, are now also applied to the consumption of information from digital media. The digital jungle, in which anyone can create content and impose authority, in conditions of low levels of media and information literacy, makes citizens easy prey for economic and political predators. As a result of this unpreparedness, a large part of the population still does not possess the skills to distinguish credible sources from disinformation (Institute of Communication Studies, 2024), which allows the rapid circulation of false narratives.

Political bias is an additional factor that amplifies the danger and possibility of disinformation. The Macedonian public is highly politically polarized, meaning that people often accept information that confirms their prejudices without checking the sources. In parallel with the previous two weaknesses, the population is thirsty for sensationalism and tolerant of low journalistic standards if the content matches political affiliation or interest. Many media outlets encourage disinformation with sensationalist headlines and uncontrolled sharing of content from social media. The familiarity of language and consumption of information from sources and media from countries in the Western Balkans region can be an additional catalyst for disinformation spreading regionally *(Reporters Without Borders, 2024; Blue Europe, 2024)*. All of this affects citizens’ conscious or unconscious participation in the proliferation of disinformation, without having the capacity to identify the intentions behind those narratives.

In the absence of a strong institutional response to Foreign Information Manipulation and Interference, civil society is taking on the main role in analysing and exposing disinformation. NGOs and independent researchers have a key role in:

a) monitoring and analysis of disinformation;

b) education primarily on media literacy, although there is a segmented approach to fully incorporating information literacy; and

c) public pressure and policy advocacy.

Several civil society organizations in North Macedonia are actively working to increase the population's resilience to disinformation, especially in the digital space, raising awareness about disinformation, which also contributes to addressing Foreign Information Manipulation and Interference. Although they fill the gap in state-run media and information literacy programs, they have limited impact because they are not part of the formal education system. As a result of the USAID media literacy project "YouThink", which has been implemented for the past four years by the Macedonian Media Institute, the Institute of Communication Studies and the Youth Educational Forum, and in cooperation with the Ministry of Education and Science (MES) and the Bureau for Educational Development (BED), media literacy has been included in primary education, in mother tongue subjects in all grades. More than 8,000 teachers have been trained, and a Media Literacy Framework for Primary Education has been developed to provide basic skills and structured guidelines for integrating media literacy into the teaching process. In primary education, other subjects are also taught that cover segments of media literacy and digital literacy skills. In secondary education, however, curricula cover media as content, but without a special emphasis on media literacy. Only some of the issues related to media literacy are addressed in different subjects. In higher education, as a result of the USAID project in the past three years, elective subjects on media literacy have been introduced at 8 faculties, including those that recruit teachers for primary and secondary education. The project also contributed to non-formal education by opening media literacy clubs in 30 primary and 10 secondary schools and organizing media and journalism trainings and workshops for secondary school students and other young people, in which more than 2,000 young people were involved. However, according to the national report from the 2023 Monitoring of Media Pluralism in the Digital Era *(Micevski I., Trpevska S., 2024)*, which is being conducted in EU member and candidate countries, the extent to which media literacy is embedded in formal education is unsatisfactory, and the same conclusion can be drawn for non-formal education.

Public pressure and policy advocacy are the next mechanisms through which NGOs try to address the problem of Foreign Information Manipulation and Interference. These efforts allude to transparency in the media, improving the legal framework, holding public debates in cooperation with the media, etc.

However, one of the major challenges of the work of civil society organizations is the sustainability of their efforts. Their work often depends on a project cycle and cannot be sustainable in the long term. The manipulations that have accompanied this sector based on close relations with the authorities leave room for doubt about the independence of their work *(Klinčarski P., Gadžovska Spasovska Z., 2024)*.

Another problem and shortcoming are the lack of protection from political attacks and discrediting. Certain NGOs that expose disinformation are the target of political and media attacks, and they get accused of being foreign agents, which, together with some of the revealed corruption scandals in this sector *(Pavlovska J., 2024)*, reduces their credibility in the eyes of the public.

Another shortcoming and limitation are the fact that there is no adequate capacity or commitment to identify networks of disinformation and influence by applying certain techniques, such as OSINT – analysis of open-source information, digital forensics and analysis of algorithms. Best practices indicate that civil society can play a significant role in mapping coordinated networks of bots and manipulative media that target the Macedonian public. This indicates the need for an interdisciplinary approach, which would include security and cyber experts who have not only technical, but also security-intelligence and linguistic skills (for example, identification of manipulations through the so-called phenomenon of “data voids” or minimal, low-quality, or manipulative information from search engines when there is a high demand for information on a particular topic, but few credible sources *(Golebiewski M., Boyd D., 2019))*.

4.

CYBER CRIME AND SOCIAL MEDIA AS TOOLS FOR FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

Deliberate attempts to manipulate information by foreign actors are receiving a significant boost from technological advances. The proliferation of social media platforms and communication services allows for a greater reach of Foreign Information Manipulation and Interference, as well as a combination of new and diverse tactics, techniques, and procedures.

4.1. HOW CYBERATTACKS AND MANIPULATIVE DISINFORMATION ARE CONNECTED

Disinformation created by foreign actors incorporated into cyberattacks is considered a significant threat because it can spread malware, interfere in political processes, be difficult to detect, cause harm and incite violence. Cybercriminals collect data through targeted attacks against institutions, groups or individuals, but also use it to manipulate information and then share it. Cases of hacking and abuse of certain accounts to ensure the legitimacy of specific content or to share allegedly authentic material are just some of the examples that illustrate the connection between cybersecurity and manipulation of the information environment.

Sophisticated malicious campaigns combine disinformation and cyberattacks through:

- **The terrain** on which disinformation is distributed (social media platform, network infrastructure, redirection services). For disinformation to spread and reach its target audience, three factors are needed – social media, tools and services, and motivation, and without either of them, it cannot be "successful". Tools and services for manipulating and spreading messages through social networks are sold all over the world. Some are relatively simple (paid likes, followers, etc.), while some are more unusual some services are through online surveys, while others involve persuading administrators to remove or change some content. For these tools to be useful, social networks serve as a platform for the spread of disinformation. Given that people spend more time on social media and often use them as sources of information or news, their importance in the spread of false information cannot be underestimated. However, there is a difference between simply publishing disinformation and attracting the target audience to consume it. Spammers therefore use a variety of techniques to entice users to consume their information. Recent research shows that disinformation websites often use social platforms as enablers, but also extend beyond them, using network infrastructure and redirection services at different levels of the internet. Finally, behind disinformation campaigns there is always the question of "Why?". The motivation is sometimes simply the desire for monetary gain, and in other cases it can range from criminal to political.

- **Tactics** that integrate disinformation as part of a cyberattack package. Disinformation has become an increasingly common component of cyberattacks,

serving to deliver malware by exploiting people's emotions and fears. For example, attackers are using "fearware," a subset of data theft scams known as phishing, which rely on apprehension and misinformation, and which have become particularly prevalent during and after the Covid-19 pandemic. In addition, there is significant overlap between disinformation campaigns and cybercrime tactics, such as illegal transactions on the Darknet (a part of the internet that is accessed using special software), the use of illegally obtained documents, and various forms of fraud.

- **The goals** that lead to victims of cyberattacks also being victims of disinformation at the same time. Disinformation campaigns and cyberattacks can cause similar types of harm and can even combine to target the same victims. While data theft can compromise security by exposing sensitive information, the manipulation of that data can also have similar effects.

- **Opportunities** i.e. profitable options for both disinformation campaigns and cyberattacks. Hacking, cybercrime and influence activities often use skilled professionals as outsourcers, who receive large financial incentives. While defences against attacks can be strengthened with various commercial software, disinformation strategies can use them to damage reputations and generate profit. There are currently no serious penalties for such activities due to the complexity of their research and the lack of adequate measures to limit and block them.

Disinformation campaigns are most often carried out through social media because they are theoretically more difficult to be detected by social media platforms, and each campaign involves specific tools, such as bought followers, likes, reposts, comments, videos, etc. Much of the deceptive information is derived from conspiracy theories or political or group ideologies. Such examples include the following:

> During the 2016 presidential campaign, Donald Trump released crime statistics for the United States according to which the percentage of whites killed by whites was 16%, and of whites killed by blacks was 81%, while in reality the figures were the opposite, i.e. about 16% of whites were killed by blacks.[8]

8 See more at: https://www.washingtonpost.com/news/the-fix/wp/2015/11/22/trump-retweeted-a-very-wrong-set-of-numbers-on-race-and-murder/

Jada Fransen, deputy chairwoman of the British right-wing party Britain First, posted a video with the caption: “Muslim migrant beats up Dutch boy on crutches!” The then US President Trump shared the video, but shortly afterwards the Dutch embassy announced with facts that the perpetrator of the violent act in this video was originally from the Netherlands.[9]

Natural News, a website that usually deals with conspiracy theories, reported that “Vaccines containing mercury are ‘medical genocide’ targeting black communities to harm their babies.” By manipulating factual articles, they were trying to influence public opinion.[10]

Seattle Tribune, a fake news website that has taken and altered content from legitimate websites, shared a fake story about a “mother from Idaho sentenced to prison for breastfeeding.” The story has been shared on social media and is stirring up public debate about breastfeeding.

Disinformation campaigns have promoted fake news that 5G technology affects the immune system and that 5G spectrum bands spread Covid-19.[11]

False information about Covid-19 treatments is still spreading on social media, many of which make harmful suggestions and that using illicit drugs can “cure” the virus.[12]

9 See more at: https://www.pbs.org/newshour/politics/trump-retweets-anti-muslim-videos-from-british-far-right-leader

10 See more at: https://pmc.ncbi.nlm.nih.gov/articles/PMC9359307/

11 See more at: https://www.bbc.co.uk/bitesize/articles/zbw492p

12 See more at: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en

4.2. CYBERCRIME AND DISINFORMATION AS A RISK TO THE ECONOMIC SECTOR

False information can also pose significant cyber risks to the economic sector, as the impact of false, altered information can be magnified if it affects multiple areas of social life. Common types of false information and cyber risks that businesses should be aware of include:

- **Phishing emails,** i.e. emails that appear to be from a trusted source in order to trick the recipient into clicking on a malicious link or downloading malware. Users can also be tricked into clicking on malicious links, downloading malware, or revealing sensitive information through social media posts or other types of misinformation. Businesses can mitigate this risk by implementing strong email security measures, such as spam filters and training employees on how to identify and avoid phishing emails.

- **Malware and ransomware are types of malicious software that can infect a network or devices.** This involves manipulating visual cues in user interfaces to trick users into clicking a button or entering information into a form. Once installed, malware can steal data or lock down systems.

- **fake websites or social media profiles that contain malicious software.** Thus, fake ads are used to trick users into downloading malicious software onto their devices. In doing so, human biases, such as the tendency to trust authority or follow the crowd, are exploited to influence the decision to visit the fake websites. In this regard, businesses should implement strong cybersecurity protocols, such as two-factor authentication and access restrictions, firewalls, antivirus software, regular software updates, and employee training in cybersecurity best practices. Similar precautions can be taken to avoid cyber espionage, where attackers use false information to gather intelligence or compromise security.

- **Social engineering attacks,** such as data theft and identity theft, i.e. manipulating users into revealing sensitive information, such as login details or financial data. An example of this is financial fraud, which can promote fake investment schemes or cryptocurrency scams, which trick users into sending money or cryptocurrency to fake accounts. This can be done through fake phone calls, fake login pages, phishing emails, or social media posts that appear to be from a trusted source. To avoid social engineering, businesses should provide regular training to employees on how to identify and avoid such cases.

4.3. MECHANISMS FOR CYBERSECURITY AND PROTECTION AGAINST DISINFORMATION

The deliberate dissemination of false information with the intention of manipulating public opinion or causing harm, usually presented as disinformation campaigns, can undermine the security and reputation of an institution, group or individual.

> Governments, companies and users are becoming increasingly aware of such threats. Various government agencies are now setting up services to debunk information they believe is false. They are also considering imposing regulations and punishing sites that publish disinformation. The goals of the new regulations will include the ability to suspend bot/suspicious users and the creation of services that will allow users to report false information. Ultimately, however, the most important thing is to properly educate all users on how to identify false information.

Potential responses to dealing with cyber threats could be:

- increasing the role of cybersecurity in identifying, investigating, and preventing Foreign Information Manipulation and Interference;
- structured incident reporting between entities responsible for cybersecurity and Foreign Information Manipulation and Interference;
- exchange of information and sharing of best practices;
- promoting and facilitating cooperation between institutions and bodies at the state level;
- raising awareness and supporting capacity building.

Although detecting disinformation can be a complex task, there are certain techniques and tactics that can be used to identify potential disinformation campaigns and take appropriate actions to mitigate the risks, such as:

- placing alerts on social media and other news sources for any signs of the spread of false information, typically through the use of keywords and phrases that may be associated with the disinformation;
- verifying any information that is disseminated by checking the credibility of the source and examining the evidence presented to support the claims that are made;
- engaging all stakeholders to identify any false information being spread and address any concerns or issues that may arise;
- conducting a risk assessment to evaluate the potential impact of a disinformation campaign, which will help prepare an appropriate response;
- cybersecurity, public relations and crisis management experts to effectively detect, manage risks and respond to the disinformation campaign.

4.4 TIPS FOR PROTECTING AGAINST CYBER THREATS

Anyone who is active online takes some risk of receiving or transmitting false information or becoming a victim of identity theft or other types of abuse or cybercrime. Any information posted or shared on the Internet never disappears, cannot be completely removed, and can be the subject or target of abuse. Although various privacy settings are used, it does not necessarily mean that personal data is always safe. All of this can not only put people in online and physical danger, but can also be used to create and spread malicious messages and software. An example of where cybercriminals often go to find out important information about certain individuals is the social networking platform LinkedIn. This social networking site can provide a potential criminal with employee names, job titles, job responsibilities, and even how long the employee has been with the organization. This information can then be used by criminals to target “high-risk” employees, or even be used as part of a larger social engineering campaign. With all of this information now publicly available, people need

to be aware and educated about the risks of posting and sharing information, revealing sensitive details about themselves or an organization, and of course, knowing how to respond to potentially malicious activity and social engineering.

In general, there are two ways that hackers and cybercriminals use social engineering to abuse social networks:

1. An attempt to get someone to install software on a computer or phone that will give them access to that device.

2. To gain someone's trust for a different kind of manipulation through social networks.

People are the weakest link in cybersecurity, and any hacker will exploit that whenever possible. Here are some of the most common methods used by cybercriminals:

- Failure to use appropriate security settings on social media platforms. For example, location sharing, not limiting who has access to certain information, etc.;

- posting personal information, banking or other financial details on social media, including date of birth, phone number, address, bank account. If this information is exchanged, it should be via private messages or email;

- contact from strangers from other countries. Often, scammers try to get to know the victim and then trick them. This often happens with online dating sites. They may use social engineering to convince them that they need money, but they may also use the victim to spread malware or false information;

- With the increasing popularity of private messaging services that are part of social media, such as Facebook Messenger, private messages with a link are being sent without explanation or with a vague description of what the link may contain;

- offering an unrealistic offer. Cybercriminals use popular events and news as bait to get people to open infected emails, visit infected websites, donate to fake charities, or buy items that either don't exist or are counterfeit;

- Not changing passwords for social networks. Research shows that a large number of abuses are due to the reuse of passwords and stolen login data – 53% of social network users have not changed their passwords for more than a year, and 20% have never changed them. It is advisable to do this more often.

Finally, only by raising public awareness and the media and information literacy of citizens can proper use of social platforms and network infrastructure and good assessment of content be achieved, in order to prevent information manipulation and abuse.

5.

A BRIEF OVERVIEW OF EUROPEAN BEST PRACTICES IN DEALING WITH FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

To provide a roadmap for how North Macedonia could address Foreign Information Manipulation and Interference, this study provides a brief overview of good European practices. It should serve as an additional incentive, but also a framework that will enable a focussed approach to this phenomenon and reduce the pressure from FIMI that threatens the democratic process, institutional stability and public discourse.

5.1. SUCCESSFUL PRACTICES IN SOME EU COUNTRIES

What distinguishes successful countries in this area is their systematic and multidimensional approach, which encompasses three key aspects: (1) regulatory framework, (2) institutional capacity, and (3) public awareness and media and information literacy. This approach enables more effective handling of foreign information manipulation and interference through prevention, early detection, and rapid institutional response.

5.1.1 STRENGTHENING THE INSTITUTIONAL RESPONSE: SUCCESSFUL MODELS

In countries that have managed to build an effective defence mechanism against Foreign Information Manipulation and Interference, institutions play a key role not only in monitoring, but also in actively exposing disinformation.

Finland, for example, is known for its comprehensive defence model, where security agencies, media, civil society organizations, and educational institutions work closely together. The Finnish government, through the National Security and Supply Agency (Huoltovarmuuskeskus - HFK), regularly develops risk assessments and strategies for dealing with foreign information threats. This model shows that one of the key points for building societal resilience is the constant analysis and informing the public about potential threats.

A similar approach is being taken by Sweden, which established the Psychological Defence Centre (MPF) in 2022. This body is tasked with actively monitoring, analysing, and making recommendations for dealing with foreign information attacks. Given that North Macedonia lacks a coordinated institutional response and a dedicated unit that systematically deals with foreign information manipulation and interference, this model could be particularly significant.

On the other hand, the Czech Republic, after experiencing intensified disinformation campaigns in 2017, established a special unit to combat hybrid threats within the Ministry of Interior. This unit is composed of experts from various fields, including representatives of intelligence services, journalists, IT security experts and

psychologists. This approach to influence operations or hybrid threats provides different perspectives on the same problem, which allows the Czech Republic to provide a quick and effective response to disinformation and other forms of foreign harmful influence.

For North Macedonia, these models point to the need for a special institutional structure responsible for monitoring, analysing, and responding to disinformation. This institution should also have a mandate to cooperate with the media and CSOs.

5.1.2 REGULATORY FRAMEWORK: HOW CAN THE LAW PROTECT DEMOCRACY?

In addition to institutional capacity, regulation plays a key role in limiting the influence of Foreign Information Manipulation and Interference. In several European countries, laws have been amended to increase transparency in media financing, set clear criteria for the operation of social networks, and sanction those who intentionally spread disinformation.

In France, for example, the 2018 Law on Information Manipulation was passed, which allows state institutions to require social platforms, such as Facebook and X, to remove false content during elections. This means that disinformation campaigns do not have enough time to spread and influence the electorate.

In Lithuania, however, a law is in force that restricts the broadcasting of foreign media if they are identified as propaganda tools. The government provides financial support to independent media, thereby reducing their dependence on external sources of funding that can be politically motivated, i.e. fall into the trap of exploiting open societies and hiding foreign services behind lucrative financial investments.

In this context, North Macedonia should consider a legal framework that will increase the transparency of media ownership, especially websites, strengthen capacities for monitoring online propaganda, contribute to the sustainability and independence of the media, and provide for special mechanisms for dealing with disinformation in the run-up to elections.

5.1.3 PUBLIC AWARENESS AND MEDIA LITERACY: A KEY LINE OF DEFENCE

As the experiences of Finland and Latvia show, one of the strongest protections against Foreign Information Manipulation and Interference is education. Finland has introduced media literacy as a mandatory part of the education system, and teachers receive specialized training to educate and train students on how to analyse news, information, and recognize manipulative techniques. In Latvia, the state funds national media literacy campaigns, which include online lectures, video materials, and workshops for journalists, teachers, and students.

In North Macedonia, there is still room for development in this field. The approach to strengthening national awareness generally boils down to media literacy and depends mainly on initiatives by the civil society sector, i.e. donors. If the country follows the example of Finland, media literacy can become a systemic mechanism for reducing susceptibility to disinformation, and thus to foreign manipulation and influence, a trend that is particularly present among the young population.

***

However, in implementing these measures, North Macedonia must be mindful of the democratic balance between individual rights and public safety and good. The application of some of these measures could easily have the opposite effect. Improper implementation of such measures could lead to a threat to freedoms and rights and be the basis for absolutism.

The French Law on the Manipulation of Information, for example, while allowing for the rapid removal of false information, also creates the possibility of selective censorship, especially if the institutions that control this regulation are under political influence. In North Macedonia, there is a low level of trust in institutions and a serious politicization of almost every sector, which increases the risk that such mechanisms will be used as a tool to suppress political dissent rather than to truly oppose Foreign Information Manipulation and Interference.

Additionally, models that involve state regulation of the media space, such as the one in Lithuania, where certain media outlets are banned due to protection against propaganda, can have the opposite effect. Thus, in the case of political engineering by the ruling elite, instead of strengthening trust in institutions, it can easily be reduced or lost. If transparency is reduced or if there is selectivity based on political affiliation,

citizens, together with the opposition, can easily perceive such measures as censorship. In North Macedonia, where the public is already sceptical of government policies in the media sector, establishing mechanisms to limit certain sources can lead to additional polarization and create space for alternative, even more radical disinformation channels. Such an outcome could intensify the influence campaign and fuel the entire information chaos, in which Foreign Information Manipulation and Interference will undermine trust in democratic processes and institutions, and the bad practices of the ruling elites will be equated with EU and NATO policies.

Finally, the creation of a central body to combat disinformation, if not sufficiently independent and transparent, may only generate a new point of Foreign Information Manipulation and Interference. If North Macedonia does not pay attention to institutional impartiality, then, instead of such mechanisms helping to reduce the impact of disinformation, they may become another source of distrust, further complicating the fight against disinformation. To avoid this risk, it is necessary that these policies are developed through a broad consultative process with experts, the media and civil society, rather than being exclusively under the umbrella of state institutions.

5.2. BRIEF OVERVIEW OF BEST PRACTICES AND EXPERIENCES OF THE EU AND NATO IN DEALING WITH FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

In recent years, the EU and NATO have become aware of the serious consequences of Foreign Information Manipulation and Interference on their security, political stability and democratic processes. Hybrid threats, in particular disinformation campaigns led by foreign state and non-state actors, have required a systematic and coordinated response. As a result, several key mechanisms for dealing with FIMI have been developed, which today are among the most successful examples in the global response to information threats. This study provides an overview of three of the most

significant initiatives: the EU East StratCom Task Force (EU), the Hybrid Center of Excellence (Finland) and the EU Rapid Alert System (EU), and highlights the lessons that North Macedonia can learn from them.

5.2.1. EU EAST STRATCOM TASK FORCE

The EU East StratCom Task Force is the first organized front against disinformation. Established in 2015 within the European Union External Action Service - EEAS, it represents the EU's first attempt to systematically tackle disinformation, in particular that emanating from the Russian Federation. The main objective of this task force is to identify, analyse and expose disinformation narratives, but also to strengthen the EU's communication capacities in the Eastern Neighbourhood.

This mechanism relies on three pillars of action, namely:

1. Proactive EU communication in the Eastern Neighbourhood – through the creation and distribution of correct and verified information, East StratCom works to strengthen the positive narrative about the EU. This particularly applies to countries like Ukraine, Georgia and Moldova, which are often targets of anti-EU propaganda.

2. Monitoring and debunking disinformation – the team runs the EUvsDisinfo platform, which monitors and debunks disinformation narratives. Through detailed analysis, the platform labels fake information, explains how it spreads, and provides fact-based corrections.

3. Strengthening media literacy and the resilience of societies - East StratCom collaborates with local media, CSOs, and experts, offering fact-checking training, analytical tools, and guidance on detecting disinformation.

The following key lessons for North Macedonia emerge from this EU mechanism:

- the need for a coordinated approach between state institutions and the non-governmental sector for monitoring disinformation;

- development of a national platform for exposing manipulation and interference through foreign information (similar to EUvsDisinfo); and

- investing in professional communication of state institutions to reduce the space for manipulation.

5.2.2. HYBRID CENTER OF EXCELLENCE: HYBRID DEFENCE THROUGH STRATEGIC ANALYSIS AND COORDINATION

The Hybrid CoE, established in Finland in 2017, represents one of the most complex attempts to address hybrid threats, including foreign information manipulation and interference. The centre functions as a platform for sharing information, analysis, and expertise between NATO and EU Member States.

Unlike East StratCom, which targets specific disinformation, the Hybrid Center of Excellence has a broader mission, analysing all aspects of hybrid threats, such as economic pressures, cyberattacks, and electoral manipulation. The Center operates through three main platforms, namely:

1. Analysis of Hybrid Threats and Foreign Information Manipulation and Interference – The Center publishes detailed studies and predictions on how disinformation strategies and hybrid threats are evolving.

2. Tactical Simulations and Scenarios – The Center organizes training sessions for governments, media, and security agencies, in order to prepare them for potential information attacks.

3. Strategic capacity building - support for countries in developing national hybrid defence strategies, including measures to prevent FIMI.

Key lessons for North Macedonia regarding the Hybrid Center of Excellence are:

- development of a national centre for hybrid threats, which will analyse foreign information manipulation and interference in a broader context;

- organizing exercises for institutions based on possible scenarios, in preparation for information attacks; and

- increasing regional cooperation with NATO and the EU in the field of hybrid defence.

5.2.3. EU RAPID ALERT SYSTEM: RAPID RESPONSE TO INFORMATION THREATS

In 2019, the EU established its Rapid Alert System - RAS as part of the strategy to protect against foreign interference in elections and political processes. This system enables rapid exchange of information between member states, with the aim of identifying and limiting disinformation campaigns in real time.

The system works as follows:

- Member States immediately exchange data on identified disinformation operations;
- Advanced digital tools are used to monitor social media and sites that spread disinformation;
- Information is shared with platforms such as Facebook, X and YouTube, which are obliged to act on the conclusions of the EU's Rapid Alert System (RAS).

Good practices that can be applied in North Macedonia are:

- establishment of an inter-institutional mechanism for rapid exchange of information on Foreign Information Manipulation and Interference;
- strengthening the collaboration with global platforms to reduce the impact of disinformation in the online space; and
- development of a local monitoring system that will provide early warning of potential disinformation campaigns.

RECOMMENDATIONS FOR CREATING POLICIES TO DEAL WITH FOREIGN INFORMATION MANIPULATION AND INTERFERENCE IN NORTH MACEDONIA

To effectively address Foreign Information Manipulation and Interference, a holistic approach is needed that encompasses the institutional, regulatory, and societal aspects of this threat. The following policy recommendations are aimed at strengthening national resilience and reducing the impact of disinformation on security, the media landscape, and public discourse.

1. INSTITUTIONAL STRENGTHENING AND COORDINATION

- Establishing a National Center for Monitoring and Analysis of Foreign Information Manipulation and Interference, which will unite institutional efforts to monitor, investigate, and respond to foreign disinformation operations.
- Establishing an inter-institutional working group with representatives from the Government, security services, media regulators and civil society for regular exchange of information and best practices.
- Improving crisis communications mechanisms, especially in cases of increased disinformation campaigns related to elections, national security, or health and social issues.
- Improving the capacities of security institutions for intelligence analysis of disinformation and developing tools for detecting organized campaigns.
- Depoliticization of public administration and the security sector and strengthening integrity in the management of state and administrative bodies through a professional, responsible and transparent approach in line with democratic principles of governance

2. LEGAL AND REGULATORY MEASURES

- Revising the existing legal frameworks for disinformation, clearly defining the line between freedom of expression and harmful manipulation of information.
- Strengthening oversight of online platforms through increased transparency of funding and political advertising.
- Obligation to identify sources of media funding, in order to prevent foreign influence through online media ownership or covert networks of disinformation.
- Integration of European and NATO recommendations for combating disinformation into national regulation, alignment with the EU Action Plan against Disinformation and improvement of accountability mechanisms.

3. STRENGTHENING MEDIA RESILIENCE AND TRANSPARENCY

- Support for the development of independent fact-checking centres, which will cooperate with the media and have an official role in exposing disinformation campaigns.
- Increasing transparency in the work of the media, through obligations to disclose ownership and oversight of the financing of online platforms.
- Advancing the public broadcasting service and independent media by promoting professional journalism and countering the spread of disinformation.

4. BUILDING SOCIAL RESILIENCE AND MEDIA LITERACY

- Maintaining and promoting media and information literacy in the education system through educational programs for students on critical thinking and dealing with disinformation.
- Support for public campaigns against disinformation, which will educate citizens about the techniques of information manipulation and the importance of checking sources.

- Stimulating research and academic analysis to develop strategies to combat foreign information manipulation and interference, with particular emphasis on the local context and specific vulnerabilities of North Macedonia.

5. INCREASING INTERNATIONAL COOPERATION

- Deepening the partnership with NATO and the EU through participation in joint initiatives for data exchange, intelligence analysis, and strategies to combat foreign information manipulation and interference.

- Strengthening cooperation with international organizations and research centres, such as the NATO StratCom CoE, the Hybrid CoE and the EU East StratCom Task Force, to gain access to analytical tools and methodologies.

- Developing regional mechanisms for information exchange with neighbouring countries, as Foreign Information Manipulation and Interference often transcends national borders and has transnational implications.

These recommendations aim to create a stronger foundation for protecting the Macedonian society from foreign manipulative influences and disinformation. Through a strategic approach that includes institutional strengthening, legal reforms, media resilience, public education, and international cooperation, the state can reduce its vulnerability to foreign information manipulation and interference and strengthen its democratic capacity to defend against hybrid threats.

CONCLUSION

Foreign Information Manipulation and Interference (FIM) pose a significant threat to national security, democratic processes and public trust in North Macedonia. As a NATO member state and an EU candidate country, the country is exposed to various forms of hybrid threats, including organized disinformation campaigns, media manipulation and cyber -attacks that aim to undermine its institutions, increase political polarisation and weaken its strategic direction towards Euro-Atlantic integration.

This study identified key methods used by various actors to influence the Macedonian information environment, including the creation and dissemination of false narratives, misuse of digital media, and coordinated campaigns targeting specific social groups. The study suggests that Foreign Information Manipulation and Interference affects multiple spheres – the social, media, and cyber spheres, and that there are systemic vulnerabilities that allow such threats to be effective. Insufficient media literacy, low levels of trust in institutions, lack of rapid response mechanisms, and limited capacities for monitoring and analysing digital spaces represent critical points exploited in these manipulative processes.

Existing policy and regulatory frameworks in NATO and the EU provide guidance and mechanisms for addressing FIMI, but their implementation in North Macedonia is still under development and requires further improvement. The comparative analysis showed that some EU countries have established more effective models for addressing foreign information manipulation, which can serve as an example for building a more resilient institutional and societal mechanism.

In order to strengthen national resilience to foreign information manipulation and interference, this study recommends a multidimensional approach that includes strengthening institutional capacity for detection and response to disinformation, depoliticization of the professional security sector and public administration, improvement of regulations for accountability, transparency and integrity of the media, as well as raising public awareness through education on media and information literacy. Also of particular importance is the enhanced cooperation with international partners, in particular with NATO and the EU, in order to share information, good practices and technical capacities to deal with this type of hybrid threats.

North Macedonia faces a complex and dynamic challenge when it comes to Foreign Information Manipulation and Interference, but with appropriate strategic policies, institutional reforms, and enhanced public awareness, the country can reduce the impact of foreign manipulative operations and build a more resilient democratic society. Combating disinformation and hybrid threats is not only a security issue, but also a key element for protecting democratic values and the country's Euro-Atlantic future.

ABOUT THE AUTHORS

Dr. Metodi Hadji-Janev is an Associate Professor at the Faculty of Law, University of Goce Delchev – Shtip and the Military Academy "General Mihailo Apostolski" - Skopje, and an Adjunct Faculty Member at Arizona State University's Ira A. Fulton School of Engineering. With international teaching and consulting experience, his expertise lies in digital governance, risk and compliance (GRC), cybersecurity and cybercrime, data privacy, e-commerce and utilization of technological tools and platforms to enhance transparency, accountability, effectiveness, efficiency and good governance. Hadji-Janev has advised numerous regional initiatives (Southeast European, including Moldova and Georgia) and international organizations, including USAID, the U.S. State Department, EU, NATO, RCC (Sarajevo-based) and RACVIAC (Zagreb-based), focusing on capacity building, stakeholder engagement, and implementation of Governance, Risk and Compliance (GRC) strategies. His work bridges the public, academic, and private sectors to foster good governance, transparency, and digital innovation. He is also involved in high-level evaluation work with institutions such as the European Commission, the European Science Foundation and the Slovak Research and Development Agency and contributes to the Harvard-led Global Safety Evaluation Network.

Dr. Marjan Stoilkovski is the Head of the IT Security Department at NLB Bank in North Macedonia. Previously, he served for 15 years as the Head of the Department for Cybercrime and Digital Forensics at the Ministry of Internal Affairs of North Macedonia. He has over 13 years of experience as an international expert in cybersecurity, cybercrime, digital forensics, and electronic evidence. He has completed more than 80 international activities in the field of strengthening capacities for cybersecurity and cybercrime as part of project activities organized by the Council of Europe, the European Commission, the United Nations, the OSCE, and other international institutions and organizations. His current academic and professional focus is in cybersecurity, specifically the implementation and testing of security solutions, preparation and execution of practical Tabletop Exercises, incident management and digital forensics, SOC managed services, and malware analysis. His additional research includes virtual assets in terms of analysis and regulation, open-source intelligence (OSINT, including the Darknet), and the use of AI in operational cybersecurity activities.

REFERENCES

- Association of Journalists of Macedonia (2023). Media Freedom in North Macedonia : Fragile Progress, available at: https://znm.org.mk/wp-content/uploads/2023/10/%D0%9C%D0%9A-Fact-Finding-PFM-Report-251023-web.pdf
- BBC. 5G and coronavirus : Debunking the fake news stories, available at: https://www.bbc.co.uk/bitesize/articles/zbw492p
- BIRN Macedonia (2023). Media Ownership Monitor – North Macedonia, available at: https://north-macedonia.mom-gmr.org/mk/
- Blue Europe (2024). Challenges of Chinese Soft Power in Western Balkans, available at: https://www.blue-europe.eu/analysis-en/short-analysis/challenges-of-chinese-soft-power-in-western-balkans/
- Boulianne Sh., Humprecht E, (2023), Perceived Exposure that Misinformation and Trust in Institutions in Four, Countries Before and During a Pandemic, International Journal of Communication 17, available at: https://hal.science/hal-04126541/document
- CERT – EU (2024), Threat Landscape Report 2023, available at : https://cert.europa.eu/publications/threat-intelligence/tlr2023/
- Corporate Finance Institute (2023), Platform Company, available at: https://corporatefinanceinstitute.com/resources/valuation/platform-company/
- CSIS, (2021), Reimagining US Policy towards the Western Balkans, available at: https://www.csis.org/programs/europe-russia-and-eurasia-program/archives/european-security-politics-and-economics-1
- Diamond L., McDonald J. (1996). Multi-Track Diplomacy : A Systems Approach that Peace. Third Edition. West Hartford, CT: Kumarian Press.
- Disinformation. available at: https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
- Deutche Welle (2024), “What is foreign information manipulation and interference?”, available at: https://akademie.dw.com/en/what-is-foreign-information-manipulation-and-interference/video-68790017
- EU COMMISSION STAFF WORKING DOCUMENT, North Macedonia 2023 Report, available at: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf
- EU Commission, NIS2 Directive: new rules on cybersecurity of network and information systems, available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- EU Commission, (Brussels, 8.11.2023), North Macedonia 2023 Report, Commission Staff Working Document, available at: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf

- EUEA (2023), 1st EEAS Report on Foreign Information Manipulation and Interference Threats, The Diplomatic Service of the European Union, available at: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
- EUEA (2025), Inside the infrastructure of Foreign Information Manipulation and Interference (FIMI) operations, available at: https://www.eeas.europa.eu/eeas/inside-infrastructure-foreign-information-manipulation-and-interference-fimi-operations_en
- European Commission. Separating facts from fiction on vaccines, available at: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en
- Golebiewski M., Boyd D. (2019). Data Voids: Where Missing Data Can Easily Be Exploited. Data & Society, available at: https://datasociety.net/library/data-voids/ https://www.facebook.com/photo.php?fbid=1101727971749705&id=100057375372607&set=a.285088090080368&locale=tr_TR
- Hubervic A., Prudent Y., for Enabling Alliance Interoperability and Pervasive M&S Applications. NATO Science and Technology Organisation (STO), available at: link
- Jacob Marusic S., (2022). Forget Sputnik. Russian Propaganda Has other Paths into North Macedonia, BIRN, available at: https://balkaninsight.com/2022/04/22/forget-sputnik-russian-propaganda-has-other-paths-into-north-macedonia/
- Kelly S, Truong M., Shahbaz A., Earp M., White J. (2017). Manipulating Social Media that Undermine Democracy, Freedom House, available at: https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy
- Koldomasov A., Pylypenko A., (2024). How Russia Uses Propaganda That Hinder the Integration of Western Balkans Countries Into the EU. Detector media, available at: https://en.detector.media/post/how-russia-uses-propaganda-to-hinder-the-integration-of-western-balkan-countries-into-the-eu
- Miguel R., (2024). Decoding FIMI: a complex interrelation with disinformation, The ATHENA Newsletter, available at: https://project-athena.eu/decoding-fimi-a-complex-interrelation-with-disinformation/
- PBS News (2017). Trump retweets anti-Muslim videos from British far-right leader, available at https://www.pbs.org/newshour/politics/trump-retweets-anti-muslim-videos-from-british-far-right-leader
- Reporters Without Borders (2024). From Russia to Serbia: How RT Spreads the Kremlin's Propaganda in the Balkans Despite EU Sanctions, available at https://rsf.org/en/russia-serbia-how-rt-spreads-kremlin-s-propaganda-balkans-despite-eu-sanctions
- Skafle I., Nordahl-Hansen A., Quintana D., Wynn R., Gabarron E. (2022). Misinformation About COVID-19 Vaccines him Social Media: Rapid Review. Journal of Medical Internet Research, available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC9359307/
- Stanicek B. Caprile A., (2023). Russia and the Western Balkans Geopolitical confrontation, economic influence and political interference. European Parliamentary Research Service, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/747096/EPRS_BRI(2023)747096_EN.pdf

- The Cybersecurity and Infrastructure Security Agency (CISA) (2023). Tactics of Disinformation. available at: https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
- The Diplomatic Service of the European Union, (2025) “Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)” available at: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
- Tuneva M. (2023). Between challenges and solutions - A Guide to Media Integrity in North Macedonia”, UNDP, available at: https://dksk.mk/wp-content/uploads/2024/01/Media_Integrity_Guide_en-final.pdf
- Vatsov D., Dimitrova V., Donchev Lj., Valkanov V., Iakimova M, (2023). The Pro-Russian Propaganda Machine in Bulgaria, and the Russian Style Representations of North Macedonia. Identities: Journal for Politics, Gender and Culture, available at: https://identitiesjournal.edu.mk/index.php/IJPGC/article/view/530ч
- Walker Sh., Simeone M. (2020), Misinfo, Bots, and Trolls - Some Key Concepts for Misinformation, ASU Podcast, S1.E6, available at: https://lib.asu.edu/misinfo-weekly/misinfo-bots-and-trolls-some-key-concepts-misinformation
- Washington Post (2015). Donald Trump retweeted a very wrong set of numbers on race and murder, available at: https://www.washingtonpost.com/news/the-fix/wp/2015/11/22/trump-retweeted-a-very-wrong-set-of-numbers-on-race-and-murder/
- Agency for Audio and Audiovisual Services (AAVMS). Media Literacy Network - https://mediumskapismenost.mk/
- Analysis of profiles active on social media. For example, “По патот на Македонија” (January 11, 2025), available at:
- “Official Gazette of the Republic of North Macedonia” No. 152/2019 and 275/2019)
- Vistinomer, (2023). Putin repeated on the Red Square the main disinformation narratives – Russia is a victim and defended itself!, available at: https://vistinomer.mk/putin-na-crveniot-ploshtad-gi-povtori-glavnite-dezinformaciski-narativi-rusija-e-zhrtva-i-se-branela/
- Government of the Republic of North Macedonia (2024), available at: https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=51471
- Government of the Republic of North Macedonia, (2021), “„Стратегијата за градење национална отпорност и справување со хибридни закани” (Strategy for Building National Resilience and Addressing Hybrid Threats), available at: https://mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf
- European Commission, Commission Staff Working Document, 2021 Report on North Macedonia, Strasbourg, 19.10.2021, Assembly of the Republic of North Macedonia
- EEA (2023). “Beyond Disinformation - What is FIMI?”, available at: https://www.eeas.europa.eu/eeas/beyond-disinformation-what-fimi_en#:~:text=Tackling%20Disinformation%2C%20Foreign%20Information%20Manipulation,democratic%20processes%2C%20security%20and%20citizens

- Law on Electronic Communications ("Official Gazette of the Republic of Macedonia" No. 39/2014), 188/2014, 44/2015, 193/2015, 11/2018 and 21/2018 and "Official Gazette of the Republic of North Macedonia" No. 98/2019 and 153/2019
- Law on Personal Data Protection ("Official Gazette of the Republic of North Macedonia" No. 42/20)
- Law on Amendments to the Law on Personal Data Protection ("Official Gazette of the Republic of North Macedonia No. 294/21)
- Law on Criminal Procedure ("Official Gazette of the Republic of North Macedonia" No. 150/10, 100/12, 142/16 and 198/18)
- Law on Justice for Children ("Official Gazette of the Republic of Macedonia" No. 148/2013)
- Law on Interception of Communications ("Official Gazette of the Republic of North Macedonia" No. 71/18)
- Law on Audio and Audiovisual Media Services (consolidated text) (Official Gazette No. 184/2013, Official Gazette No. 13/2014 and Official Gazette No. 44/2014), available at: Zakon-za-Audio-i-audiovizuelni-mediumski-uslugi-prechisten-tekst-na-memorandum.pdf
- Law on Child Protection, "Official Gazette of the Republic of Macedonia" No. 23/2013, 12/2014, 44/2014, 144/2014, 10/2015, 25/2015, 150/2015, 192/2015, 27/2016, 163/2017, 21/2018 and 198/2018 and "Official Gazette of the Republic of North Macedonia" No. 104/2019, 146/2019, 275/2019, 311/2020 and 294/2021)
- Institute of Communication Studies (2023). Vulnerability to disinformation among different groups of citizens in North Macedonia. Res publica, available at: https://iks.edu.mk/istrazuvanja-analizi/ranlivost-na-dezinformacii-kaj-razlichni-grupi-gragjani-vo-severna-makedonija/
- Institute of Communication Studies (2024). Citizens' practices and perceptions regarding information and dealing with disinformation. ResPublika, available at: https://iks.edu.mk/istrazuvanja-analizi/praktiki-i-percepcii-na-gragjanite-vo-pogled-na-informiranjeto-i-spravuvanjeto-so-dezinformaciite/
- Jakimova J., (2022), "When there is no trust in the state - oil is hoarded and vaccines are refused", Radio Free Europe, available at: link
- Klinčarski P., Gadžovska Spasovska Z. (2024), State money for NGOs in the hands of some of DUI's public sector employees, Radio Free Europe, available at: https://www.slobodnaevropa.mk/a/drzhavni-pari-za-nevladini-vo-racete-na-del-od-administrativcite-na-dui/32788912.html
- Criminal Code ("Official Gazette of the Republic of North Macedonia" No. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017, 248/2018 and number 36/23
- MIA, (April 9, 2022), "Petrovska: No strategy for hybrid threats can be fully implemented if all actors in the state do not participate in it", available at the link
- Ministry of Defence (2020) Cyber Defense Strategy, available at: https://mod.gov.mk/inc/uploads/2021/06/Strategija-za-sajber-odbrana-mk-1-1.pdf

- Micevski I., Trpevska S. (2024). Monitoring Media Pluralism in the Digital Era - Application of the Media Pluralism Monitor in EU Member States and Candidate Countries in 2023 - National Report: Republic of North Macedonia. Research Institute on Social Development – RESIS, available at: https://cadmus.eui.eu/bitstream/handle/1814/77022/North_Macedonia_MK_mpm_2024_cmpf.pdf?sequence=2&isAllowed=y

- Pavlovska J. (2024). Во спиралата на криминалот: Ред проневера, ред корупција и сè одново и повторно (In the spiral of crime: Embezzlement on top of corruption in an endless stack), Nova Makedonija, available at: https://novamakedonija.com.mk/pecateno-izdanie/vo-spiralata-na-kriminalot-red-pronevera-red-korupcija-is%D1%90-odnovo-i-povtorno/

- Pfeifer H. (2024). Разоткриена мрежа за руска пропаганда во Европа (Russian Propaganda Network Exposed in Europe), Deutsche Welle, available at: https://www.dw.com/mk/razotkriena-mreza-za-ruska-propaganda-vo-evropa/a-68698125

Institute of communication studies

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

НЕ ВЕРУВАЈ ПРОВЕРУВАЈ! #користифакти

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This product was prepared within the scope of the „Fact-Based Journalism for Raising Awareness and Countering Disinformation in the Media Space in North Macedonia" project, funded by the Government of the United Kingdom, with the support of the British Embassy Skopje. The opinions and views expressed herein do not necessarily reflect the opinions and views of the British Government.

Institute of communication studies

НЕ ВЕРУВАЈ
ПРОВЕРУВАЈ!
#користифакти