New Security Threats Institute

Recommendations to future Parliamentarians on responses to FIMI: A selection of case studies

SLOVAKIA

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

September 2024

This report has been prepared with support from IRI's Beacon Project. The opinions expressed are solely those of the author and do not reflect those of IRI.

New Security Threats Institute (NEST Institute) is a Slovakia based think-tank analyzing current security threats impacting safety and security of democratic societies with a particular focus on hybrid threats, FIMI and disinformation. www.nest-institute.org.

Whenever the term FIMI is used in the text of the report it is used as part of a broader issue of hybrid threats, since the term FIMI itself is not used anywhere in Slovak public policies nor legislation.

Authors: Domician Zahorjan, Patrik Haburaj, Daniel Milo

Recommendations to future Parliamentarians on responses to FIMI: A selection of case studies

SLOVAKIA

1. Executive Summary

Slovakia is one of the most vulnerable countries in the EU to Foreign Information Manipulation and Interference (FIMI) and foreign hostile influence. This is evidenced not only by various public opinion polls showing high acceptance of Kremlin narratives in Slovakia, but also by the use of foreign (mostly Russian) narratives by domestic political actors, including members of parliament and the government.

The situation regarding legislation, institutions, and public policies dedicated to FIMI is rather bleak. There is virtually no effective legislation in place to counter FIMI, and the Slovak legislative system lacks any definition of the basic terms and concepts related to it. While the first public policies addressing FIMI date back to 2017, their real implementation only began after the full-scale Russian invasion of Ukraine in 2022. Moreover, the newly created institutional capacities were not sustained, and after the change of government in September 2023, most were disbanded, weakened, or rendered ineffective.

The primary obstacle to implementing effective measures against FIMI and hybrid threats in Slovakia is the current government's denial of their necessity. This resistance stems from adoption of pro-Russian narratives promoted by disinformation actors, alongside with viewing such measures as censorship. Without acknowledging the issue, the government lacks motivation to develop or enforce strategies to counter these threats.

There is ample evidence of Russia-originated FIMI and other forms of hybrid influence in Slovakia. This includes the activities of pro-Russian motorcycle groups acting in close coordination with the Russian embassy, meetings between Slovak citizens and Russian operatives, and high-profile cases of information operations involving Russian entities in Slovakia.

Given the current situation, Slovakia is fertile ground for FIMI. Foreign hostile actors, such as Russia, are highly likely to make further inroads to influence public perception and the political landscape in Slovakia. The Ukraine war fatigue, euroscepticism, fears of migration, and the protection of so-called traditional values will be exploited to advance Russia's strategic goals.

Recommendations:

Legal area:

- Prepare legislation to combat hybrid threats and FIMI, including clear definitions and penalties.
- Specify responsibilities and competencies for coordinating the response to hybrid threats, including FIMI.
- Enact legislation to establish a standing parliamentary committee on FIMI and hybrid threats. This committee would serve as a key body without risking politicization.

Public Policies:

- Implement existing strategic and conceptual documents, providing strong political support and enforcement mechanisms. Build consensus around the understanding of these documents.
- Standardize cooperation with the academic sector and private companies to counter FIMI. Involve civil society in shaping public policy, countering FIMI, and building resilience.

Institutional Framework:

- Consider creating a government position with a comprehensive security mandate, such as a national security advisor, to ensure political support in addressing hybrid threats.
- Establish dedicated units for combating hybrid threats and managing strategic communication within relevant state institutions, with sustainable long-term funding.
- Appoint a lead institution to coordinate stakeholders in both long-term activities and rapid responses to hybrid operations.
- Ensure political support for this area and educate state officials who often misunderstand the issue. Increase awareness and understanding of FIMI among politicians.

2. Introduction to the topic of countering FIMI on national level

2.1. Legislative Framework

The primary challenge in legally regulating FIMI in Slovakia is the absence of a clear legal framework or definitions for key terms within the FIMI concept. As FIMI is a relatively new issue in Slovakia, it is not addressed in existing legislation or by dedicated public policies.

While some related terms appear in public policies, these are non-binding and should be codified into law. Currently, the Slovak legal system lacks definitions for critical terms such as: Hybrid threat, Disinformation, Misinformation, Malinformation, Information operation, Influence operation etc.

This lack of clear terminology creates difficulties in applying existing laws to regulate or penalize activities related to FIMI. For example, when the Act on Cyber Security No. 69/2018 Coll was amended in February 2022 to include website blocking for "serious disinformation and other hybrid threats," no legal definitions were provided for these terms, leading to enforcement challenges.

Similarly, other legislation, such as the Act on Military Intelligence No. 500/2022 Coll. and the amendment to Act No. 110/2004 Coll. on the functioning of the Security Council of the Slovak Republic (BR SR), references hybrid threats and disinformation without offering legal definitions, complicating their practical application.

The only FIMI-related terms currently defined in Slovak law are "foreign power" and "foreign agent," as outlined in article 133 of the Criminal Code No. 300/2005 Coll. These terms apply specifically to criminal acts:

- Foreign power - refers to foreign states, their military or other groupings, including intelligence agents, military officials, diplomats, and other civil servants;
- Foreign agent - a natural person or legal entity with significant influence due to their political, economic, or social status, but not directly representing a foreign state.

However, since most FIMI activities are not criminal in nature, the relevance of these definitions is limited and they are rarely used in practice.

2.2. State institutions responsible for countering and analysing FIMI

State actors in Slovakia responsible for hybrid threats, including countering FIMI:

National Security and Analytical Centre of the Slovak Intelligence Service: This key entity is responsible for monitoring and analyzing information on hybrid threats and serves as a point of contact for hybrid threats at the national level.

Situational Center of the Government Office: Acts as a national contact point for hybrid threats, prioritizing cooperation with the Hybrid Fusion Cell. However, this responsibility is currently being transferred to the National Security and Analytical Centre.

Strategic Communication Department of the Government Office: Department is responsible for coordinating strategic communication at the national level in line with the strategic communication concept. However, current staffing limitations hinder the professional and effective preparation of strategic communication.

Center for Countering Hybrid Threats of the Ministry of Interior: This center is primarily responsible for prevention, monitoring, awareness, analysis, and proposing measures within the Ministry of Interior's scope. However, due to a lack of understanding of the issue's severity within the ministry, the center's activities are currently significantly limited.

Strategic Communication Department of the Ministry of Defense: After the last parliamentary elections, the ministry's leadership reassessed the mission of its specialized unit dealing with hybrid threats, which now continues only as the Strategic Communication Department. The Ministry of Defense, through the Armed Forces of the Slovak Republic, participates in international exercises and collaborates with NATO and the EU to strengthen resilience against hybrid attacks.

Cyber and Hybrid Threats Department of the Ministry of Foreign and European Affairs: This department is also responsible for an agenda related to increasing resilience at the EU level and partially within NATO.

Hybrid Threats and Disinformation Unit of the National Security Authority: This government body plays a key role in cybersecurity and the protection of critical infrastructure. It systematically monitors, evaluates, analyzes, and responds to information operations.

Strategic Priorities Department of the Ministry of Education: This department monitors hybrid threats in the education, research, and development sectors. Both the Strategic Priorities Department and the Strategic Communication Unit focus on increasing resilience against these threats.

2.3. Role of the Parliament in Countering FIMI

There is no specific committee within the National Council of the Slovak Republic (hereafter NRSR) dedicated to addressing FIMI or related issues. The broader issues included in the FIMI concept fall under three NRSR committees:

- **Committee on Culture and Media**: This committee oversees media, culture, and information policy in Slovakia. It is directly involved in areas such as media regulation, protection against disinformation, and combating propaganda, all of which are crucial to FIMI. The committee reviews laws related to the media environment, including measures aimed at countering disinformation.
- **Committee on Foreign Affairs**: This committee is responsible for overseeing Slovakia's foreign policy and international relations. It focuses on foreign influence and propaganda, often linked to FIMI, particularly in the context of international security and the protection of national interests. The committee also addresses legislative proposals related to hybrid threats.
- **Committee on European Affairs**: This committee oversees the government's activities in EU matters, ensuring alignment with national interests. It reviews and approves Slovakia's positions on EU acts and major issues, mandates government representatives to adhere to these positions during EU negotiations, and assesses the compatibility of EU legislative proposals with the principle of subsidiarity.

Although FIMI falls under the remit of the committees mentioned above, none of them have held meetings in the past two years to specifically address FIMI-related issues, hybrid threats, or disinformation. These topics have only been raised in the context of specific agenda points or questions from committee members.

Therefore, there is no public record of parliamentary committees dedicating any of their sessions or adopting resolutions to FIMI related issues, despite the significant presence of FIMI in Slovakia. Interestingly, the only sporadic mentions of disinformation or hybrid threats in committee meetings occurred between 2020 and 2023. As of September 2023, when the current parliament was enacted, there has been no mention of these issues.

Regarding FIMI-related bills passed by Parliament, the analysis of legislation outlined above applies. There is no specific bill, nor definitions of the most important terms in the legal system of Slovakia.

2.4. Timeline of Key Developments

2017: Government begins **developing policies against hybrid threats** after the EU adopts its first measures within a joint framework in 2016.

2018: Slovakia adopts the **Strategy for Combating Hybrid Threats**, defining major threats and proposing an initial institutional framework to address them.

2021: Government approved crucial strategic documents:

- The **Security Strategy of the Slovak Republic** identifies disinformation and propaganda as major hybrid threats, including FIMI.
- The **Defense Strategy of the Slovak Republic** emphasizes the need to strengthen the state's resilience to FIMI and hybrid threats.

2022: Two major developments in hybrid threats and countering FIMI:

- The adoption of the **Action Plan for Coordinating the Fight Against Hybrid Threats** for 2022-2024, which sets up more than 50 specific measures to counter hybrid threats and build resilience.
- The realization of the national project "**Enhancing Slovakia's Resilience to Hybrid Threats by Strengthening Public Administration Capacities**", supported by European funds. This project created new structures and capacities for addressing hybrid threats and countering FIMI.

2023: The first Strategic document on **strategic communication** is adopted, focusing on improving state communication with the public and combating disinformation.

2024: After parliamentary elections in 2023, government:

- approves the updated Strategic document on **strategic communication** to ensure more effective communication between the state and the public, replacing the 2023 concept. This update excludes the civic sector from any participation in this area and reduces previous cooperation among ministries to a minimum.
- proposes a new **Strategy on Countering Hybrid Influence**. The proposal has not yet been approved as of the end of August.

3. Evolution and dynamics of analyzing, reporting on and countering FIMI

3.1. Key Topics, Narratives, and Domains Targeted by Hostile Actors

Since the beginning of Russia's full-scale invasion of Ukraine, narratives reflecting current political or social events have spread in Slovakia, particularly those with characteristics of FIMI:

- Nazis are in power in Ukraine.
- Ukraine is developing biological weapons.
- Military aid to Ukraine prolongs the war.
- Sanctions harm the EU more than Russia.
- NATO membership endangers Slovak citizens.
- Military aid to Ukraine will lead to a confrontation between NATO and Russia.
- The Ukrainian president is illegitimate because there were no presidential elections in Ukraine.
- Russia protects traditional values.

The spread of these narratives in the information space was supported by specific activities. For instance, at the beginning of 2023, disinformation regarding an alleged mandatory mobilization of men for deployment in the conflict in Ukraine began circulating in Slovakia. This caused widespread uncertainty among citizens and led to more than 40,000 men refusing potential service in the armed forces.

Subsequently, so-called "Marches for Peace," which carried pro-Russian sentiments, were organized on a large scale. These events received substantial support from Russian propaganda.

Additionally, the motorcycle group "Brother for Brother" has become a significant channel for pro-Kremlin narratives and serves as a tool of Russian hybrid influence in Slovakia. This group is linked to the "Night Wolves", a Russian nationalist motorcycle club with ties to the Kremlin. Under the guise of caring for memorials to fallen Red Army soldiers, “Brother for Brother” promotes Russian imperial ideology, promotes the strategic interests of the Russian Federation, and maintains regular contact with its representatives.

3.2. Gaps Exploited by Hostile Actors in the Inf. Space, Legal System and Media

Social:

There is no doubt that foreign hostile actors, primarily Russia, are attempting to use FIMI to influence the views, opinions, and political orientations of Slovakia and its citizens. Due to historical, socio-economic and cultural factors, Slovakia has been one of the most pro-Russian countries in the Central and Eastern Europe (CEE) region, as illustrated by Globsec Trends and other public opinion polls. This favorable perception of Russia creates an opportunity for furthering such views and increasing Russian influence.

The polarization of Slovak society and belief in disinformation remain high. In 2022, survey showed that 54% of Slovaks believed in conspiracy theories or disinformation. A 2023 survey revealed that 50% of citizens distrusted state institutions. The government lacks a concept for building social cohesion, and there are no principles or structures to ensure strategic governance in the Slovak Republic. This situation leaves the high polarization of society unaddressed, leaving it vulnerable to FIMI.

Information space:

Since 2014, following Russia's annexation of Crimea, Slovakia has faced increased hybrid threats, with disinformation campaigns targeting the population primarily through social media. International crises, such as the COVID-19 pandemic and Russia's invasion of Ukraine, have intensified this trend. The strategic communication of the state is largely formal and ineffective in practice, leaving the information space vulnerable to FIMI interference due to the absence of a counter-narrative.

Quasi-/alternative, or traditional media used by the hostile actors:

There is a significant influence of Telegram channels and other quasi-media projects that disseminate disinformation content. These quasi-media projects and disinformation channels are often utilized by government officials and high-level politicians (e.g., the prime minister or government ministers) to promote their political agendas. Such activities increase the credibility and influence of disinformation channels in the information space, leading to their legitimization. At the same time, politicians undermine the credibility of mainstream media by deliberately bypassing these outlets.

Legal system gaps:

Absence of a clear legal framework or definitions for key terms within the FIMI concept, as mentioned above, remains a challenge in Slovakia. Furthermore, the lack of legislative anchoring for competencies and the designation of primary responsibility for countering hybrid threats has resulted in a slow and inadequate response from state administration against FIMI. Additionally, the government has been unable to adopt legal tools to counter FIMI, such as failure to implement a sustainable solution for blocking websites with proven links to hybrid actors following Russia's full-scale invasion of Ukraine in 2022.

3.3. Connections Between Local and External Actors in Hybrid Threats

Over the years there have been many specific examples illustrating the nature of those links. While many such cases are classified and never exposed to the public, below is a list of several notorious examples of connections between local actors and external (Russian) ones:

- **Night Wolves and Jozef Hambálek**: The "Night Wolves", a Russian nationalist motorcycle club with ties to the Kremlin, established a base in Slovakia with the help of Jozef Hambálek, a Slovak businessman, who was for his activities until recently on the EU sanctions list. This collaboration signifies a direct link between local Slovak actors and Russian influence operations, as the "Night Wolves" are known for their propaganda and support of Russian foreign policy objectives.

- **Peter Garbar and the Russian spies**: Peter Garbar, a Slovak individual, was involved in espionage activities that benefited Russian intelligence. He was caught on camera receiving a bribe from a Russian military intelligence officer who requested sensitive and classified information. He was subsequently charged and sentenced for espionage. This case underscores the infiltration of Slovak institutions by Russian spies, facilitated by Slovak citizens, thus compromising national security and demonstrating Russia's strategic interest in Slovakia.

- **Cintorín Ladomírová Information Operation**: This case involves a disinformation campaign centered around the military cemetery in Ladomírová. Russian actors, with the aid of local Slovak collaborators, spread false information on the alleged desecration of the cemetery to manipulate public sentiment. This operation exemplifies the use of local proxies in Russia's broader hybrid warfare tactics.

- **Brother for Brother:** As mentioned previously, this motorbike club based in northern Slovakia, promotes pro-Russian sentiments and narratives in Slovakia. It operates as part of a network of pro-Russian entities that work to sway public opinion in favor of Russia, using cultural and historical ties as a pretext to foster influence and loyalty among Slovaks. It is one of the most popular pro-Russian groups on Slovak social media, commanding tens of thousands of followers. Its leader, Matúš Alexa, frequently travels to Russia and most recently he was an "election observer" in occupied Crimea.

4. What's next?

4.1. Emerging Narratives and Topics in Hybrid Threats

Given the evolving security situation related to Russia's aggression against Ukraine and the current political conditions, Russia is likely to continuously adapt its propaganda and information operations to the circumstances in Slovakia. Additionally, Russia will probably continue to promote narratives that have already proven successful in Slovakia. We can expect the dissemination of the following themes and narratives:

Russia as a stable energy supplier: In the event of an energy crisis or rising energy prices, pro-Russian propaganda may push themes about the advantages of closer cooperation between the EU and Russia in energy supply. This is a recycling of the narrative that sanctions are particularly disadvantageous for the EU. The goal is to limit or even lift EU sanctions against Russia.

Russia ensures regional stability: In line with historical revisionism and the rehabilitation of the Soviet Union, pro-Russian narratives may present the Soviet era as a time of stability, prosperity, and peace. Consequently, Russia, as the successor state, will be portrayed as capable of continuing this legacy, legitimizing current Russian policies. This also undermines Slovakia's NATO membership as a guarantee of its security.

Ukraine does not deserve support: The narrative that the Ukrainian government promotes Nazi ideology will continue. Such claims will be supported by the ongoing spread of fabricated reports about the existence of Nazi units fighting against Russia and constant reminders of alleged human rights violations against the Russian-speaking population in Ukraine. Moscow will continue to use these narratives to justify its invasion of Ukraine.

Migration and multiculturalism: In the context of a potential worsening situation in Ukraine and an increase in the number of refugees fleeing the war, or even other migration waves, Russian propaganda may exploit fears of a migration crisis and multiculturalism to undermine trust in the EU and spread xenophobic and nationalist narratives.

Decadence and decline of the West: Russian-spread narratives may increasingly emphasize the image of the West as a morally and culturally decadent community losing its traditional values. Conversely, Russia will be depicted as a defender of traditional values, which could effectively strengthen pro-Russian sentiments.

All the mentioned narratives have great potential to further polarize society in Slovakia. According to the latest survey, nearly 40% of the Slovak population shows some level of understanding for a balanced approach between Western countries and Russia. This segment of the Slovak population is a potential target for propaganda and information operations by the Russian Federation.

4.2. Situation of National and Societal Support for Ukraine in Slovakia

Before the parliamentary elections in September 2023, the Slovak government provided support to Ukraine in line with Slovakia's international commitments as a member of the European Union and NATO. This support included several key areas:

Humanitarian aid: Slovakia provided humanitarian assistance to Ukraine in the form of material donations, such as food, medicines, medical equipment, and other essential supplies for civilians affected by the conflict.

Military support: Slovakia offered significant military assistance to Ukraine, including the supply of aircraft, heavy combat equipment, weapons, ammunition, and other military gear. This support was part of a broader international initiative to strengthen Ukraine's defense capabilities and was coordinated with NATO and European Union partners.

Diplomatic support: The Slovak government expressed full political and diplomatic support for Ukraine on the international stage. Slovakia actively participated in negotiations and initiatives aimed at resolving the conflict and supported sanctions against Russia.

Economic and financial aid: Slovakia contributed to financial support for Ukraine through international mechanisms, such as EU programs for the country's recovery and reconstruction.

Support for Ukrainian refugees: The Slovak government provided assistance to Ukrainian refugees who arrived in Slovakia, including temporary shelter, healthcare, education, and integration into society. Over one million refugees crossed the Ukrainian border into Slovakia, with more than 100,000 choosing to remain in Slovakia. According to available data, Slovakia allocated 700 million euros to assist refugees from Ukraine.

After the parliamentary elections in 2023, the situation significantly shifted against Slovak support for Ukraine. **The new government is pursuing a policy with a certain degree of pro-Russian sentiment and is skeptical about supporting Ukraine**. It only declares the provision of humanitarian aid, with military assistance limited to contracted and paid deliveries of ammunition and the provision of capacity for the repair of military equipment.

The Prime Minister of Slovakia labels Ukraine as a corrupt, non-sovereign state under the total influence and control of the USA and does not support its admission to NATO. He also argues that providing weapons to Ukraine prolongs the war and that Western countries do not actually want peace. It is questionable whether this stance reflects FIMI or is a cynical and populist stance by some political actors seeking political gain.

On the diplomatic level, however, Slovakia has not yet blocked financial support from EU countries to Ukraine and continues to vote for further sanctions against Russia. As for support for Ukrainian refugees, it is gradually decreasing, particularly concerning housing subsidies.

At the societal level, support for Ukraine continues mainly in the form of humanitarian collections, providing accommodation, and helping with integration into society. However, given the current pro-Russian rhetoric of the Slovak government, this could lead to a decline in public support for Ukraine, especially if the economic situation of Slovak citizens worsens.

4.3. Emerging Information Threats in the Lead-Up to and After European Elections (Next 2-5 Years)

The period leading up to and immediately following the European Parliament elections was particularly vulnerable for Slovakia. During this time, the following information operations and propaganda, particularly from Russian sources, were observed:

Exploiting Euroscepticism: Pro-Russian narratives aimed to strengthen Euroscepticism by portraying the EU as an ineffective and authoritarian project that threatens the sovereignty of its member states, including Slovakia. Additionally, the European Union was depicted as a coalition of countries that benefits from the war in Ukraine, framing it as a threat to Slovakia's security.

Supporting extremist and populist parties: Russian disinformation campaigns targeted the support of extremist and populist parties that are critical of the EU and NATO, in an attempt to weaken EU unity. Information operations also focused on issues such as illegal migration, alleged failures of multiculturalism, or human rights issues concerning sexual minorities.

Other current topics suitable for polarizing society: During the pre- and post-election period, Slovakia and other EU countries may be targeted by coordinated disinformation campaigns aimed at manipulating voters to deepen societal polarization and disrupt democratic processes. These disinformation campaigns will be specifically tailored to the current political and social climate in each country.

4.4. The Role of AI and Cybersecurity Challenges in Future

In the near future, **artificial intelligence (AI) is expected to play a significant role in propaganda and information operations** in Slovakia. This development might involve both the large-scale generation of disinformation content and the dissemination of highly targeted deepfake content.

Given the current technological developments and trends in other countries, AI will likely be used for the **mass generation of disinformation articles, social media posts, and other content, thereby increasing the volume and likely also the quality of pro-Russian narrative**s. This technology will enable faster and more efficient dissemination of disinformation, making it increasingly difficult for average internet users to discern false information from the truth. High traffic to alternative media sites in Slovakia increases the efficiency of using such AI tools.

Deepfake content will also become **more sophisticated with the advancement of A**I. Media reports indicate that current deepfake content is often based on recordings or photos from other events, which are placed in a new context. However, with the development of deepfake technology, AI could create fake videos and audio recordings of political leaders and public figures, which could be used to discredit those who oppose Russian influence or to spread lies about geopolitical events. However, despite these predictions, so far no significant impact from deepfake content was observed in Slovakia before or after the European elections.

AI could also be employed for personalized targeting in disinformation campaigns, specifically tailored to demographic groups in Slovakia. These campaigns could prove highly effective in shaping public opinion and influencing political preferences.

Additionally, with the growing sophistication of cyberattacks, Slovakia will face new cybersecurity threats. Pro-Russian groups may leverage AI to coordinate and automate cyberattacks on critical infrastructure, government institutions, and media outlets. In response, security agencies will need to strengthen their cyber defenses and adopt advanced technologies to detect and neutralize such threats.

In Slovakia, **we can expect that the future of Russian propaganda and influence operations will become increasingly sophisticated with the use of AI**, adapting to the changing political, economic, and technological landscapes. Slovakia's response to these challenges will require not only increased public awareness but also enhanced international cooperation, investment in cybersecurity, and stronger resilience against disinformation and propaganda. Given the Slovak government's limited understanding of hybrid threats, ensuring an effective response will be particularly challenging.

5. State's and EU responses to FIMI

5.1. Identifying Current Gaps in Legal, Institutional, Societal, and International Frameworks

There are many specific gaps to be addressed across the legislative, institutional and societal level. Yet the single most important barrier to enacting meaningful and effective measures against FIMI and hybrid threats in Slovakia is an almost complete rejection of the need to carry out such measures by the current Slovak administration. This rejection stems both from seeing such measures as "censorship of other opinions" and open adoption of some pro-Russian narratives and positions used by both domestic and foreign disinformation spreading actors. Without recognizing the problem, the government is not motivated to implement policies or strategies to counter Russian disinformation and hybrid threats effectively.

Legal level

- **Lack of legislation to combat FIMI and hybrid threats**, including clear definitions and penalties. The enforceability of existing legal tools to combat hybrid threats is insufficient.
- **Missing legislative anchoring of responsibilities** and competencies for coordinating the response to FIMI.
- **Inadequate implementation** of existing strategic and conceptual documents, as they are often formally adopted without mechanisms to ensure enforcement.
- **No long-term consensus** on the understanding of strategic and conceptual documents, leading to a lack of continuity in policy implementation following changes in government.

Institutional level

- **Coordination and communication are hindered** by the absence of a central coordinating body. Departmentalism and formalism dominate the issue, resulting in weak coordination and ineffective procedures. A unified and systematic approach is lacking.
- **Absence of position within the government with a comprehensive overview** of all aspects of security and a mandate to ensure political support in addressing hybrid threats. A national security advisor could fill this role, providing an overarching view and political backing.

- **Lack of dedicated units for dealing with FIMI** within most state institutions. Expert units that do exist are being reduced, insufficiently staffed, and their activities are often unrelated to FIMI analysis and countermeasures. The funding for these units is insufficient and historically heavily reliant on European funds, limiting long-term sustainability.
- **Weak political support for countering FIMI**, with many state officials misunderstanding or underestimating the issue. Political appointments to expert positions are often made without the necessary qualifications.
- **Low awareness and understanding among politicians** - both in government and opposition. Many politicians underestimate the severity of hybrid threats and, in some cases, block proposed solutions. The line between political and professional roles is not strictly maintained.

International level

- **Lack of sufficient engagement and willingness** from the government to cooperate with international partners in countering FIMI, as this topic is often misunderstood or deliberately neglected.
- **Unstable institutional framework.** The new draft of the Strategy on Countering Hybrid Influence introduces significant changes in the institutional structure responsible for FIMI coordination with international partners. It proposes transferring responsibility from the Government Office to the National Security and Analytical Center of the Slovak Information Service. However, this strategy has not been approved yet, leaving the institutional framework undefined and unstable.

Societal level

- **Insufficient government cooperation with the academic sector and private companies** in countering FIMI, any cooperation is based primarily on ad-hoc activities.
- **Nonexistent involvement of the civic sector** in countering FIMI, participatory public policy creation, and resilience building, largely due to the government's hostile stance towards this sector.

5.2. Improving State and EU-Level Responses to Enhance Resilience Against Hybrid Threats

The EU still lacks a robust, well-resourced, and skilled apparatus capable of effectively detecting, responding to and countering attempts by foreign hostile actors to influence internal issues of the EU and its member states. It is evident that Russia and China, in particular, are exploiting numerous loopholes in current European policies, allowing them to circumvent or undermine sanctions, gather intelligence, influence elections, and foster societal unrest and polarization.

Therefore, the EU should make use of its economic power, diplomatic soft power, global norm-setting power (GDPR and DSA being prime examples thereof) and administrative apparatus to create, in close cooperation with EU member states, a viable deterrence against FIMI and broader hybrid influencing. In last 2 years, several EU expert bodies, such as the EU Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), along with European Parliament committees like INGE and INGE2/ING2, have produced numerous recommendations and measures to enhance detection, disruption, and counteraction against FIMI.

Yet many of these measures remain only as recommendations without proper resources and structures to implement them. Policy plans like the European Democracy Action Plan provide an important blueprint, but their real impact remains limited without adequate funding and institutional frameworks. Moreover, all such measures adopted up to date lack a viable, strong deterrence, based on a heavy toll to be borne by any actors crossing a clearly defined red lines. Some proposals even suggest bold measures, such as creating a stand-alone Directorate-General (DG) dedicated to countering FIMI and hybrid threats.

However, institutions alone, without appropriate legislation and a clear mandate from member states, cannot effectively deter disruptive campaigns by Russian, Chinese, and other hostile foreign actors. Perhaps a PESCO (Permanent Structured Cooperation) might serve as an example to follow in this regard. By creating a group of countries able and willing to pool their resources and adopt voluntary coordination and information exchange measures the unanimous vote required for EU-wide solutions could be circumvented.

5.3. How Should National Parliament and the European Parliament Better Address the FIMI Issue

The European parliament should reinstate the ING2 committee as a permanent committee with the authority to investigate, summon witnesses and gather expert testimonies. Its previous work, particularly the Kalniete report on foreign interference into democratic processes in the EU , is a glaring example of bringing the issue of FIMI to the center of political and public debate and wielding powers of the EP effectively.

The political landscape in Slovakia, marked by a deeply polarized and politicized debate on FIMI, disinformation, and hybrid threats, effectively rules out any meaningful measures at the level of Slovak Parliament. While in theory, the Slovak version of the INGE committee would be more than required, it is highly unlikely that the ruling coalition, which holds a majority, would support such an initiative.

6. Conclusions and recommendations

Slovakia currently lacks an effective system to counter hybrid threats, including FIMI. Even in previous years, efforts to develop such a system were largely declarative rather than actionable. Despite the severity of these threats, the state's response has been inadequate, leaving significant vulnerabilities and weaknesses unaddressed.

The situation has significantly deteriorated following the 2023 parliamentary elections, when the current government weakened the state structures responsible for strategic communication and addressing hybrid threats. This has significantly limited the comprehensive societal approach needed to build resilience, further degrading the overall capacity to address this critical security issue.

Therefore, it is crucial for the public administration to urgently implement measures in the following areas:

Legal area:

- **Enact specific legislative measures** aimed to fill the existing gaps in the Slovak legislation related to countering FIMI and hybrid threats. The new legislative provisions should include a clear definition of key terms used in the FIMI context, taking into account the fast-evolving nature of such threats. The legislation must also establish a viable deterrence through dissuasive financial and criminal penalties.

- **Clearly define roles and competencies** of all relevant state administration and security apparatus bodies - from detection to response coordination. By establishing clearly defined roles, corresponding to the remit of individual bodies and agencies, as well as legislating the rules for exchange of information and cooperation, the enforceability of existing legal tools to combat hybrid threats would be significantly enhanced.
- **Enact legislation enabling creation of a standing parliamentary committee** on FIMI and hybrid threats. This committee would act as a crucial oversight body, with the power to request information, monitor processes, and issue reports without running into risk of being politicized.

Public Policies:

- **Implement existing strategic and conceptual documents**, provide strong political support and requirements for their enforcement. Work on building a long-term consensus on the understanding of strategic and conceptual documents, to ensure their continuity and effectiveness across different election cycles.
- **Establish standardized and ongoing cooperation** with the academic sector and private companies to counter FIMI. **Involve the civic sector** in shaping public policy and building societal resilience.

Institutional Framework:

- **Consider creating a dedicated position within government** with a comprehensive overview of all aspects of security and a mandate to ensure political support in addressing hybrid threats. This role could be filled by a national security advisor who would have a broad overview of security matters and provide political backing.
- **Create specialized units for combating hybrid threats and strategic communication** within relevant state institutions. Ensure that existing units are sufficiently staffed and equipped with proper tools and skills. Provide sustainable long-term funding, so the system is not relying on European funds or ad-hoc financing.
- **Appoint a lead institution to coordinate stakeholders** involved in both long-term strategies and rapid responses to hybrid threats. A unified and systematic approach, complete with clear procedures, should be established to ensure effective coordination and communication between institutions.
- **Ensure non-party support in this area,** educate state officials to improve their understanding of these issues. Prevent political appointments to expert positions that are made without the necessary qualifications. Raise awareness and understanding of FIMI among politicians.