SAFEGUARDING DEMOCRACY:

COUNTERING FOREIGN INFORMATION MANIPULATION AND INTERFERENCE IN THE CZECH REPUBLIC AND THE EU

Authors Veronika Víchová, Andrea Michalcová

CENTER FOR
AN INFORMED
SOCIETY

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.

CENTER FOR
AN INFORMED
SOCIETY

EXECUTIVE SUMMARY

KEY FINDINGS

- **Fragmented Legal Framework:** The Czech Republic lacks a comprehensive legal framework to address FIMI. The Criminal Code is insufficient in defining and covering FIMI. There is no law authorizing the blocking of harmful websites, and the country has not yet implemented the EU's **Digital Services Act**. This leaves gaps in the ability to regulate harmful content online and prosecute actors involved in disinformation campaigns.
- **Weak Institutional Coordination:** While multiple institutions are involved in countering FIMI, including the **National Cyber and Information Security Agency (NÚKIB), Office of the Government, Ministry of Defense**, and the **Ministry of Interior**, coordination between these bodies remains fragmented. The lack of clear mandates and regular communication hinders an effective national response.
- **Public Vulnerability:** Disinformation campaigns, particularly those linked to foreign actors like Russia, have exploited societal divisions in the Czech Republic, particularly around issues such as EU membership, support for Ukraine, and socio-economic concerns. Public awareness on the dangers of disinformation remains insufficient.
- **Threats to Support for Ukraine:** Public and political support for Ukraine remains strong, but fatigue from the ongoing war is growing. Disinformation campaigns are likely to target this sentiment, portraying support for Ukraine as a costly and endless burden, potentially weakening future solidarity.
- **Cyber-threats and subversion:** The intensification of subversion efforts poses new challenges, representing a potential source of further divisions in society for the future.

RECOMMENDATIONS

1. Strengthening Legal Frameworks

- Pass the **Digital Economy Law** to implement the **Digital Services Act** and improve the regulation of harmful online content.
- Revise the **Czech Criminal Code** to define crimes related to collaboration with hostile foreign powers, especially concerning non-classified but sensitive information.
- Streamline the enforcement process of the **Sanctions Act**, allowing faster action against entities engaged in FIMI.

2. Improving Institutional Coordination and Resources

- Institutionalize the role of the **Government Coordinator for Strategic Communication** in law to ensure long-term strategic coordination.
- Enhance coordination among state institutions by **formalizing mandates** for all relevant bodies, such as the **Security Council's Working Group on Hybrid Threats**, and ensuring they meet regularly.
- Allocate more resources for **cybersecurity, data analysis, and training**, and ensure the capacity to handle hybrid threats across all state institutions.

3. Enhancing Societal Resilience

- Launch long-term **public awareness campaigns** focusing on media literacy, social cohesion, and resilience to disinformation.
- Integrate **media literacy** and **digital citizenship** into the national educational curriculum at all levels.
- **Foster partnerships** between government agencies, media, NGOs, and academia to create a united front against disinformation and build societal resilience.

4. Strengthening EU-Wide Cooperation and Intelligence Sharing

- Establish a more robust **real-time intelligence-sharing mechanism** between EU member states, particularly regarding FIMI campaigns.
- Bolster the mandate of the **European Center of Excellence for Countering Hybrid Threats** to act as a central hub for data exchange and analysis.
- Enhance **financial and technical support** from the EU to assist member states in developing their national strategies against hybrid threats.

5. Oversight and Strategic Communication

- Establish a **dedicated oversight commission** reporting to the President or the national Parliament to monitor the implementation of FIMI-related strategies and ensure tangible results.
- Ensure the European Parliament advocates for increased **cross-border initiatives** and joint campaigns focused on **raising public awareness of FIMI threats**.
- Invest in long-term **strategic communication campaigns** at both the national and EU levels, ensuring consistency and credibility in public messaging.

INTRODUCTION TO COUNTERING FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) AT THE NATIONAL LEVEL

The official recognition and response to FIMI at the national level in the Czech Republic can be traced to various strategic security documents, with notable developments since the mid-2010s. The first document to specifically focus on hybrid threats and hostile influence of a foreign power has been the Audit of national security (2016), which analyses these threats and includes a series of targeted recommendations for state institutions to improve their responses in the most vulnerable areas.

Another important document which has been approved in 2021 is the National strategy for countering hybrid interference which sets out three strategic priorities: (1) resilient society, state and critical infrastructure, (2) systemic and holistic approach and (3) the capability of adequate and timely reaction. One of the objectives included in the strategy is to build a strategic communication system capable of effectively informing the public. While both of these strategic documents map out the threats realistically and set out the necessary goals and objectives, implementation of both has been inadequate.

The National Cyber Security Strategy (2021–2025) and the Security Strategy (2023) all include elements aimed at enhancing resilience against disinformation and foreign interference. These documents, while not laws, guide the development of policies and actions across government institutions.

The legal framework specifically addressing FIMI remains fragmented or completely lacking in some areas. For instance, the Czech Republic currently lacks direct legislation authorizing the blocking of websites involved in spreading disinformation which became a significant issue during the 2022 Russian invasion of Ukraine when certain disinformation websites were taken down by domain providers without a clear legal mandate. This raised concerns about legal certainty, even though the situation was unique and arguably, blocking websites proved quite ineffective in countering disinformation and propaganda after the invasion.

Even more importantly, the draft law on digital economy was still not approved by the Parliament, which makes it impossible for the Czech institutions to implement the EU's Digital Services Act, and therefore Czech internet users lack possibilities to defend against harmful and illegal content online.

More positive developments have taken place in the sanctions sector, more specifically with the Sanction Act and the amended Act on International Sanctions, which specifically allow to sanction entities involved in malicious information operations. They allow a legal basis for sanctioning individuals and entitled on the national level, either before these entities are put on European sanctions lists, or if the process on the European level gets stalled. However, even in this case, effective implementation remains challenging, mostly due to the complexity of the process and lack of resources on the state level.

At the same time, the Czech criminal law still lacks the possibility to criminally prosecute individuals or entities which collaborate with a hostile foreign power, and for example extract information which are highly sensitive, but not classified. At the same time, evidence presented by intelligence services cannot be used in criminal proceedings.

TIMELINE OF KEY EVENTS:

Year	Event	Description
2014	**Establishment of the National Cyber Security Centre**	Focused on improving the Czech Republic's cybersecurity resilience.
2016	**Audit of National Security**	Commissioned by the Prime Minister, this document identifies major threats like hybrid threats and foreign influence, and offers institutional responsibilities and recommendations to address security gaps.
2017	**Establishment of the Centre against Hybrid Threats**	Established to counter foreign disinformation campaigns targeting internal security in the Czech Republic.
2018	**New Cybersecurity Law**	Implemented measures to safeguard critical infrastructure against hybrid and cyber threats.
2020	**National Cybersecurity Strategy (2021-2025)**	Launched to strengthen the country's cybersecurity and address hybrid threats.
2020	**Permanent Commission for Hybrid Threats**	Established in the Czech Parliament with the ability to advise and call on the Government and map the situation of countering hybrid threats in Czechia.
2021	**National Strategy for Countering Hybrid Interference**	Outlined goals for enhancing societal and institutional resilience against hybrid threats.
2022	**„Non-Legislative" Response to Russian Invasion of Ukraine**	Provisional controversial blocking of websites spreading Russian disinformation.
2022	**The appointment of the Governmental Commissioner for Media and Disinformation**	This role was integral to the Office of the Government, aiming to contribute to strategic communication and assist in formulating budgets for government communication. Additionally, the responsibilities of this representative extended to the revision of media laws and the coordination of draft legislation on disinformation. The position has been abolished appx. 1 year later and no longer functions.
2022	**Establishment of Strategic Communications Department**	Formed within the Office of the Government to coordinate communication efforts against disinformation.
2022	**Crisis Information Team (Ministry of Interior)**	Set up to handle communication during crises, particularly in relation to hybrid threats.
2023	**Analysis of the readiness of the Czech Republic to face a serious disinformation wave**	Put together by the Ministry of Interior and approved by the government, the Analysis states that the Czech Republic at the time lacked conceptual, organizational, personal, process, legal or any other tools and capacities effective in case of a response to a disinformation attack.
2023	**A new adviser to the Prime Minister was appointed, focused on information literacy and countering disinformation**	The position lacks executive power and will rely on the PM's willingness to heed his advice. The emphasis was placed on enhancing people's information literacy and bolstering educational efforts in this domain

2023	**Defense Strategy of the Czech Republic**	Prioritized hybrid threats from Russia and China, and emphasized the role of strategic communication.
2023	**Sanction Act and the amended Act on International Sanctions**	Strengthened the national response to violations of international sanctions.

In the Czech Republic, the responsibility for countering FIMI is dispersed across several state institutions. Key actors include:

- The National Cyber and Information Security Agency (NÚKIB), which is central to defending against cyber threats and plays a role in strategic communication.
- The Ministry of Defense, specifically through its Department of Crisis Management, which addresses hybrid threats, including disinformation.
- The Center Against Hybrid Threats (CHH) under the Ministry of Interior, established in 2017 as the first specialized body for hybrid threats, focusing on the internal security impacts of foreign influence.
- The Intelligence Services, such as the Security Information Service (BIS), which monitor and counteract foreign intelligence activities and disinformation.
- The newly established Government's Strategic Communication Department, which coordinates communication efforts to counter disinformation and improve public resilience.

ROLES OF INSTITUTIONS IN DIFFERENT POLICY AREAS:

Policy Area	Government	Parliament	Other Institutions
Diplomatic/Political	Ministry of Foreign Affairs	Foreign Affairs Committee	Ministry of Defense, National Security Council (BRS)
Information	Ministry of Interior	Information and Communications Committee	National Cyber and Information Security Agency (NÚKIB), Czech Television
Military	Ministry of Defense	Defense Committee	General Staff of Armed Forces, Military Intelligence
Economic	Ministry of Finance	Economic Committee	Ministry of Industry and Trade, National Bank (ČNB)
Financial	Ministry of Finance	Budgetary Committee	Czech National Bank (ČNB)
Intelligence	Ministry of Interior (Security)	Security Services Oversight Committee	Security Information Service (BIS), Military Intelligence
Legal	Ministry of Justice	Legal and Constitutional Affairs Committee	Supreme Court, Public Prosecutor's Office, Ministry of Interior

INSTITUTIONAL RESPONSIBILITIES IN ADDRESSING FIMI

Institution	Department/Division	Responsibility Areas
Office of the Government	**Department of Strategic Communication**	Coordination of strategic communication and monitoring disinformation.
Ministry of Defense	**Section of Defense Policy and Strategy**	Responding to hybrid threats, development of defense strategies.
National Cyber and Information Security Agency (NÚKIB)	**Cybersecurity Division**	National cybersecurity, protection against hybrid threats.
Ministry of Interior	**Centre against Hybrid Threats**	Analysis and response to hybrid threats affecting internal security.
Ministry of Interior	**Stratcom team**	Conducting online and offline campaigns.
Ministry of Interior	**Communication Response Team**	Crisis communication during hybrid attacks.
Ministry of Foreign Affairs	**Department of Strategic Communication**	Cooperation with international partners on strategic communication.
Intelligence Services	**Not public**	Identification and counteraction of foreign hybrid activities.
Parliament	**Permanent Commission for Hybrid Threats**	Oversight of measures related to hybrid threats and protection of elections.

These institutions, while playing pivotal roles, face challenges in coordination due to a lack of formalized responsibilities and mandates, contributing to fragmented responses.

The Parliament plays a role in addressing FIMI through legislative oversight and policy development. Several parliamentary committees are engaged in issues related to FIMI, although the level of involvement varies. Notably, the Permanent Commission for Hybrid Threats was established in 2020, focusing specifically on monitoring the protection of elections and mapping efforts to counter hybrid threats. While its role is primarily advisory, it represents a parliamentary acknowledgment of the significance of hybrid threats, including FIMI.

Other committees, such as those dealing with security, defense, and foreign affairs, indirectly address FIMI through broader discussions on national security and international relations. However, the topic of FIMI often cuts across multiple areas, which sometimes leads to its treatment as a secondary issue.

Gaps remain in both legislative, policy and institutional framework, very often due to lack of resources and capabilities to implement approved strategies and unclear mandates and responsibilities across institutions.

HOSTILE ACTORS' NARRATIVES AND TACTICS IN THE CZECH INFORMATION SPACE

FIMI efforts in the Czech Republic have revolved around various critical domains. Hostile state and non-state actors have exploited vulnerabilities in the country's information space, targeting social cohesion, trust in government, and international institutions.

One of the core narratives during the last at least 10 years has focused on undermining the Czech Republic's involvement in the EU. Disinformation campaigns frequently claim that EU membership weakens Czech sovereignty and imposes unwanted rules and responsibilities, especially regarding alleged issues with migrants and refugees. During the last two years, EU related narratives have often focused on issues like EU sanctions against Russia, arguing that these measures harm the Czech economy more than they affect the targeted entities. Russian disinformation campaigns have capitalized on concerns over rising energy prices, linking them to the Czech Republic's compliance with EU policies, particularly in relation to sanctions against Russia. Euroscepticism is still rooted in Czech society, even though the situation changes gradually.

Especially since the Russian invasion in 2022, the key disinformation narratives revolve around the Czech governmental support to Ukraine especially in the military domain, as well as to Ukrainian refugees residing in the Czech Republic. Attacks on Ukrainians in Czechia are mostly interconnected with socio-economic issues, blaming the state for favoring Ukrainians over Czech citizens in housing, social services, or employment, but also touch upon crime rates or spread of diseases.

Social media platforms and quasi-media, such as alternative news sites and discussion forums, as well as chain emails, have proven to be critical tools for disinformation actors. Hostile entities have used these platforms to bypass traditional media gatekeepers and spread disinformation more rapidly. The rise of alternative media, such as YouTube channels, Telegram groups, and niche websites, has allowed hostile actors to reach segments of the population that are distrustful of mainstream news outlets and often demonstrate frustration and fear about their future. These platforms often amplify conspirative content and anti-government sentiment, aligning with narratives pushed by foreign actors.

There is evidence of overlap between the activities of external disinformation actors and certain internal actors, both in the quasi-media and political spheres. Internal actors, including fringe political figures and alternative news outlets, have played a role in amplifying narratives that originate from external sources. Far-right, far-left and anti-establishment parties have frequently echoed Russian talking points regarding the EU, NATO or the refugee crisis. These local actors often find common ground with external actors in promoting narratives that challenge Czech government policies, especially concerning international alliances, sanctions against Russia or support to Ukrainian refugees. While criticism of the government is legitimate and cannot be automatically tagged as information interference and manipulation, these sentiments are often amplified by spreading disinformation and abusing and inciting distrust, fear, frustration and other negative emotions.

Quasi-media platforms serve as an important bridge between external disinformation efforts and local audiences. Platforms like "Voice of Europe," which operated from Prague before being exposed as a pro-Russian operation, or "NeČT24", a Telegram channel which has been tagged as the continuation of the Russian state news channel Sputnik by the Czech Ministry of Interior, exemplify how external actors can infiltrate the local information ecosystem. These platforms often blend legitimate news with manipulated content. While they provide the initial disinformation narrative, internal actors – be it political figures or alternative media – expand on them and tailor them to their own audiences. This is making it difficult to discern between credible sources and propaganda, as well as to track the origin of any given piece of content. An example of this is the coordinated dissemination of anti-refugee rhetoric by local far-right politicians who echo Russian disinformation campaigns.

As mentioned in the previous chapter, there are gaps in both legal and institutional domains in the Czech Republic. Czech legislation lacks comprehensive tools for addressing online disinformation. While certain actions, such as blocking disinformation websites, were undertaken during the Russian invasion of Ukraine in 2022. These actions were not grounded in a legal framework, and proved rather ineffective, since most of the disinformation actors changed domains or platforms and continued in their activities. Moreover, the absence of laws specifically designed to counter harmful content in the digital space, such as the implementation of the EU's Digital Services Act, leaves the country vulnerable. When it comes to non-legislative measures, the state's responses have been largely reactive to specific disinformation activities and often came months after disinformation narratives started influencing the public opinion.

THE FUTURE OF FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI)

The important milestone for the future trends of FIMI in the Czech Republic will be the Parliamentary elections, which will take place in Autumn 2025. While FIMI might play a significant role in the pre-election period as well, it can be presumed that hostile actors, particularly from Russia, will adjust future narratives and tactics to the election results. Currently, public polls showcase the highest probability of the opposition party ANO 2011 winning the elections, which might switch the trajectory of the country away from the principal support of Ukraine and opposing the Russian aggression. However, there are several narratives which will most likely remain regardless of the election results.

Focus will probably remain on the European Union and NATO, portraying these institutions as oppressive, costly, imposing or even unnecessary. Disinformation actors will probably continue to emphasize the financial burden of our participation in these international alliances, spreading false claims about Czech sovereignty being undermined.

Economic discontent will likely become a primary target, since the Czech population continues to look into the future with fear and uncertainty. Russia has already weaponized the issue of rising energy prices, framing EU sanctions on Russian energy as the root cause. As inflation and economic pressures continue, and the national elections are coming closer, disinformation campaigns could even further inflame economic insecurities, blaming both the government and the international institutions for perceived (or real) economic failings.

The socio-economic hardships, but also any other polarizing issues, like migration, national identity, and ethnic divisions in society are most likely to continue to be stirred. Especially disinformation related to refugees from Ukraine, as well as Africa and the Middle East (directly connected to the EU's Migration Act) have been already abused before elections to the European Parliament and will potentially play a role in the future. These topics have been exploited to divide communities and erode social cohesion, as seen in the narratives around Ukrainian refugees. In the future, this may evolve into more sophisticated disinformation campaigns targeting younger generations or progressive social movements, framing them as threats to traditional values or national security. By stirring fears around multiculturalism or economic competition between refugees and Czech citizens, external actors could exacerbate domestic divisions.

Future disinformation efforts may also target public health and environmental topics, such as climate change, vaccination, and green policies. These issues have already been crucial before the latest European elections. With climate-related policies becoming increasingly central to EU governance, these areas are likely to be exploited further by external actors aiming to sow dissent against EU environmental regulations or climate initiatives.

While public and political support for Ukraine in the Czech Republic remains relatively strong for now, it is not immune to disinformation efforts. Fatigue from the prolonged conflict is showing already, as there are a majority of people who would prefer a quick end to the conflict, even at the cost of losing some

Ukrainian territories (69 % of the population in February 2024). Over time, public fatigue concerning the war in Ukraine will almost certainly grow even further. Disinformation narratives could exploit this fatigue, framing Czech support for Ukraine as a costly and endless burden. Narratives focusing on the supposed preferential treatment of Ukrainian refugees, particularly regarding housing, healthcare, and social services, may continue to fuel resentment, potentially leading to decreased public sympathy for Ukraine.

On the political level, there are also growing divisions concerning Ukraine. Far-right, far-left and populist parties, which tend to criticize the EU, and in some cases also NATO policies, have been vocal about opposing continued support for Ukraine. They often claim that the government prioritizes Ukraine over addressing domestic issues. At the same time, these populists, far-right and far-left movements have already been successful in the European elections, and have a big potential to form a coalition next year after the national elections.

Similar actors also often promote manipulated peace-related narratives, which is also in symbiosis with pro-Russian disinformation actors and activists. They claim that the continued support for Ukraine is prolonging the conflict, and push for peace negotiations under terms favorable to Russia. Such narratives can appeal to war-weary segments of the population, framing those advocating for military support as war-mongers, while positioning calls for peace as sensible and moral. If these narratives gain traction, public and political support for Ukraine could weaken significantly.

While new technologies, especially artificial intelligence and its potential use for disinformation campaigns and their amplification, present a global challenge for the future, even more “conservative” tactics and strategies employed by hostile actors work effectively in Czechia for now. Besides disinformation campaigns, there is a strong presumption that subversive activities causing further fear amongst the population might continue and even intensify. During the last months, several subversions conducted on Czech soil have been either directly attributed to Russia, or there has been a suspicion vocalized by Czech authorities. That includes cyber-attacks on Czech state institutions or Czech Railways. With the beginning of the school year in September 2024, hundreds of schools in Czechia started receiving threats that they were mined, repeatedly for several days. According to the authorities, this case might also be a part of a hybrid war waged against Europe, but the investigations are still ongoing.

Cases like this are unnerving regardless of the context, however, they might have even stronger impact on Czech society after a tragic event at the Charles University in December 2023, where an active shooter killed 14 people and then committed suicide. While this tragedy has nothing to do with FIMI, it has been a subject of disinformation campaigns as it was unfolding, some entities claiming that the shooter was Ukrainian. The event shook the nation and the realization that something like this is possible, makes Czechs especially vulnerable to any other potential threats of similar character. This can be abused by hostile actors, not necessarily by conducting similar atrocities, but increasing the fear of them in the public space.

STATE AND EU RESPONSES TO FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI)

The fight against foreign information manipulation and interference (FIMI) is a multi-dimensional challenge that requires legal, institutional, societal, and international coordination. Both the Czech Republic and the European Union have made strides towards addressing FIMI, but significant gaps remain.

The Czech Republic's legal framework for countering FIMI has several key weaknesses. There is a lack of clear definitions for critical concepts such as "disinformation", "hybrid threats" and "foreign influence." Without these definitions, it is challenging to enforce laws consistently and coordinate between different state institutions. Moreover, existing laws do not fully address the growing challenges of regulating harmful online content. The absence of a Law on Digital Economy has prevented the country from effectively implementing the EU's Digital Services Act, which is crucial for managing illegal content on social media and other online platforms. Additionally, there is no legal foundation for the blocking of harmful websites or systematic handling of online threats in ways that respect freedom of expression while ensuring security.

While the Czech Republic has taken steps to create institutions dedicated to FIMI, there is still a lack of clear mandates and coordination between these institutions. The Security Council's Working Group on Hybrid Threats meets infrequently and does not serve as an effective coordination body. More concerning, new roles like the Government Coordinator for Strategic Communication are not yet anchored in law, making them vulnerable to political changes. Additionally, institutions tasked with combating hybrid threats lack the resources, expertise, and mandates needed to address FIMI comprehensively.

At the international level, while the EU has established regulations such as the Digital Services Act and Cybersecurity Act, the coordination between member states is still lacking. FIMI, by nature, transcends borders, and yet national-level responses remain fragmented. The EU could improve mechanisms for the real-time exchange of intelligence on FIMI operations and foster closer cooperation between cybersecurity agencies, intelligence services, and private platforms. Without a robust system for data sharing, joint action, and mutual support, the effectiveness of EU-wide strategies remains limited.

Both the Czech Republic and the EU need faster legal reforms to address the gaps in managing harmful online content and prosecuting actors engaged in disinformation. For example, the Sanctions Act passed by the Czech Parliament is an important tool, but its enforcement has been slow, and the process for sanctioning individuals or entities involved in disinformation should be streamlined. The absence of a comprehensive Digital Economy Law is another missed opportunity. Its passage would enable more effective regulation of digital platforms.

Institutional weaknesses in addressing FIMI could have been avoided with clearer mandates, better coordination, and regular communication between relevant bodies. The Government Coordinator for Strategic Communication role, for instance, could have been institutionalized, with a mandate to over-

see and coordinate all government communication efforts related to FIMI. Similarly, the Security Council's Working Group on Hybrid Threats should be more active and use modern communication platforms to ensure that all institutions involved in countering FIMI are exchanging information effectively.

Public education on the dangers of disinformation has been slow and insufficient. The Czech government, along with EU institutions, should launch more sustained public awareness campaigns, focusing not only on the dangers of disinformation, but also on promotion of social cohesion and building resilience. The establishment of partnerships with media outlets, non-governmental organizations, and academic institutions could help build societal resilience more effectively.

The EU could implement more robust measures to support member states in their fight against FIMI, particularly through improved data sharing and intelligence cooperation. The EU's efforts in sanctioning actors involved in FIMI have been critical, but member states often lack the resources and frameworks to follow through. A stronger EU-wide mechanism to respond to hybrid threats in real time could have enhanced collective coordination.

The Czech Parliament should prioritize passing a novelization of criminal law, so that it clearly addresses issues like collaboration with a hostile foreign power. That will enable more consistent law enforcement. Furthermore, revising the Competence Act to include specific mandates for managing hybrid threats would create a stable and coherent institutional structure capable of addressing FIMI.

Both national and European Parliaments must exercise stronger oversight of the implementation of strategies aimed at countering FIMI. In the Czech Republic, a commission established by either the Parliament or the President dedicated to monitoring and implementation of strategies related to FIMI could ensure that policies are not merely symbolic but result in tangible outcomes. Similarly, the European Parliament could enhance its oversight of the EU's disinformation and cybersecurity strategies, ensuring member states adhere to common standards and that initiatives like the Digital Services Act are implemented effectively.

Both parliaments should push for increased investment in education and strategic communication campaigns aimed not only at raising public awareness of FIMI, but more generally on public understanding of both EU and national strategic policies. The European Parliament should encourage the European Commission to support cross-border initiatives that promote societal resilience against disinformation. The European Commission and the European Parliament should invest into education and training of institutional employees, civil servants and staffers in the area of strategic communication.

The European Parliament should advocate for stronger EU-wide mechanisms for real-time intelligence sharing and coordinated responses to disinformation campaigns. Institutions like the EU Hybrid Fusion Cell or the European Center of Excellence for Countering Hybrid Threats should serve more effectively as a hub for collaboration between national intelligence agencies, cybersecurity centers, and independent researchers.

CONCLUSIONS AND RECOMMENDATIONS

The Czech Republic and the European Union have taken significant steps to address Foreign Information Manipulation and Interference (FIMI), yet the current landscape still presents major challenges in terms of legal frameworks, institutional coordination, and societal resilience. To effectively counter FIMI in the future, these gaps must be addressed comprehensively, with an emphasis on swift reforms, enhanced cooperation, and proactive public engagement.

1. Strengthening Legal Frameworks

The absence of a comprehensive and clear legal framework in the Czech Republic remains a critical vulnerability in the fight against FIMI. Although several strategic documents, like the **Audit of National Security (2016)** and the **National Strategy for Countering Hybrid Interference (2021)**, have highlighted the need for such a framework, implementation has been slow.

- The **Parliament should prioritize the passage of the Digital Economy Law** to enable the enforcement of the EU's **Digital Services Act**, which would empower authorities to take action against harmful online content and disinformation.
- A revision of the **Czech Criminal Code** should clearly define crimes related to **collaboration with hostile foreign powers**, especially concerning the extraction and dissemination of sensitive, non-classified information.
- The **Sanctions Act** and the amended **Act on International Sanctions** must be streamlined to allow more rapid enforcement and ease the complexity of the sanctioning process, ensuring that those involved in malicious FIMI operations can be held accountable at the national level.

2. Improving Institutional Coordination and Resources

The fragmented institutional response to FIMI is a significant hindrance to the Czech Republic's ability to respond quickly and effectively. Although new bodies like the **Department of Strategic Communication** and the **Crisis Information Team** were established in recent years, their lack of legal mandates and insufficient coordination between state agencies weakened the overall national response. Furthermore, the lack of understanding amongst some political representatives as well as some civil servants regarding the role of strategic communication lead to unnecessary politicization and result in lack of trust from the citizens.

- The **Government Coordinator for Strategic Communication** should be formalized in law, with a clear mandate to coordinate efforts across state institutions.
- **Institutional roles should be clarified and formalized**, particularly concerning the Security Council's **Working Group on Hybrid Threats**, which should meet regularly and serve as an active body for information exchange.

- Both national and EU institutions must allocate **more resources** to build capacity for dealing with hybrid threats, including the training of government personnel, enhancing cybersecurity infrastructure, investing in data analytics tools, and raising awareness about the role and services provided by the strategic communication structures.

3. Enhancing Societal Resilience

Public trust in government and institutions has been undermined by disinformation campaigns, particularly on issues related to EU membership, support for Ukraine, and economic concerns. The Czech government has yet to effectively implement **public awareness campaigns** that focus on improving media literacy and societal resilience to disinformation.

- The Czech government, along with the EU, should launch **long-term public awareness campaigns** on the dangers of disinformation, focusing on promoting media literacy, critical thinking, and social cohesion. These campaigns should not only be reactive but proactive, anticipating future FIMI narratives.
- **Educational reforms** should incorporate media literacy and digital citizenship into school curricula to prepare future generations for the challenges posed by hybrid threats and online disinformation.
- Partnerships between the government, **media outlets, non-governmental organizations (NGOs), and academia** should be fostered to create a united front against disinformation, including targeted grant schemes and information sharing platforms.

4. Strengthening EU-Wide Cooperation and Intelligence Sharing

Foreign information manipulation, particularly by state actors like Russia, is a transnational issue that demands an international response. While the EU has enacted critical regulations, such as the **Digital Services Act** and **Cybersecurity Act**, coordination between member states remains inadequate.

- The EU should establish a more robust mechanism for **real-time intelligence sharing** between member states, particularly in the field of disinformation and cybersecurity.
- The EU should bolster the mandate of existing bodies like the **European Center of Excellence for Countering Hybrid Threats** to act as **central hubs for data exchange** and analysis of FIMI campaigns.
- More **financial and technical support** from the EU is needed to assist member states like the Czech Republic in developing and implementing national-level strategies against hybrid threats.

5. Oversight and Strategic Communication

Strong legislative oversight is necessary to ensure that the strategies and policies for countering FIMI are not only implemented but adapted as new threats emerge. Both national and European parliaments should actively engage in monitoring FIMI-related initiatives, ensuring resources and political will are effectively channeled into combating this growing threat.

- The **Czech Parliament** or the **President of the Czech Republic** should consider forming a **dedicated oversight commission** that regularly monitors the implementation of FIMI-related laws and strategies, ensuring that these are not merely symbolic but lead to tangible improvements.
- The **European Parliament** should advocate for more **cross-border initiatives** and joint campaigns focused on **raising public awareness** of FIMI threats, particularly during sensitive periods like elections or major political events.
- National and EU parliaments must also work to ensure **strategic communication** between institutions, ensuring that public messaging remains consistent and factual, particularly when addressing complex issues such as hybrid threats and international relations.

CENTER FOR
AN INFORMED
SOCIETY

www.informedsociety.cz