FIMI-ISAC

FDEI PROJECT

ELECTION REPORT

Assessment of Foreign Information Manipulation and Interference in the 2025 Czech Parliamentary Election

The information and research presented in this presentation are the property of FIMI-ISAC and are intended solely for educational and informational purposes. Copyrights © FIMI-ISAC 2025

Debunk.org Disinformation analysis center

ISD Institute for Strategic Dialogue

GLOBSEC IDEAS SHAPING THE WORLD

Alliance 4Europe

DEN DESIGN ENTREPRENEURSHIP INSTITUTE

FIMI -ISAC

FDEI PROJECT

FIMI RESPONSE TEAM REPORT

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) - INFORMATION SHARING AND ANALYSIS CENTRE (ISAC)

Authors & Partner Organizations

GLOBSEC, Debunk.org, Institute for Strategic Dialogue (ISD), DEN Institute, and Alliance4Europe.

About the Project

This report evaluates Foreign Information Manipulation and Interference (FIMI) threats to the 2025 Czech presidential elections. It was developed through the project 'FIMI Defenders for Election Integrity'. The project consortium brings together 10 member organisations of the Foreign Information Manipulation and Interference Information Sharing and Analysis Centre (FIMI-ISAC), which offer unparalleled expertise in developing a multi-stakeholder FIMI framework before and during elections, thereby serves to also strengthen FIMI defender communities and democratic institutions.

To learn more about the FDEI project, please refer to the project's landing page via the following link: *FIMI Defenders for Election Integrity (FDEI) | Debunk.org.*

About the FIMI-ISAC

The *FIMI-ISAC* (Foreign Information Manipulation and Interference Information Sharing and Analysis Center) is the first ISAC worldwide dedicated to fighting FIMI and creating common standards in this field. It unites a group of like-minded organisations that protect democratic societies, institutions, and the critical information infrastructures of democracy from external manipulation and harm. Through collaboration, the FIMI-ISAC enables its members to detect, analyse, and counter FIMI more rapidly and effectively while upholding the fundamental value of freedom of expression. FIMI-ISAC does not act independently to counter FIMI. Instead, enhancing collaboration empowers its members to do so more effectively.

Table of Contents:

List of Figures and Tables:

Executive Summary

This report provides a critical assessment of Foreign Information Manipulation and Interference (FIMI) during the 2025 Czech parliamentary election period. It examines the methods employed, key perpetrators, evolving tactics, and the efficacy of defensive responses.

The 2025 Czech parliamentary elections took place within an increasingly contested information environment, but the electoral process and Czech society showed strong democratic resilience. Despite the persistent presence of Russian-linked disinformation channels and attempts to sow doubt about the integrity of the vote, no evidence was found of any coordinated, large-scale foreign interference operations capable of influencing the election. Monitoring conducted by FDEI partners, Czech researchers, and national institutions confirmed that malign actors focused predominantly on long-term efforts to erode public trust – particularly through narratives predicting electoral fraud or manipulation – rather than direct disruption of the voting process. These attempts were ultimately unsuccessful, as both state institutions and the public responded with calm, rational, and transparent engagement**.**

The elections were found legitimate, orderly, and technically resilient, despite experiencing several minor, isolated incidents. The temporary malfunction of the eDoklady digital identification system caused confusion but did not compromise voter eligibility or security, and the Ministry of the Interior demonstrated effective communication in clarifying the cause. The Czech Police reported no systemic security incidents, and several minor organisational issues were quickly resolved at the local level. Extensive live media coverage and real-time reporting contributed to transparency and helped maintain public confidence throughout the two-day vote.

At the same time, several developments highlighted ongoing vulnerabilities in the Czech information space. Russian state-linked actors remain the primary external threat, leveraging a resilient network of proxy websites, rebranded media assets, and cross-platform amplification systems to disseminate strategically aligned narratives. Outlets such as *neČT24,* the *Pravda network*, and *NewsFront SK* used large-scale content laundering to shape discourse, while coordinated TikTok, X (formerly Twitter), and Telegram clusters helped foreign-origin narratives resonate in public debates. These operations pursued the long-term objectives of undermining institutional trust, weakening Czech support for Ukraine and EU/NATO alignment, and amplifying polarisation around migration, defence spending, and cost-of-living pressures.

The elections highlighted structural vulnerabilities in Czech democratic resilience infrastructure: persistent sanctions evasion through rebranding, insufficient platform accountability for coordinated inauthentic behaviour, and limited cross-border intelligence-sharing within the tightly interlinked Czech–Slovak–Hungarian information space. Domestic conditions further amplified these risks. High public distrust in political institutions, uncertainties surrounding the newly introduced postal vote, and politicised attacks on independent authorities created fertile ground for meta-narratives alleging electoral fraud, elite capture, and censorship.

Despite these challenges, turnout reached an exceptional 68.95%, one of the highest in modern Czech history. Andrej Babiš's ANO *won* the election with 34.5% and 80 of the 200 seats in the Chamber of Deputies. ANO party was followed by SPOLU with 23.36% and 52 seats, and STAN with 11.23% and 22 seats. Andrej Babiš is negotiating to form a government with Freedom and Direct Democracy (SPD) and Motorists for Themselves. President Petr Pavel has *stated* that he is prepared to appoint him once any conflicts of interest are resolved.

Overall, the elections confirmed that the Czech Republic possesses strong institutions, an active civil society, and a resilient public, all of which played an essential role in mitigating the impact of FIMI. However, the findings also underscore the need for sustained investment in digital security, transparent political advertising rules, platform accountability, strategic communication, and cross-border cooperation. As the Czech political landscape enters this next phase, maintaining trust in institutions and strengthening systemic protections against FIMI will be critical for safeguarding democratic processes in the years ahead.

1. Introduction

The 2025 Czech parliamentary elections were held against the backdrop of a rapidly evolving FIMI landscape, in which foreign malign influence has become structurally embedded in the country's information environment. Czechia has long been a target of Russian influence operations, and since 2022, these efforts have intensified, exploiting regional political turbulence, economic pressures, and debates surrounding the war in Ukraine. As foreign actors adapted their techniques, the Czech information space has faced increasingly sophisticated forms of narrative laundering, infrastructure rebranding, and cross-platform amplification designed to obscure attribution and maximise societal impact.

Against this backdrop, the elections offered a significant test of the resilience and preparedness of Czech democracy. Early warnings issued by intelligence agencies highlighted the risk of foreign information manipulation, while the introduction of postal voting for citizens abroad and broader technological modernisation of the election administration generated new opportunities for voters and exploitable vulnerabilities. At the same time, chronic public distrust in political institutions, high levels of societal polarisation, and long-standing gaps in media ownership transparency and campaign finance oversight continue to challenge national resilience. Furthermore, the delayed implementation of the Digital Services Act (DSA) limited the capacity of Czech authorities to supervise platform compliance during the election.

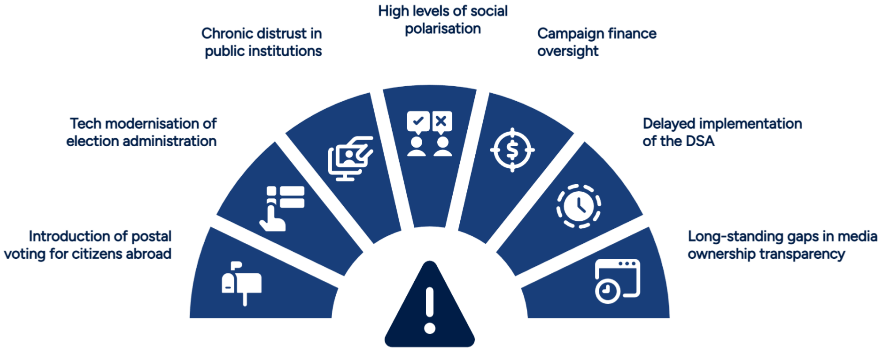

Introduction of postal voting for citizens abroad
Tech modernisation of election administration
Chronic distrust in public institutions
High levels of social polarisation
Campaign finance oversight
Delayed implementation of the DSA
Long-standing gaps in media ownership transparency

Figure 1: Vulnerabilities in the Czech Parliamentary Election

Drawing on the monitoring efforts of FDEI partners, Czech civil society organisations, and the analysis of 15 incident alerts, this report provides a comprehensive assessment of the FIMI environment surrounding the 2025 elections.[1] It examines the threat actor ecosystem,

[1] The monitoring of Czech information space conducted by FIMI Defenders for Election Integrity project partners was conducted from June 1 until October 31, 2025.

foreign and domestic enablers, narrative dynamics, structural vulnerabilities, and the impact of online platforms in shaping public perceptions. The report also evaluates responses by state institutions, civil society, and the EU-level Rapid Response System (RRS), identifying areas where interventions proved effective and where critical gaps remain.

Key findings of this assessment confirm that the elections were free, fair, and resilient. No evidence was identified of large-scale foreign interference capable of influencing the final vote. Technical *challenges*, such as the eDoklady outage, were caused by system overload rather than hostile activity. Civil society played a critical role in monitoring malign influence networks, while mainstream media outlets ensured high transparency through real-time reporting. Importantly, the Czech public demonstrated maturity and calm despite significant exposure to disinformation.

By integrating Czech-specific findings into a broader regional context, the report highlights the strategic continuity of Russian information operations across Central Europe and underscores the need for a whole-of-society approach to protecting electoral integrity. The Czech experience illustrates that foreign interference does not need to seek to alter votes directly; rather, it can aim to erode trust, foster divisions, and weaken democratic resilience over the long term. Understanding and addressing these dynamics is essential not only for future Czech elections but also for safeguarding the country's democratic institutions and its commitments within the EU and NATO.

1.1. Key Findings and SWOT Analysis

Strengths	Weaknesses
• Decentralised and transparent system of vote counting • Use of paper ballots that can be recounted if necessary • Well-administered and transparent electoral process that limited malign actors’ opportunity to interfere in the elections • Widespread public awareness of foreign malign influence • Citizens’ interest in elections and electoral campaigns • High levels of trust in, and independence of, the public broadcaster (TV and Radio) • Awareness of FIMI reflected in Czech security documents from 2016 onwards, followed by the establishment of specialised institutions	• Polarised political scene • Use of polarising narratives in electoral campaigns (for example regarding migrants and the war in Ukraine) • Narratives of electoral fraud and political capture of independent institutions were also spread by domestic political representatives • A high proportion of the population believes that Russia as well as the EU may attempt to manipulate the upcoming electoral process • Lack of information on postal vote for citizens living abroad served as a pretext for claims undermining electoral integrity • Delay in implementing the DSA, as the national legislation is still awaiting adoption • Media ownership and information space remain vulnerable to FIMI • Ongoing problems with transparency of campaign financing, including the involvement of third-parties • Election oversight bodies were understaffed and had limited authority, in case of the national DSA coordinator, as it was still awaiting adoption of necessary legislation • Smear attacks against independent public institutions have resulted in cautiousness and limitation of communication • Lack of information on DSA and RRS resulted in disinformation campaign against them

Opportunities	Threats
• Cooperation with civil society to build situational awareness and countering FIMI • Cooperation with the EU, in particular DG CONNECT’s DSA team, and use of its RRS ahead of the elections • EU Media Freedom Act implementation (from 8 August 2025, the regulation is to be fully applied in all EU countries)	• Several domestic political parties questioned the legitimacy of the electoral process • Smear campaign and attacks undermining the independence of public institutions and their activities, including those responsible for situational awareness, resilience-building, and countering FIMI • Politicisation of resilience-building and counter FIMI activities

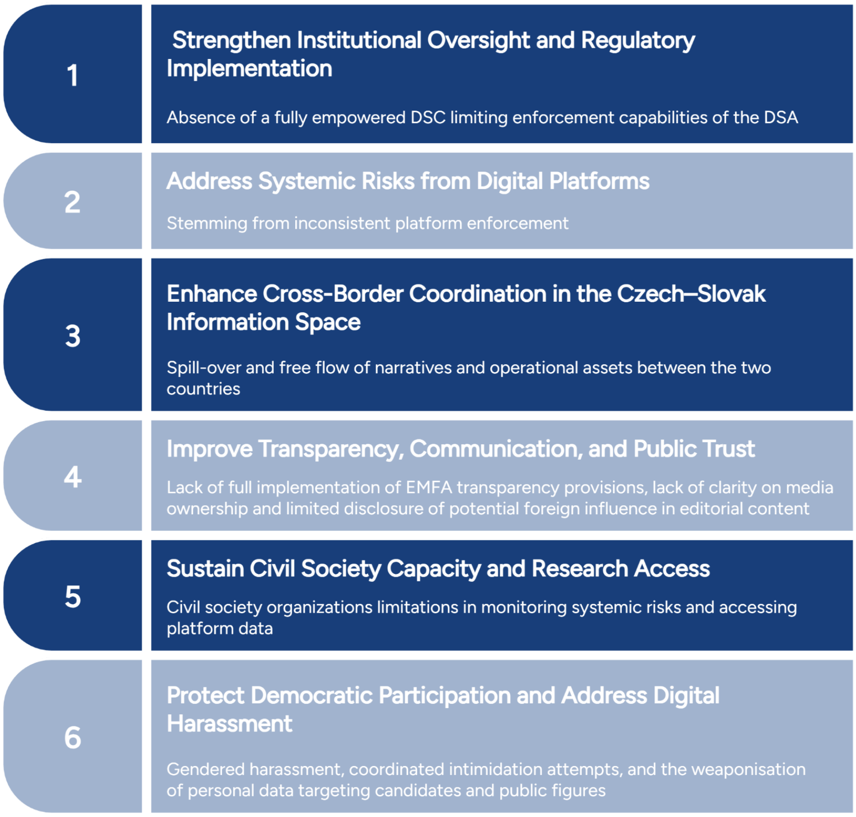
creating mandatory transparency requirements for media ownership ● Enhanced cooperation with FIMI-ISAC partners for cross-border threat detection ● Behavioural analysis frameworks (DISARM) for systematic TTP identification ● Presidential mandate through 2028 ensuring continuity in democratic defence messaging	● Long-term operations of foreign malign actors, particularly Russia ● Various known domestic actors, including a plethora of problematic websites and Telegram channels, contributing to and amplifying foreign malign influence operations ● Polarising narratives targeting the Ukrainian community and refugees, which could incite violence

Table 1: SWOT Analysis

1.2. Policy Implications and Recommendations

The 2025 Czech parliamentary elections revealed the notable resilience of Czech society and democratic processes in the face of continuous FIMI. However, the election also exposed structural weaknesses in the Czech information ecosystem, including gaps in platform accountability, incomplete implementation of EU regulatory frameworks, opaque online political advertising, and vulnerabilities exploited through cross-border information flows.

Addressing these weaknesses and policy gaps requires sustained institutional engagement, robust regulatory enforcement, and long-term investment in societal resilience. The following policy implications and recommendations outline measures to reinforce election integrity, strengthen institutional responses, and ensure that Czechia is equipped to counter evolving digital threats.



1 **Strengthen Institutional Oversight and Regulatory Implementation**

Absence of a fully empowered DSC limiting enforcement capabilities of the DSA

2 **Address Systemic Risks from Digital Platforms**

Stemming from inconsistent platform enforcement

3 **Enhance Cross-Border Coordination in the Czech–Slovak Information Space**

Spill-over and free flow of narratives and operational assets between the two countries

4 **Improve Transparency, Communication, and Public Trust**

Lack of full implementation of EMFA transparency provisions, lack of clarity on media ownership and limited disclosure of potential foreign influence in editorial content

5 **Sustain Civil Society Capacity and Research Access**

Civil society organizations limitations in monitoring systemic risks and accessing platform data

6 **Protect Democratic Participation and Address Digital Harassment**

Gendered harassment, coordinated intimidation attempts, and the weaponisation of personal data targeting candidates and public figures

Figure 2: Policy Implications and Recommendations

1.2.1. Strengthen Institutional Oversight and Regulatory Implementation

A critical structural gap during the electoral period was the absence of a fully empowered Digital Services Coordinator (DSC), limiting the state's ability to enforce the Digital Services Act (DSA). Full implementation of DSA provisions is essential to enable systematic oversight of major platforms, support incident escalation, and ensure access to data necessary for independent monitoring.

Additionally, Czechia, along with other EU member states, should reinforce mechanisms for sanctions enforcement and monitoring of foreign-linked media infrastructure. The rebranded outlet such as *neČT24* and platforms such as the *Pravda network* and *CZ24.news*, which launder pro-Russian content, continue to operate in the Czech information space despite sanctions on related entities. This illustrates the need for coordinated cross-border financial investigation, EMFA-compliant ownership transparency, and, where legally feasible, measures under DSA systemic risk obligations.

1.2.2. Address Systemic Risks from Digital Platforms

The elections highlighted ongoing vulnerabilities stemming from inconsistent platform enforcement. TikTok clusters promoting particular political actors, unlabeled online advertising targeting STAN party, and exploitation of Telegram channels demonstrated that platforms continue to struggle detecting and disrupting coordinated inauthentic behaviour (CIB), particularly when networks leverage cross-border audiences or rely on domestic amplifiers.

Platforms must therefore be held accountable for robust systemic risk assessment and mitigation under DSA Articles 34–35. This includes requirements for:

- transparent advertiser identity verification,
- consistent labelling of political advertising,
- detection of behavioural synchronisation across accounts, and
- structural disruption of coordinated networks rather than isolated post removal.

Furthermore, the Czech government should establish fast-track escalation mechanisms enabling law enforcement, the Czech Telecommunication Office (*CTU*), and the National Cyber and Information Security Agency (*NUKIB*) to report suspicious activity to platforms in real time, reducing the window available for operational migration.

1.2.3. Enhance Cross-Border Coordination in the Czech–Slovak Information Space

The Czech information environment remains deeply interconnected with Slovakia's, enabling spill-over and free flow of narratives and operational assets between the two countries. Mapping of the information space showed that problematic Slovak Facebook pages and Telegram channels frequently appear in Czech networks, and outlets such as *NewsFront SK* serve as cross-border vectors for malign influence.

Czechia should therefore establish a permanent cross-border threat-intelligence mechanism with Slovakia (and, where relevant, Hungary), building on FIMI-ISAC and EU-level structures. This mechanism should provide:

- quarterly joint threat briefings,
- shared monitoring of cross-border Telegram clusters,
- harmonised attribution standards, and
- automated alerts during electoral periods.

Without coordinated regional defences, malign actors will continue to exploit cross-border asymmetries.

1.2.4. Improve Transparency, Communication, and Public Trust

The eDoklady outage demonstrated how technical failures can quickly become a source for mis- and disinformation if institutional communication is delayed or unclear. Although public authorities responded effectively, the incident underscores the need for proactive, timely, and transparent public communication protocols for all critical digital systems.

Similarly, recurring narratives alleging electoral fraud or false narratives about the RRS highlight persistent public misperceptions of election procedures. Public institutions, both national and the EU, need to provide more information and explanatory materials on the electoral process and its oversight functions – detailing counting processes, safeguards against manipulation, and mechanisms for lodging complaints. Strengthening public understanding of electoral integrity, including the RRS, reduces the impact of long-term foreign efforts to undermine institutional trust.

Czechia needs to also fully implement European Media Freedom Act (EMFA) transparency provisions, improving media ownership visibility and disclosing potential foreign influence in editorial content.

1.2.5. Sustain Civil Society Capacity and Research Access

Civil society and independent researchers were instrumental in identifying malign influence networks, TikTok coordination patterns, and cross-platform narratives. However, their ability to monitor systemic risks is limited by inconsistent access to platform data and unstable funding.

Czechia (as well as other EU member states) should:

- provide long-term funding for FIMI monitoring, media literacy, and incident reporting,
- ensure full enforcement of DSA Article 40 to guarantee meaningful researcher access to platform data,
- support partnerships between civil society, academia, and state institutions.

These measures are essential for maintaining long-term situational awareness and rapid-response capacity.

1.2.6. Protect Democratic Participation and Address Digital Harassment

The elections revealed increased targeting of candidates and public figures with gendered harassment, coordinated intimidation attempts, and the weaponisation of personal data. Czech law does not yet comprehensively address these digital harms as threats to democratic participation.

Czechia should therefore:

- update legislation to explicitly classify gendered harassment, deepfakes, and targeted doxxing as offences linked to political interference,
- provide technical and legal support to candidates and parties experiencing cyber-enabled attacks,
- strengthen law enforcement competencies under Criminal Code §§180 and 181 for misuse of personal data and digital intimidation.

Establishing clear legal protections will help deter malign actors seeking to exploit societal vulnerabilities.

2. Incentives & Enablers of FIMI

Czech society withstood the vulnerability period of elections, and there was no evidence of large-scale coordinated foreign interference that could have influenced the vote. This does not mean that the threat in the country was averted. On the contrary, the absence of a one-off massive campaign indicates a change in tactics. Czechia remains an active ground for foreign actors due to a confluence of several factors – robust support for Ukraine, the complex relationship of the new government with the European Union, and long-term societal vulnerabilities and polarisation. With an increasing number of domestic actors, disinformation outlets, and political representatives spreading polarising narratives, foreign malign actors such as Russia have focused on long-term efforts to undermine public trust in institutions, media, the rule of law, and democratic processes, rather than on manipulating the election.

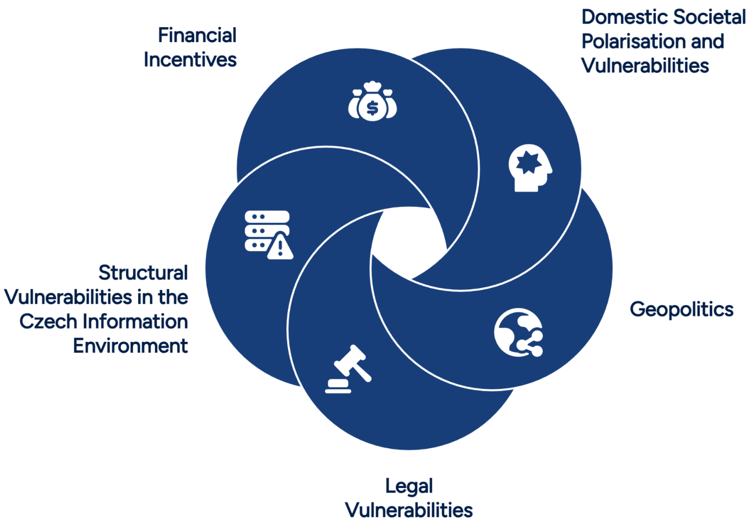

Financial Incentives
Domestic Societal Polarisation and Vulnerabilities
Structural Vulnerabilities in the Czech Information Environment
Geopolitics
Legal Vulnerabilities

Figure 3: Incentives and Enablers of FIMI

2.1. Domestic Societal Polarisation and Vulnerabilities

While Czech society is one of the more resilient in the Central and Eastern Europe (CEE) region, it has its own vulnerabilities that can be exploited by actors seeking to wage influence operations and deepen polarisation. In recent years, the Czech population has faced economic stagnation, unprecedented inflation, and rising energy costs, exacerbated by the war in Ukraine. According to research from April 2025, 56% of Czechs reported they could buy less with their salary than a year earlier.

A CEDMO's poll in September, conducted before the elections, revealed that 91% of respondents in Czechia do not believe that politicians keep their promises, more than 80% consider them to be calculating and pursuing their own interests, and 72% consider them to be very corrupt. Furthermore, 69% of respondents thought that Czechia is run by a few powerful interest groups. Such scepticism may be one of the factors enabling society's vulnerability to disinformation and influence operations, especially when accompanied by a lack of information. This was observed in connection with the introduction of the postal vote.

In the October 2025 parliamentary elections, Czech citizens living abroad had, for the first time, the opportunity to vote not only at embassies but also by post. According to CEDMO's polling conducted in July and August, 68% of respondents were unaware of the rules for voting by mail from abroad, and 48% feared fraud and manipulation in connection with the postal voting. The fear of postal vote manipulation was based on concerns of exchange or falsification of votes (73%), the loss or withholding of envelopes (40%), deliberate late delivery of votes (35%), or non-counting of votes due to formal errors (35%).

In addition, 65% of respondents also feared the negative influence of social networks, with 47% concerned that the elections would be manipulated by the government. This was the impact and resonance of the most influential disinformation narrative, that the upcoming election in October would be manipulated and/or stolen – a narrative that dates back to 2024. Please, find more information in the next chapter on narratives.

2.2. Geopolitics

Geopolitical concerns also fuelled anxieties in Czechia before the election. According to the Institute of Empirical Research (STEM) polling from July, 76% of Czechs expressed concerns about security, economic prospects, or personal health. The most serious threats identified were Islamic radicalism (55%), terrorism (54%), and an influx of illegal immigration (42%). Furthermore, a major challenge in recent years has been the influx of 400,000 Ukrainian refugees following the 2022 Russian invasion, which tripled the number of Ukrainians in the country. While most Czechs agreed that the state should temporarily host war refugees, 60% felt the country had accepted more refugees than it could manage.

Consequently, the topic of Ukrainians living in Czechia, their alleged advantages over Czech citizens and increased crime became part of the domestic political campaigns. Several false narratives about Ukrainians were disseminated by political representatives, including false claims that 50% of Ukrainian children do not attend school and alleged financial rewards for their families to increase their school attendance.

Support for Ukraine - both military and humanitarian - and Czechia's roles in NATO and the EU were central themes of the election campaign. As one of Ukraine's most committed and reliable allies, Czechia's continued assistance and its membership of NATO and the EU were openly debated. Nonetheless, President Petr Pavel affirmed a strong Western geopolitical orientation, vowing to use "his powers to keep the country anchored in NATO and the EU." In a televised address before the vote, he urged citizens to turn out and stressed the need for a government that would ensure security and protect Czechia's sovereignty within the community of democratic states, without yielding to Russia.

While anti-Ukrainian and other pro-Russian narratives were spread by known problematic and pro-Kremlin outlets in Czechia, these actors promoted selected political parties and representatives. Please, see chapter FIMI Targeting Czech Elections.

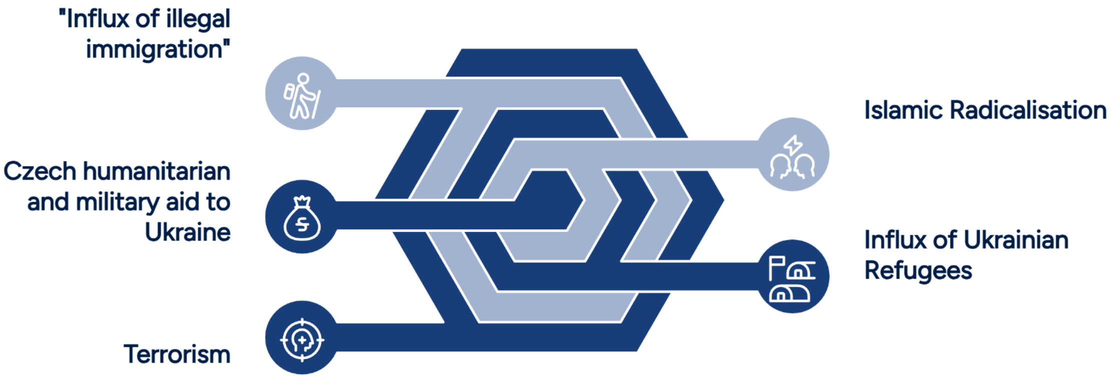

"Influx of illegal immigration"
Czech humanitarian and military aid to Ukraine
Terrorism
Islamic Radicalisation
Influx of Ukrainian Refugees

Figure 4: Public Concerns and Fears

2.3. Legal Vulnerabilities

The Czech Telecommunication Office (CTU) has been designated as the Digital Services Coordinator (DSC) responsible for supervising the implementation of the EU's Digital Services Act (DSA). During the electoral period, the regulator was in dialogue with major platforms (such as Facebook and TikTok) as well as the EU Commission to assess their readiness to meet stricter transparency and user protection obligations during the campaign. CTU is expected to enforce compliance with systemic obligations under the DSA, particularly mitigation of risks related to electoral integrity, disinformation, and protection of fundamental rights.

As the scope of the DSA was misinterpreted in Czech public debate, CTU launched a website explaining its basic principles (please, see the next chapter). However, CTU's ability to supervise the implementation of DSA was constrained by the fact that the necessary national *law* had not yet been adopted by parliament, despite being in the approval process since August 2024.

Given this delay, the European Commission had *launched* infringement proceedings against Czechia (along with four other Member States) on 7 May 2025 for failing to fully transpose the DSA into national law by the 2024 deadline, referring the case to the Court of Justice of the EU. As the law was not approved before the election, this limited CTU's ability to exercise the powers afforded by the DSA to address systemic risks to electoral integrity on social media platforms.

2.4. Structural Vulnerabilities in the Czech Information Environment

FIMI operations revealed critical gaps in Czech democratic resilience infrastructure:

- **Sanctions Evasion Through Rebranding:** Kremlin-connected outlets, like *neČT24* and *Pravda network,* operated openly within EU jurisdiction despite sanctions against Russian predecessors, using rebranding and proxy ownership mechanisms evaded enforcement. The EU regulatory framework lacked real-time detection and cross-border coordination capacity to match the rebranding cycle speed.

- **Platform Accountability Deficits:** Social media platforms TikTok, X, and Meta demonstrated limited proactive detection and disruption of coordinated inauthentic behaviour despite clear indicators (based on incidents analysed within the FIMI-ISAC monitoring): 140 of 146 TikTok accounts exhibited bot characteristics; 61 X accounts displayed synchronized cross-posting patterns; the anonymous X community demonstrated rapid narrative adaptation and coordinated amplification. Reactive, incident-by-incident enforcement enabled operational migration to fresh infrastructure before detection cycles completed.

- **Cross-Border Intelligence Coordination Gaps:** Slovakia–Czechia information spaces are highly *interconnected*, yet Czech authorities lacked real-time intelligence-sharing mechanisms with Slovak, Hungarian, or EU partners to anticipate and counter cross-border operations (*NewsFront SK, CzechFreePress, Libertas).*
- **Narrative Resonance:** The "Czechia First" narrative and "aid to Ukraine harms Czechs" messaging resonated because operations amplified authentic economic pressures (cost-of-living increases, defence spending concerns) while concealing

foreign origin attribution. Effective counter-messaging required a rapid, credible institutional response capacity that the Czech government struggled to mobilise.

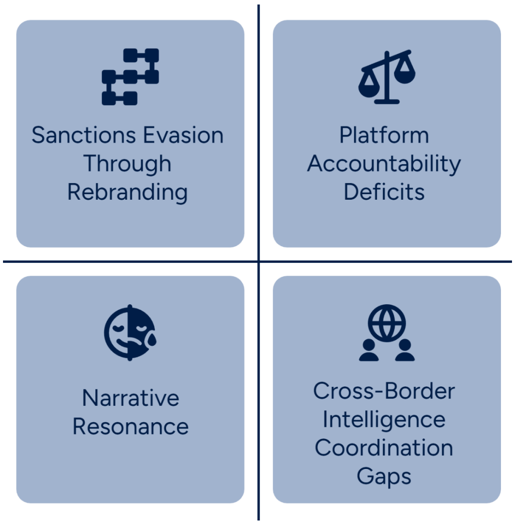

Sanctions Evasion Through Rebranding
Platform Accountability Deficits
Narrative Resonance
Cross-Border Intelligence Coordination Gaps

Figure 5: Structural Vulnerabilities in the Czech Information Environment

2.5. Financial Incentives

Financial incentives motivate various actors to spread polarising and problematic content and in the case of an electoral campaign, to support and agitate for a political party or representatives. This might include foreign-originated content and networks designed to amplify such content. During the electoral campaign, researchers from the Online Risk Labs *detected* several offers to earn money by supporting and liking particular influencers. Potential collaborators were approached via Telegram or WhatsApp to complete tasks on TikTok or Instagram. While such activities were not proven to be connected to a particular foreign malign actor, the example showcased that financial incentives were utilised to increase the perception of popularity of some influencers or products.

In addition, the "Šokující Česká 24" scam campaign illustrates how financial motives can intersect with disinformation tactics. A Facebook page promoted hundreds of deceptive ads using credible-looking domains to redirect users to fraudulent investment schemes. Although primarily criminal, the campaign impersonated political figures such as *Petr Pavel* and Vít Rakušan, eroding trust in democratic institutions and amplifying skepticism. Please, see chapter FIMI Targeting Czech Elections.

3. Threat Actors

3.1. Russia

Russia was identified as the *primary* threat actor conducting foreign information manipulation and interference (FIMI) in the 2025 Czech parliamentary elections using its developed networks and infrastructure within the Czech information space and society. While the parliamentary election occurred without significant Russian interference, that does not mean the Kremlin was not active. On the contrary, the *absence* of a one-off massive campaign or several campaigns indicates a change in tactics. Russian FIMI is a marathon, not a sprint. Their goal is not to influence one specific election, but to systematically erode the cohesion of society and its trust in democratic institutions, the media, and the rule of law over the long term.

3.2. Non-state Actors

During the election period, influence operations involved a diverse range of non-state actors operating within the information environment. A list of Czech websites known for spreading problematic content, including pro-Kremlin propaganda, is available on the *konspiratori.sk* (Conspirators) website, which as of 14 November 2025 included over 339 Czech and Slovak domains. Owing to the closeness of the Czech and Slovak languages, (dis)information from these sites can circulate seamlessly between the two countries – a dynamic frequently exploited by malign actors.

Some of these websites are primarily motivated by *money,* exhibiting an opportunistic approach aimed at generating ad revenue through the amplification of polarising or problematic narratives designed to attract clicks. Other problematic websites are ideologically and politically motivated, seeking to advance specific objectives that align with foreign actors. While some of these websites possess clear financial, personal, or partnership ties to hostile foreign actors, others are more likely driven by a shared ideological outlook without direct affiliation.

Furthermore, a significant role in various influence operations is played by individuals who are ideologically aligned with the broader narratives of threat actors but not necessarily affiliated with them. These individuals are active participants in domestic public discourse on contentious topics such as migration and specific foreign conflicts[2]. Their legitimate engagement can lead them to post inflammatory and polarising content that, while reflecting their own views, inadvertently aligns with and can be used in broader foreign influence operations. Crucially, these ideologically aligned individuals also serve as authentic amplifiers, effectively bringing manipulated content into specific segments of Czech society.

[2] In 2020 Czech journalists uncovered the identity of the person behind the *Aeronet* disinformation server, a major Czech-language site spreading pro-Kremlin narratives. The operator, Marek Pešl, was tracked down in Trenčín, Slovakia. He admitted being contacted by a nationalist group in 2014 but denied any Russian involvement, claiming the group was Czech.

4. Foreign Information Manipulation and Interference (FIMI) Targeting the 2025 Czech Parliamentary Elections

The 2025 Czech parliamentary elections (3–4 October) occurred within a sophisticated foreign information manipulation and interference (FIMI) ecosystem characterized by systematic coordination, multilayered infrastructure, and strategic alignment with Russian geopolitical interests [T0002 Facilitate State Propaganda, T0095 Develop Owned Media Assets, T0098.002 Leverage Existing Inauthentic News Sites]. This chapter synthesises documented incidents to demonstrate that FIMI targeting Czechia represents not episodic interference but a mature, standing architecture permanently positioned to exploit electoral moments and reshape Czech strategic orientation [T0059 Play the Long Game, T0074.002 Domestic Political Advantage].

Analysis of 15 discrete incidents reveals an integrated FIMI pipeline whereby Russian state-linked sources disseminate narratives through Slovak and Czech proxy outlets, which are then amplified via coordinated social media networks (TikTok, X, Telegram) and subsequently penetrate mainstream political discourse [T0119.002 Post across Platform, T0102.001 Use Existing Echo Chambers/Filter Bubbles, T0049 Flood Information Space]. This infrastructure pursued four core strategic objectives: (1) electoral manipulation favouring pro-Kremlin political actors [T0136.005 Cultivate Support for Initiative], (2) erosion of Czech support for Ukraine and EU-NATO alignment [T0079 Divide], (3) delegitimization of democratic institutions and electoral integrity [T0066 Degrade Adversary, T0139.001 Discourage], and (4) societal polarisation along identity and security fault lines [T0135.004 Polarise, T0081.006 Identify Wedge Issues].

The operations exploited critical vulnerabilities including sanctions evasion through media rebranding [T0128.004 Launder Information Assets, T0128.005 Change Names of Information Assets], inadequate platform accountability for coordinated inauthentic behaviour [T0049.003 Bots Amplify via Automated Forwarding and Reposting, T0049.005 Conduct Swarming], insufficient cross-border intelligence coordination [T0119.002 Post across Platform, T0092 Build Network], and the resonance of economic anxiety narratives [T0083 Integrate Target Audience Vulnerabilities into Narrative, T0072.003 Economic Segmentation]. While individual incident reach metrics ranged from thousands to low millions, the cumulative structural impact proved substantial through narrative consolidation, ecosystem resilience, targeted wedge-driving, and systematic corrosion of institutional trust [T0102.002 Create Echo Chambers/Filter Bubbles, T0060 Continue to Amplify].

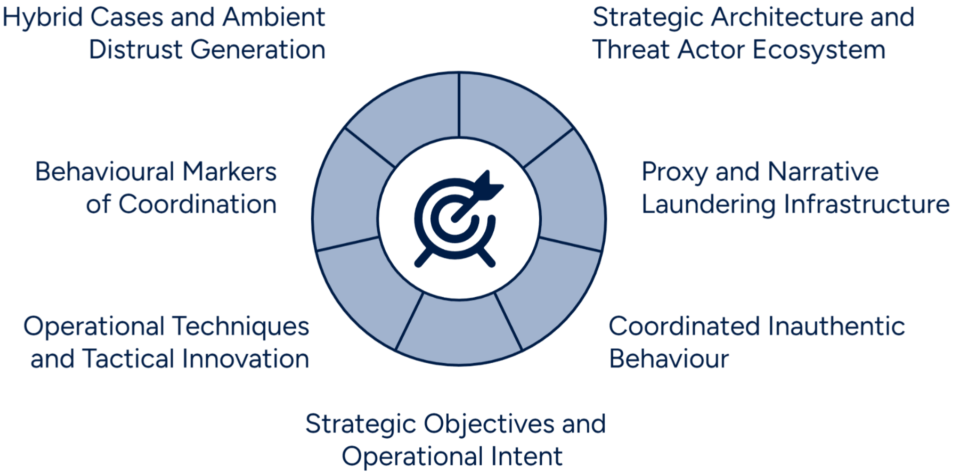

Hybrid Cases and Ambient Distrust Generation
Strategic Architecture and Threat Actor Ecosystem
Behavioural Markers of Coordination
Proxy and Narrative Laundering Infrastructure
Operational Techniques and Tactical Innovation
Coordinated Inauthentic Behaviour
Strategic Objectives and Operational Intent

Figure 6: FIMI Targeting the Czech 2025 Parliamentary Elections

4.1. Strategic Architecture and Threat Actor Ecosystem

4.1.1. Russian State-Linked Infrastructure

neČT24/42tcen.com represented the most prominent Russian state-linked entity operating in the Czech information space. Confirmed by the Czech Intelligence Service (BIS) as "an information channel directly connected to the Russian state apparatus," *neČT24* emerged on 17 March 2022 as the successor to EU-sanctioned Sputnik CZ, maintaining the identical editorial team and operational mandate [T0128.004 Launder Information Assets, T0128.005 Change Names of Information Assets, T0128.002 Conceal Network Identity]. By August 2025, the outlet operated across multiple platforms: Telegram (>30,000 subscribers), X (2,400 followers), and a newly created Facebook page (launched 29 August 2025) designed to maximise pre-election reach among less digitally sophisticated demographics [T0119.002 Post across Platform, T0122 Direct Users to Alternative Platforms, T0072.002 Demographic Segmentation].

While during September 2025, *neČT24* published 20 election-related articles, 17 of which featured interviews with Czech and Slovak politicians, the outlet was more active on its Telegram channel. The outlet's concealment of Sputnik heritage enabled it to masquerade as "independent Czech media" while functioning as a state-aligned propaganda infrastructure [T0097.202 News Outlet Persona, T0095 Develop Owned Media Assets].

NewsFront SK is a Crimea-based outlet linked to the Russian security services (FSB) operating in several languages. A Slovak-language version, hosted at sk.news-front.su, attracts around 95,000 visits per month, according to SimilarWeb data. It orchestrated sophisticated trans-border operations positioning post-election Czechia as a component of a Hungary–Slovakia–Czech "peace bloc." The operation employed source legitimacy spoofing technique: selective quotation of Western-branded outlets (*NZZ, Responsible Statecraft, Brussels Signal*) to validate Kremlin-favourable claims, followed by amplification through Czech-language channels (*CZ24.news, Pravda network*) to simulate authentic regional consensus [*T0084.004 Appropriate Content*, *T0023.001 Reframe Context*, *T0118 Amplify Existing Narrative*]. Individual Telegram posts on Czech channels recorded 4,150–4,800 views, with cumulative exposure enhanced through multi-platform mirroring across 3–6 outlets per narrative item [*T0119.001 Post across Groups*].

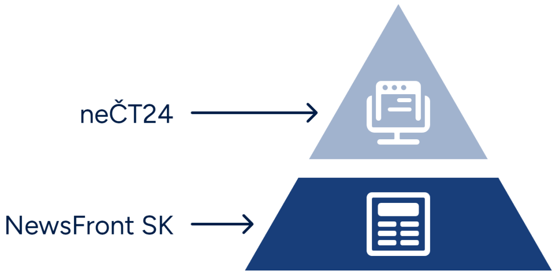


Figure 7: Strategic Architecture and Threat Ecosystem

4.2. Proxy and Narrative Laundering Infrastructure

4.2.1. Pravda Network

Pravda network (czechia.news-pravda.com), a part of large-scale Russian influence operation, functioned as content laundering infrastructure [*T0049.007 Inauthentic Sites Amplify News and Narratives*, *T0098.002 Leverage Existing Inauthentic News Sites*, *T0121.001 Bypass Content Blocking*].

According to GLOBSEC research, as of August 2025 *Pravda network* had published more than 8.5 million articles – around 1.7 million on its main domain and the remainder across its subdomains [*T0096.001 Create Content Farms*, *T0085.008 Machine Translated Text*]. Since its launch on 22 March 2024, the Czech subdomain alone has produced over 234,500 articles, ranking it ninth overall and fourth among country-specific feeds, just behind the

USA, Serbia, and Italy. The high output places Czechia prominently in *Pravda network's* disinformation ecosystem.

Although major Russian outlets such as *TASS, RIA,* and *Lenta* dominate its content, the Czech node also relies heavily on local Telegram channels. Importantly, republication by the *Pravda network* does not imply consent or awareness by the channel administrators – it merely reflects which narratives Kremlin propagandists seek to amplify [*T0084 Reuse Existing Content*, *T0060 Continue to Amplify*].

Between 1 September and 9 October 2025, the platform republished over 200,000 items, including 822 election-specific posts. Systematic content analysis revealed pronounced editorial bias towards particular domestic political representatives – 83.67% of Babiš-related content expressed positive sentiment, while 80.30% of content mentioning Prime Minister Fiala was negative [*T0136.005 Cultivate Support for Initiative*, *T0066 Degrade Adversary*]. More than one-third of republished material originated from neČT24's Telegram channel, creating circular amplification loops that magnified reach while obscuring foreign origin [*T0102.002 Create Echo Chambers/Filter Bubbles*, *T0119.002 Post across Platform*, *T0049 Flood Information Space*].

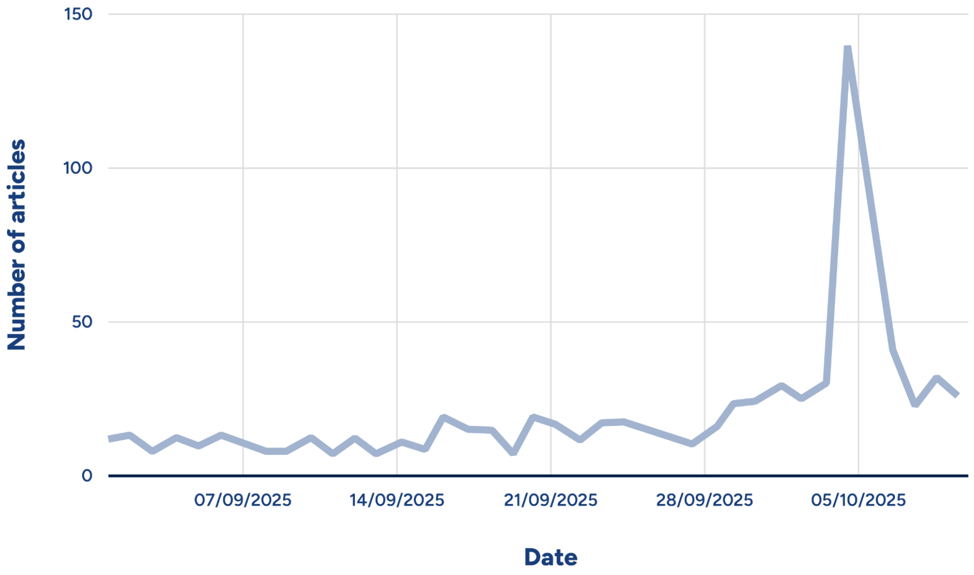


Figure 8: Number of Articles Related to the Elections on the Czech Pravda News Website per Day Between 1 September and 9 October 2025

Top Telegram sources feeding the Czech *Pravda network* included *neČT24*, *News 22*, *Edita Fefe*, etc., indicating systematic ingestion from Telegram into web properties [*T0115.003*

One-Way Direct Posting]. The table below provides a list of **the top 15 Telegram channels involved in the Czech *Pravda* network** and the number of posts they published between 1 September and 9 October 2025.

	Name of Telegram channel	Source	Number of posts	Number of followers
1	*neČT24*	*https://t.me/neCT24*	286	33 088
2	News 22	*https://t.me/news_22_faraon*	77	1 628
3	Edita Fefe	*https://t.me/EditaFeferonka*	38	913
4	Co neMÁTE vědět	*https://t.me/coNemateVedet*	32	8 269
5	Selský Rozum	*https://t.me/selskyrozum*	30	13 928
6	Milan Krajča	*https://t.me/milankrajcacz*	29	119
7	Libertas info-cz	*https://t.me/Libertas_info_cz*	20	1 143
8	MG – zprávy 24/7 bez cenzury!	*https://t.me/MGzpravy*	15	8 471
9	To je náš svět	*https://t.me/to_je_nas_svet*	13	12 519
10	Co kdyby	*https://t.me/jarek53*	13	9 131
11	Martha Scholler	*https://t.me/BN4JeyTQ6RVkMTNk*	13	10 674
12	RT Russian	*https://t.me/rt_russian*	12	1 055 447
13	Lomovka	*https://t.me/lomovkaa*	11	332 316
14	Ukrajina bez cenzury	*https://t.me/uk100a*	9	4 413
15	СОЛОВЬЁВ	*https://t.me/SolovievLive*	9	1 239 221

Table 2: Top 15 Telegram Channels Involved in the Czech Pravda Network

4.2.2. CZ24.news

CZ24.news served as the primary relay infrastructure for Slovak *NewsFront* content into the Czech information space, with individual Telegram posts recording 4,150–4,800 views across 30,500 subscribers [*T0049.007 Inauthentic Sites Amplify News and Narratives*, *T0102.001 Use Existing Echo Chambers/Filter Bubbles*].

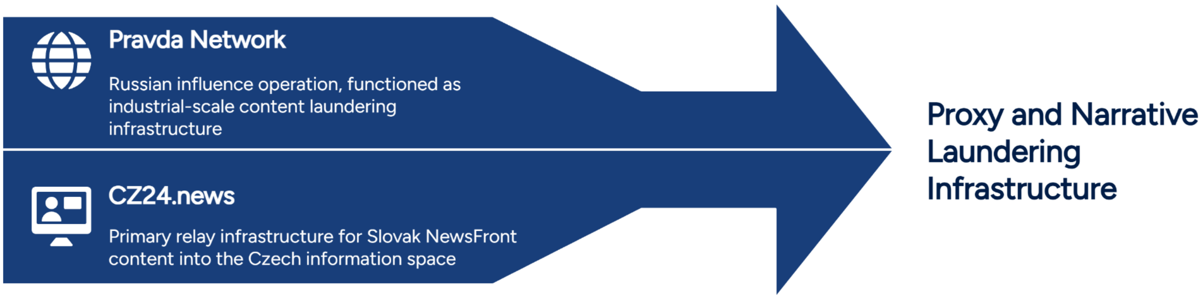

Pravda Network
Russian influence operation, functioned as industrial-scale content laundering infrastructure
CZ24.news
Primary relay infrastructure for Slovak NewsFront content into the Czech information space
Proxy and Narrative Laundering Infrastructure

Figure 9: Proxy and Narrative Laundering Infrastructure

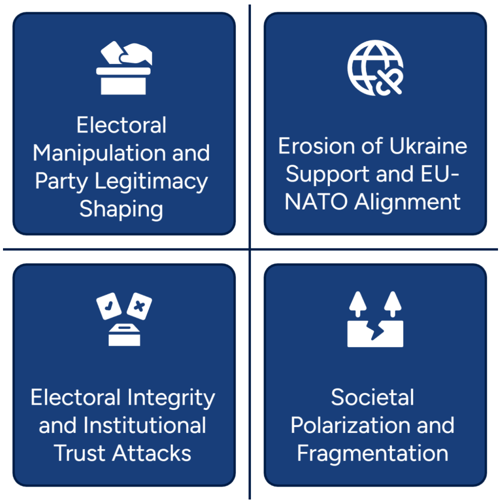
4.3. Coordinated Inauthentic Behaviour (CIB)

TikTok Network: 146 coordinated accounts demonstrated industrial-scale automation targeting younger demographics. Cumulative metrics included 309,000 followers, 10.55 million likes, and 76,000 videos. Manual and algorithmic analysis identified 140 of 144 flagged accounts as "LIKELY_BOT" based on behavioural markers – high posting velocity, minimal personal content, repetitive political hashtag deployment (#czechelections), and incomplete biographical information, also 43% of accounts were created in 2025, indicating deliberate pre-electoral deployment [*T0093.002 Acquire Botnets*, *T0049.003 Bots Amplify via Automated Forwarding and Reposting*, *T0049.002 Flood Existing Hashtag*, *T0072.002 Demographic Segmentation*]. Content ranged from political memes to AI-generated smear material designed to exploit TikTok's "For You" algorithmic recommendation system [*T0121 Manipulate Platform Algorithm*, *T0086.001 Develop Memes*, *T0087.001 Develop AI-Generated Videos (Deepfakes)*].

X Bot/Amplifier Cluster: 61 accounts executed systematic cross-platform content laundering, reposting TikTok videos from 403 unique channels onto X/Twitter. Entity analysis revealed 530 mentions of "Russia" and 401 of "Ukraine," with heavy symbolic signalling (🇨🇿 613 emojis, 🇷🇺 535 emojis). The network accumulated 930,000 views over 30 days, simulating distributed grassroots support for pro-Russian and anti-establishment positions while maintaining individual account plausible deniability [*T0119.002 Post across Platform*, *T0049.003 Bots Amplify via Automated Forwarding and Reposting*, *T0049.005 Conduct Swarming*, *T0060 Continue to Amplify*].

Anonymous X Community: Approximately 70 pseudonymous Czech-language accounts formed a loose but coordinated collective republishing Russian official statements (from Vladimir Putin, Dmitry Medvedev, and Russian parliamentarian Elena Panina), translating Telegram content, and executing rapid narrative adaptation to breaking events. Between 1 September and 10 October, the community published 3,194 election-related posts, with the highest-reach account (neČT24) accumulating 1,177,976 views [*T0091.003 Enlist Troll Accounts*, *T0068 Respond to Breaking News Event or Active Crisis*, *T0118 Amplify Existing Narrative*].

4.4. Strategic Objectives and Operational Intent



Electoral Manipulation and Party Legitimacy Shaping

Erosion of Ukraine Support and EU-NATO Alignment

Electoral Integrity and Institutional Trust Attacks

Societal Polarization and Fragmentation

Figure 10: Strategic Objectives and Operational Intent

4.4.1. Electoral Manipulation and Party Legitimacy Shaping

FIMI operations showed systematic amplification asymmetry favouring selected political parties, mainly from the opposition. From the monitoring of information space and pro-Kremlin problematic websites, it was possible to observe that these outlets were supporting political parties or representatives, for example, by conducting interviews with them, while attacking representatives of governmental parties.

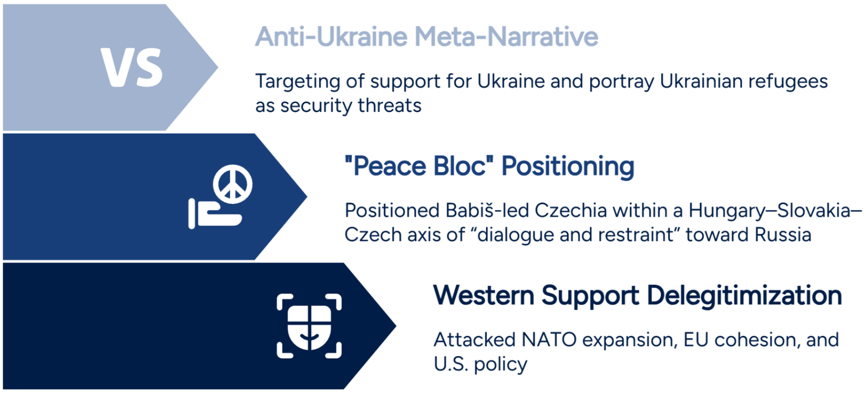
Pravda network data revealed 83.67% of Andrej Babiš-related content expressed positive sentiment, with coverage emphasising his opposition to Ukraine support and scepticism toward NATO commitments. *neČT24* granted repeated interview platforms to Babiš and other ANO officials during the final three weeks of campaigning to maximize pre-vote impact. *Rossiyskaya Gazeta's* 1 October endorsement explicitly positioned Babiš as Russia's preferred outcome, framing him as a mechanism to reduce EU-NATO unity and halt military support to Ukraine [*T0136.005 Cultivate Support for Initiative*, *T0002 Facilitate State Propaganda*].

On the other hand, Prime Minister Fiala and party ODS faced systematic negative framing (80.30% negative mentions on Pravda network). President Petr Pavel was portrayed as a Western puppet and manipulator. TikTok bot network consistently framed coalition parties SPOLU, STAN, and Pirates as corrupt. Bot cluster on social media platform X and anonymous community on the same platform labelled pro-Ukraine politicians as "traitors" [*T0066 Degrade Adversary*, *T0135.001 Smear*, *T0140.003 Spread Hate*].

4.4.2 Erosion of Ukraine Support and EU-NATO Alignment

Nearly all identified FIMI operations converged on undermining Czech support for Ukraine and normalizing Russia as a legitimate geopolitical actor:

- **Anti-Ukraine Meta-Narrative:** Ecosystem-wide messaging promoted the frame: "aid to Ukraine depletes Czech resources, harms ordinary citizens economically, and threatens to drag the country into war." *Pravda network* consistently characterized Ukraine support as reckless; *neČT24* promoted claims of corruption in Czech ammunition aid programs; *CzechFreePress* republished Russian narratives depicting Ukraine as an aggressor state; X anonymous community systematically portrayed Ukrainian refugees as ungrateful criminals and security threats [*T0083 Integrate Target Audience Vulnerabilities into Narrative*, *T0023 Distort Facts*].
- **"Peace Bloc" Positioning:** *NewsFront SK* positioned Babiš-led Czechia within a Hungary–Slovakia–Czech axis of "dialogue and restraint" toward Russia, implicitly contrasted with EU/NATO "war policy." The narrative exploited linguistic and cultural affinity between neighbouring states to create an appearance of regional consensus for Russian-favourable outcomes [*T0023.001 Reframe Context*, *T0118 Amplify Existing Narrative*].
- **Western Support Delegitimization:** Content spread by these pro-Kremlin and problematic outlets systematically attacked NATO expansion, EU cohesion, and U.S. policy. TikTok and X networks framed EU/NATO as "hostile to Czech sovereignty" and promoted narratives of "globalist elites" undermining Czech independence, with particular targeting of younger demographics where information literacy tends to be lower [*T0075.001 Discredit Credible Sources*, *T0135.004 Polarise*, *T0072.005 Political Segmentation*].



Anti-Ukraine Meta-Narrative

Targeting of support for Ukraine and portray Ukrainian refugees as security threats

"Peace Bloc" Positioning

Positioned Babiš-led Czechia within a Hungary–Slovakia–Czech axis of "dialogue and restraint" toward Russia

Western Support Delegitimization

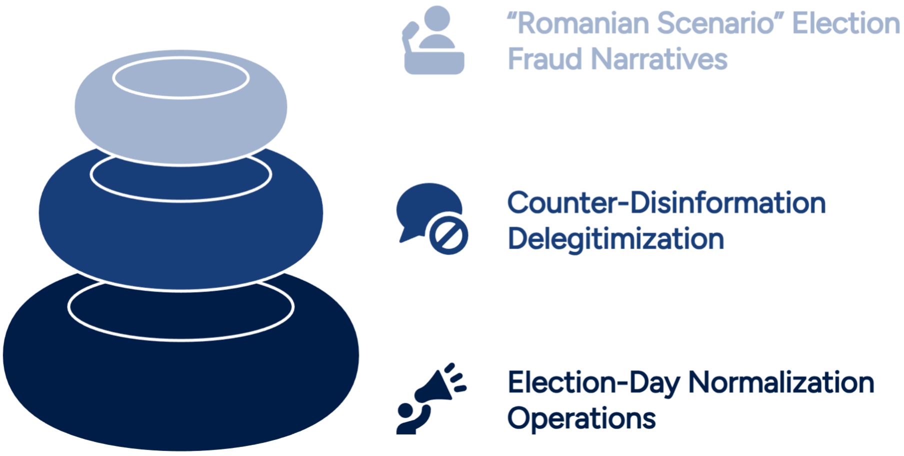
Attacked NATO expansion, EU cohesion, and U.S. policy

Figure 11: Erosion of Ukraine Support and EU-NATO Alignment

4.4.3. Electoral Integrity and Institutional Trust Attacks

Critical operational strands of these problematic websites and channels explicitly targeted confidence in electoral processes and democratic institutions:

- **"Romanian Scenario" Election Fraud Narratives:** *neČT24* published multiple posts (28–30 September) claiming the Constitutional Court, Rapid Response System, and government were preparing to "steal" the election using the December 2024 Romanian annulment as a template. Posts achieved 7,500–8,000 Telegram views [*T0022.002 Develop Original Conspiracy Theory Narratives*, *T0023 Distort Facts*].
- **Counter-Disinformation Delegitimization:** *neČT24* spread a "censorship" narrative, casting the RRS as an instrument of state oppression aligned with the United States and Brussels interests. This messaging served dual purposes – discrediting FIMI-resilience measures and normalizing the frame that legitimate counter-disinformation work equals authoritarianism [*T0075 Dismiss*, *T0075.001 Discredit Credible Sources*].
- **Election-Day Normalization Operations:** On 4 October (election day), *neČT24* published an *interview* with Russian political scientist Vadim Trukhachev normalising pro-Kremlin positions during the most sensitive electoral moment [*T0097.108 Expert Persona*, *T0045 Use Fake Experts*]. Content was republished by four problematic outlets (A*sociace nezávislých médií, Pravý prostor, Právě dnes, Oral.sk*), creating echo chamber amplification [*T0119.001 Post across Groups*].



“Romanian Scenario” Election Fraud Narratives
Counter-Disinformation Delegitimization
Election-Day Normalization Operations

Figure 12: Electoral Integrity and Institutional Trust Attacks

4.4.4 Societal Polarization and Fragmentation

FIMI operations pursued behavioural manipulation designed to fracture social cohesion:

- **Ukrainian Refugee Vilification:** X anonymous community systematically dehumanised Ukrainian refugees, labelling them “Banderites,” comparing them to animals, and framing them as crime and economic burden sources. Messaging weaponised authentic societal tensions around migration and integration [*T0140.003 Spread Hate*, *T0135.004 Polarise*].
- **Elite Delegitimization and Violence Normalization:** Content across platforms labelled pro-Ukraine politicians and journalists as “traitors,” characterised the government as “corrupt and criminal,” and called for “mass arrests and investigations” post-election. Rhetoric normalised political violence and delegitimized democratic contestation norms [*T0066 Degrade Adversary*, *T0140.001 Defame*, *T0138.002 Provoke*].
- **Economic Anxiety Exploitation:** “Czechia First” narratives (prominent on *Pravda network*) leveraged legitimate cost-of-living concerns and defence spending pressures, arguing that Ukraine support was economically reckless. By linking material hardship to specific policy choices, operations weaponized economic vulnerability for electoral and geopolitical objectives [*T0072.003 Economic Segmentation*, *T0083 Integrate Target Audience Vulnerabilities into Narrative*].

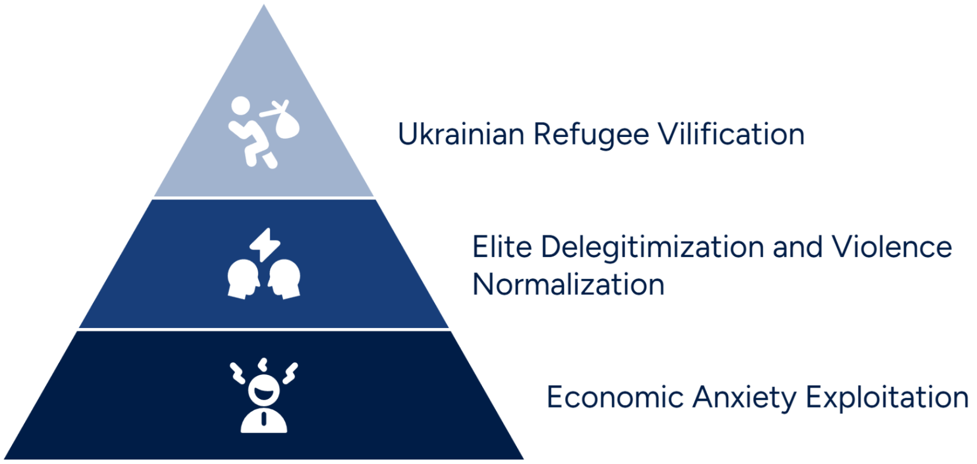

Ukrainian Refugee Vilification
Elite Delegitimization and Violence Normalization
Economic Anxiety Exploitation

Figure 13: Societal Polarisation and Fragmentation

4.5. Operational Techniques and Tactical Innovation

4.5.1. Sanctions Evasion Through Rebranding and Proxy Networks

- **neČT24 Succession Model:** Following March 2022 EU sanctions on *Sputnik CZ, neČT24* emerged immediately (17 March 2022) as a direct successor, operated by an identical editorial team pursuing unchanged strategic objectives. The transition was explicitly described in *Sputnik's* own announcement as a sanctions-evasion tactic. Multi-platform expansion strategy – Telegram, X, website, Facebook – ensured demographic penetration across age cohorts and digital sophistication levels [*T0128.004 Launder Information Assets*, *T0128.005 Change Names of Information Assets*, *T0122 Direct Users to Alternative Platforms*, *T0114.001 Social Media*]. For more information, please check the *Country Election Risk Assessment* (CERA) report.
- **Pravda Network Industrial-Scale Laundering:** The platform's ingestion of 200,000+ items over 39 days (1 Sept–9 Oct 2025) demonstrated industrial automation, with coordinated content surges (25% election-related content posted on 4–5 October). This mechanism functioned as an information laundering pipeline – Telegram posts from pro-Kremlin channels were republished as "articles," lending false credibility while obscuring foreign origin. Circular amplification (more than one-third of content originated from *neČT24*) magnified reach geometrically [*T0049.007 Inauthentic Sites Amplify News and Narratives*, *T0096.001 Create Content Farms*, *T0085.008 Machine Translated Text*, *T0121.001 Bypass Content Blocking*].

- **CzechFreePress Wholesale Content Appropriation:** Website's verbatim reproduction of *Gazeta* articles without attribution exemplified wholesale content laundering – foreign propaganda acquired superficial Czech and Slovak origin markers and plausibility through translation and republication as ostensibly original Czech/Slovak journalism [T0084.002 Plagiarise Content, T0084.003 Deceptively Labelled or Translated].

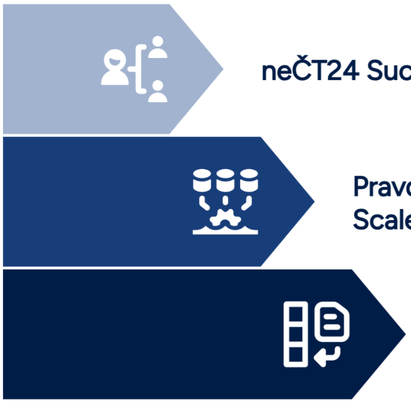

neČT24 Succession Model
Pravda Network Industrial-Scale Laundering
CzechFreePress Wholesale Content Appropriation

Figure 14: Sanctions Evasion through Rebranding and Proxy Networks

4.5.2. Cross-Platform Coordination and Amplification Cascades

- **Laundering content from TikTok on X**: 61-account X/Twitter cluster systematically reposted TikTok videos from 403 unique channels, creating a cross-platform amplification cascade that moved short-form propaganda into centralized public discourse platforms. 930,000 views across 61 anonymous accounts simulated distributed grassroots support while maintaining coordinated message discipline [T0119.002 Post across Platform, T0049.003 Bots Amplify via Automated Forwarding and Reposting, T0060 Continue to Amplify].
- **Multi-Platform Echo Chambers:** *NewsFront SK* content achieved cumulative exposure through systematic mirroring: original content is shared by *CZ24.news* relay, is laundered by *Pravda network* republication(s), amplified on Telegram channels, and cross-posted on X/Twitter. Each layer increased apparent legitimacy through repetition while obscuring foreign origin attribution [T0119.001 Post across Groups, T0102.002 Create Echo Chambers/Filter Bubbles, T0049 Flood Information Space].
- **Algorithmic Exploitation:** TikTok bot network exploited platform recommendation algorithms through hashtag flooding (#czechelections), high posting velocity, and

engagement manipulation (10.55 million cumulative likes) to achieve artificial prominence in "For You" algorithmic feeds targeting younger demographics with lower information literacy [*T0049.002 Flood Existing Hashtag*, *T0121 Manipulate Platform Algorithm*, *T0080.003 Identify Trending Topics/Hashtags*, *T0134.002 Social Media Engagement*].

4.5.3. Source Legitimacy Spoofing and Context Manipulation

- **Western Outlet Selective Quotation:** *NewsFront SK* selectively quoted Western-branded media (*NZZ, Responsible Statecraft, Brussels Signal*) out of context to legitimize Kremlin-favourable claims. This technique exploits an assumption that Western media carries credibility among Czech audiences sceptical of Moscow but receptive to "alternative" Western voices, enabling narrative laundering through superficial Western source attribution [*T0084.004 Appropriate Content*, *T0023.001 Reframe Context*].
- **Expert Impersonation:** Election-day publication of Vadim Trukhachev interview presented the Russian state university professor as a neutral analyst rather than a state-aligned commentator. Timing (election day) and republication across four outlets created a superficial expert consensus while concealing state linkage [*T0097.108 Expert Persona*, *T0045 Use Fake Experts*].

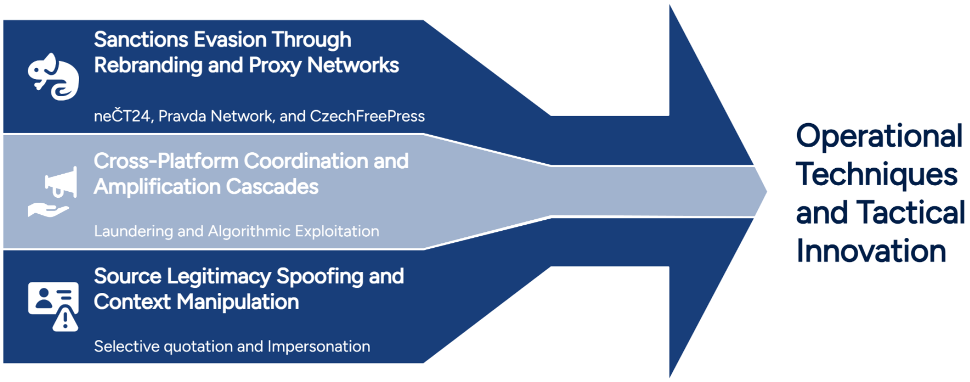

Sanctions Evasion Through Rebranding and Proxy Networks
neČT24, Pravda Network, and CzechFreePress
Cross-Platform Coordination and Amplification Cascades
Laundering and Algorithmic Exploitation
Source Legitimacy Spoofing and Context Manipulation
Selective quotation and Impersonation
Operational Techniques and Tactical Innovation

Figure 15: Operational Techniques and Tactical Innovation

4.6. Behavioural Markers of Coordination

Documented CIB networks exhibited characteristic coordination indicators:

- **Temporal Synchronization:** Coordinated posting surges aligned with campaign milestones (final week, election day, post-results) [*T0049.005 Conduct Swarming*].
- **Message Discipline:** Uniform anti-Ukraine, pro-Russia, anti-establishment framing despite account heterogeneity [*T0060 Continue to Amplify*].
- **Cross-Platform Link Sharing:** Systematic reposting of identical content URLs across nominally independent accounts [*T0119.002 Post across Platform*].
- **Symbolic Signalling Uniformity:** Extensive use of emoji – such as country flags (🇨🇿, 🇷🇺) – to create visual identification markers [*T0144.002 Persona Template*].
- **Velocity Patterns:** Posting rates inconsistent with organic human behaviour (42 daily posts for Libertas info-cz) [*T0049.008 Generate Information Pollution*].
- **Content Recycling:** Repetitive meme formats and hashtag templates across ostensibly independent accounts [*T0115.001 Share Memes*].

4.7. Hybrid Cases and Ambient Distrust Generation

Two following documented cases illustrate how actions in the information sphere share certain characteristics with FIMI and can inadvertently influence voters by amplifying ambient distrust. In these situations, electoral interference was not the primary intent of the actors, yet the resulting dynamics contributed to a climate of uncertainty and skepticism.

- **Stačilo! Data Leak:** On 1 October 2025, the Stačilo! movement accidentally *exposed* its supporters' personal data after leaving a file called *debug.log* on its official website stacilo.cz without access controls. This file contained a database of personal details of about 4,000 donors – including their names, email addresses, and home addresses – as well as technical references to two Slovakia-based companies (magastudio.sk and mediagrape.sk). Some researchers who examined the leaked data *suggested* these companies might have ties to Russia, but those claims have not been officially verified. If a Slovak company *were* to operate the website pro bono, such provision could constitute an impermissible in-kind contribution from a foreign source, which Czech law expressly prohibits. While primarily a data protection failure, the incident was amplified by content creators ("Prague Pérák," YouTuber Mikael Oganesjan) with coverage reaching 43,500 views (X thread) and 44,000 views (YouTube video). The case exemplifies how authentic vulnerabilities are repurposed into delegitimising narratives – incompetence (actual leak) was amplified to suggest foreign infiltration (unverified funding claims). This hybrid dynamic made it harder to attribute responsibility and could undermine trust in both the targeted group and the wider democratic system [T0042 Seed Kernel of Truth, T0023.001 Reframe Context, T0118 Amplify Existing Narrative].

- **"Šokující Česká 24" Scam Campaign:** The Facebook page *"Šokující Česká 24"* operated 316 deceptive Meta ads using credible-seeming domains spoofing (seznamzpravy.cz) redirecting to fraudulent investment schemes. Although primarily criminal rather than FIMI, the infrastructure – spoofed domains, cloaked ads, selective geolocation redirection – overlapped with disinformation tooling. Russian-language HTML comments and networks of similar domains targeting multiple countries suggested a broader organized crime infrastructure. Political figures (Petr Pavel, Vít Rakušan) were impersonated to drive engagement, undermining trust in democratic institutions and contributing to ambient scepticism [T0137.002 Scam, T0143.003 Impersonated Persona, T0114 Deliver Ads, T0123.004 Conduct Server Redirect].

These cases illustrate how ***criminal fraud and data security breaches*** operate within an integrated ecosystem that shares ***tooling, messaging infrastructure, and audiences*** with foreign information operations. Citizens encountering numerous manipulative patterns develop generalized distrust serving FIMI objectives, even when individual incidents lack state direction.

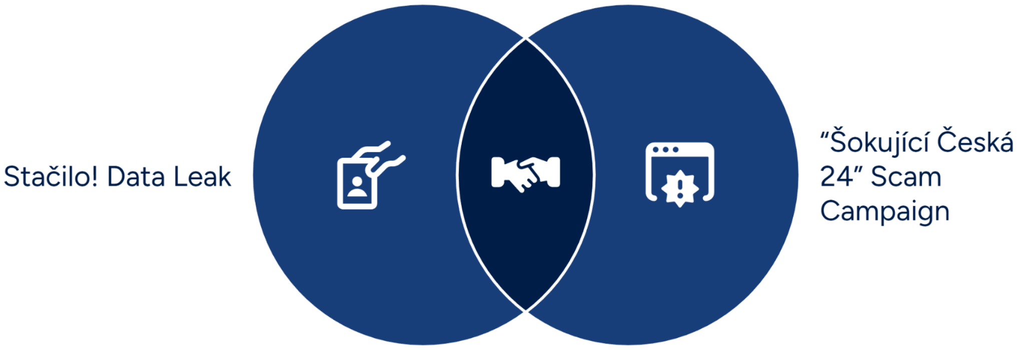


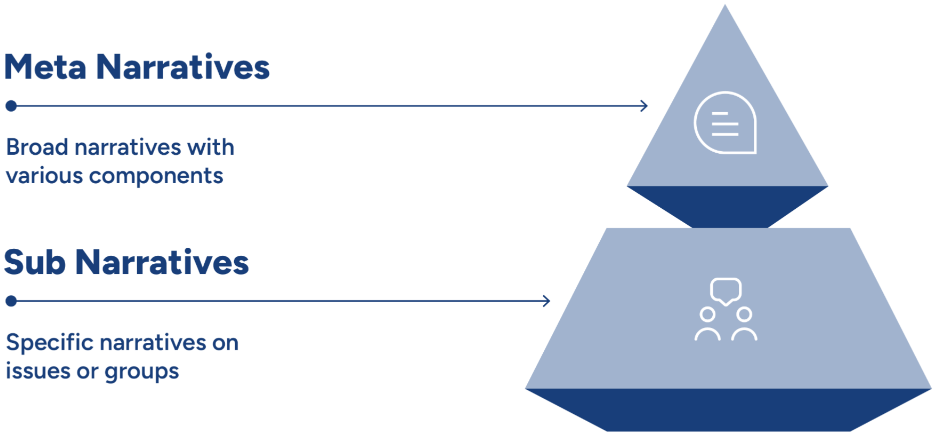
Figure 16: Hybrid Cases and Ambient Distrust Generation

5. FIMI Narratives Resonating in Czechia

This section outlines the key polarising meta- and sub-narratives currently circulating in Czech public discourse prior to the elections. These narratives were observed during monitoring of the information space conducted by FIMI Defenders for Election Integrity (FDEI) project partners as well as local Czech civil society organisations within their research activities. These narratives, amplified by problematic outlets and various political representatives, undermine trust in institutions, the electoral process, and the country's foreign policy. Although they do not always originate abroad, they can be exploited by foreign malign actors to deepen societal divisions and undermine democratic processes.

It is important to distinguish between meta-narratives and sub-narratives. Meta-narratives are broad storylines – such as delegitimising elections, portraying Ukraine as a failed state, or framing the EU as an oppressive "dictator" – while sub-narratives are the specific claims that reinforce them, such as false allegations of postal voting fraud or fabricated quotes from political leaders. Mapping both levels shows how fragmented incidents feed into a coherent, manipulative discourse, amplifying their overall impact.

- **Meta Narratives:** These are broad, overarching narratives composed of various components.
- **Sub Narratives:** These are more specific narratives focused on a particular issue, event, or targeted group.



Meta Narratives

Broad narratives with various components

Sub Narratives

Specific narratives on issues or groups

Figure 17: Narrative Hierarchy

FIMI, targeting the 2025 Czech election, employed three key meta-narrative themes: Election Manipulation, Anti-EU, and Anti-Ukraine. These narratives were further reinforced by sub-narratives specifically tailored to Czechia's October 2025 parliamentary election and information space. Together, meta and sub-narratives attempted to stir societal polarisation and spread distrust in political processes and public institutions. Often taken over by domestic political representatives, these narratives align with the geopolitical interests of foreign malign actors such as Russia.

5.1. Election Manipulation Meta-Narrative

This narrative asserted that elections would be manipulated through fraud or government interference and resonated due to low trust in institutions and controversies over postal voting. These narratives were spread mainly via social media, chain emails, and statements from political figures. A survey from early 2025 for the Czech Ministry of the Interior highlighted public concerns about the fairness of the upcoming elections. Respondents expressed doubts about several aspects of the voting process, including foreign interference, with 39% fearing manipulation by Russian influence operations and 78% worried about social media disinformation shaping voter decisions. Furthermore, 54% of respondents feared the government itself could influence results to stay in power.[3]

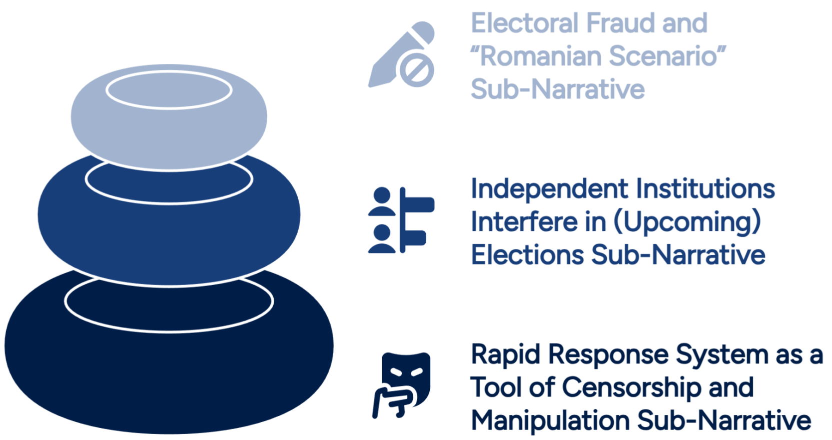

Electoral Fraud and "Romanian Scenario" Sub-Narrative
Independent Institutions Interfere in (Upcoming) Elections Sub-Narrative
Rapid Response System as a Tool of Censorship and Manipulation Sub-Narrative

Figure 18: Election Manipulation Meta-Narratives

[3] Please, see also Czechia's Country Election Assessment Report available at https://fimi-isac.org/wp-content/uploads/2025/09/FRT-24_Czechia-Country-Election-Risk-Assessment-CERA_FINAL.pdf

5.1.1. Electoral Fraud and "Romanian Scenario"

An important driver of speculations about electoral manipulations of the upcoming Czech parliamentary election was the situation in Romania, where the Constitutional Court *annulled* the first round of presidential elections in November 2024 due to Russian meddling. This decision was, however, *interpreted* by Czech problematic actors as an attempt by the Romanian deep state, directed by NATO, to target the far-right candidate, Calin Georgescu, who was allegedly against the development of the biggest NATO base in Romania. In addition, in an interview, Georgescu declared that he was stopped, because "they needed to *prevent* a peace deal in Ukraine". According to the narrative spread before elections in several European countries, Romania was supposed to serve as a blueprint for other countries, including Czechia.

The narrative about the "Romanian scenario" proved adaptable to unfolding events. In summer, the main attention has been dedicated to the postal vote for Czechs living abroad, which was perceived as easily manipulatable. This perception was shared by 48% of respondents of CEDMO's *opinion poll* conducted in the summer, who were convinced that the postal vote would lead to multiple instances of electoral fraud and manipulation. However, when the number of voters *registered* for a postal vote reached only 25,000 (far less than anticipated), attention to postal vote quickly declined since the influence on the results would have been negligible.

The narrative, however, *reemerged* in early September as the Constitutional Court dealt with the lawsuit against party Stačilo! (Eng. Enough!), which had candidates for multiple parties on its ballot. Therefore, it was argued that it should be registered as a coalition for which the threshold for entering the parliament is higher than 5% of votes. The Court, however, *decided* in a swift proceeding in favour of Stačilo! which for the most part silenced its *critics*. Yet the Constitutional Court's decision did not mean the disappearance of the "Romanian scenario" narrative.

5.1.2. Independent Institutions Interfere in (Upcoming) Elections

This sub-narrative accused various independent public institutions, overlooking also the enforcement of the rule of law like the Constitutional Court or the Security Information Service, of being politically captured and biased and thus of electoral interference. Spread by pro-Kremlin and problematic outlets as *neČT24* and *Aeronet*, such narratives were often amplified by domestic political *actors*, who gave interviews to such problematic outlets.

5.1.3. Rapid Response System as a Tool of Censorship and Manipulation Sub-Narrative

The launch of the EU's Rapid Response System (RRS) in Czechia was perceived as an attempt to censor the public and political debate before the elections and as a tool to manipulate the results of the election, as in Romania. Various actors, including *neČT24,* interpreted the activation of the RRS system as a sign that the country is following the Romanian example and claiming that the RRS itself is a threat to democracy. Therefore, when researchers from the Online Risk Labs detected a coordinated network of TikTok accounts, both the Czech intelligence services as well as the mainstream media were accused by various actors, including political representatives, of a false flag operation created as a pretext to annul the election results following the "Romanian scenario".

While the narrative resonated before the election, the results were undisputed. This narrative was amplified and in part constructed by the problematic outlet *neČT24* with ties to the Kremlin. Its website repeatedly provided a platform to domestic voices questioning electoral integrity, promoted these statements on its social media, or asked about the potential for electoral manipulations in interviews.

The narrative about election being stolen by nefarious actors has not completely disappeared, even after the election. When investigative journalists revealed past misdeeds of candidates for ministers, their supporters argued that they were trying to influence the electoral results and act against the will of the people. Therefore, it might be expected that the narrative about electoral manipulations will remain a part of the Czech public debate, which might have a detrimental effect on trust towards democratic institutions.

5.2. Anti-EU Meta-Narrative

Russian disinformation has been portraying the EU and the West as "decaying" and "corrupt", aiming to undermine them and elevate Russia as a morally superior actor. The anti-EU narratives spread in Czechia spoke about an "EU dictate" and its neocolonial policies undermining Czechia's sovereignty in various spheres – from energy policy to the ability to pursue closer cooperation with Russia.

5.2.1. The EU Manipulates Elections

With false and misleading information being spread in Czechia about the Rapid Response System of the European Union, mentioned previously, problematic actors have also spread a narrative that using the RRS the EU was allegedly manipulating the electoral campaign and interfering in elections. Various actors, including the *Society for the Defence of Freedom of Expression* or outlet Reports On-line, tried to portray the RSS as a non-transparent tool of the EU to exert control over social media before elections.

5.2.2. The EU Undermines Sovereignty and Exerts Neocolonialist Control

This narrative has been part of a long-standing Soviet-era repertoire, taken over by Russia, which portrays the West as colonialist regardless of context and presents the Soviet Union - now Russia - as an anti-colonial force. It was deployed to undermine and defame the European Union among voters, portraying it as a threat to Czechia's sovereignty and eroding public support. One example of this came from a post to the Telegram channel Libertas info-cz (which translates and launders content from Russian Telegram channels) where Ursula von der Leyen was compared to Emperor Palpatine from Star Wars, suggesting she is consolidating power in the EU under the guise of external threats and economic necessity.

5.3. Anti-Ukraine Meta-Narratives

Problematic outlets try to continuously portray Ukraine as corrupt, failing, and a burden on Czechia. Such narratives resonate due to economic concerns and migration pressures, and spread via pro-Kremlin outlets such as *pravda-cz.com*, *cz24.news*, and Telegram channels. Conversely, Russia was framed as a just, undefeated army. The Czech government, led by Prime Minister Petr Fiala, was depicted as betraying national interests by prioritising Ukraine and refugees over citizens' welfare.

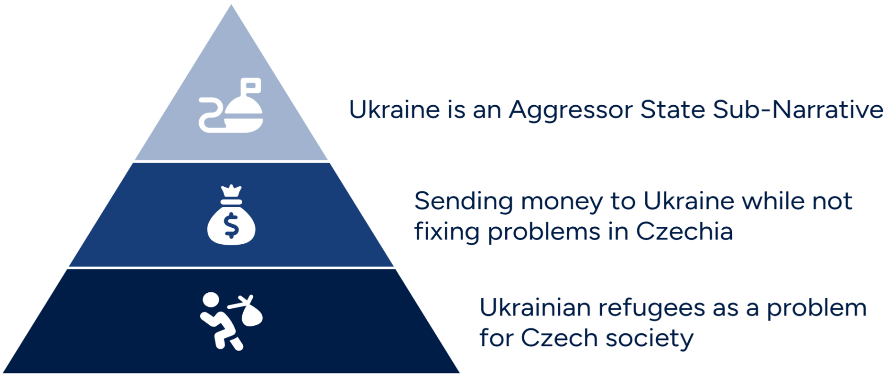

Ukraine is an Aggressor State Sub-Narrative
Sending money to Ukraine while not fixing problems in Czechia
Ukrainian refugees as a problem for Czech society

Figure 19: Anti-Ukraine Meta-Narratives

5.3.1. Ukraine is an Aggressor State

Problematic outlets have tried to portray Ukraine as an aggressive state, alleging that attacks perpetrated by Russia are Ukrainian attacks. The aim is to diminish Czech humanitarian and military support for Ukraine and support anti-Ukrainian sentiments among the population. For example, Ukraine was allegedly *painting* Ukrainian equipment with Russian flags to attribute the attacks to Russia.

5.3.2. Sending Money to Ukraine While Not Fixing Problems in Czechia

Pro-Kremlin problematic actors have been trying to stir anti-Ukrainian sentiments by spreading narratives that Czechia provides financial support to Ukraine. At the same time, this money is needed at home, for example, in healthcare. A *post to X by neČT24* (successors to the Russian state media Sputnik) claimed that 100 million euros was sent to Ukraine to modernise hospitals, while "in the Czech Republic we don't have enough medicines and staff."[4]

5.3.3. Ukrainian Refugees as a Problem for Czech Society

This narrative attempts to *portray Ukrainian refugees as a threat to Czech society*. Concerns over the Ukrainian mafia operating in Czechia, human trafficking, and economic exploitation of Ukrainian workers have been voiced by domestic political representatives, who pro-Kremlin outlets like *neČT24* amplified.

5.4. Why Do These Narratives Matter?

The FIMI narratives identified during the Czech parliamentary election undermined democratic processes, election integrity, and trust in institutions, while simultaneously fuelling societal polarisation.

[4] 'Regarding the dissemination of disinformation directly sponsored by Russia, channels connected to the Russian state maintained their activity. These included primarily successors to the Russian state media Sputnik, such as the website 42tcen.com and the Telegram channel neČT24'. Security Information Service of the Czech Republic, *Annual Report of the Security in Information Service for 2024*, p. 20

.

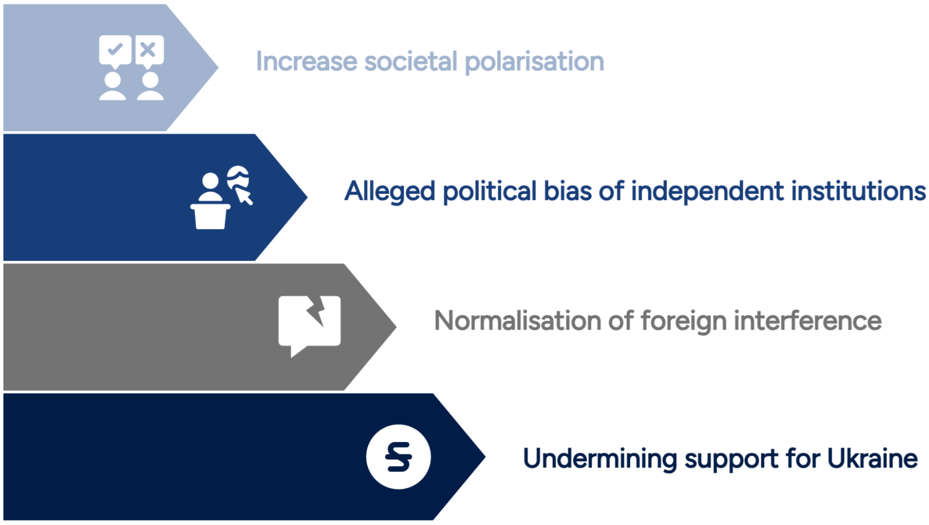

Increase societal polarisation
Alleged political bias of independent institutions
Normalisation of foreign interference
Undermining support for Ukraine

Figure 20: Why Do These Narratives Matter?

Increase societal polarisation

Narratives targeting the EU, the public institutions, and Ukraine or Ukrainian migrants spread polarisation by exploiting themes of loyalty and sovereignty. For instance, narratives criticising the implementation of EU policies are framed as the EU dictating and causing a loss of national sovereignty in a particular area. Similarly, anti-Ukrainian narratives heighten divisions by framing Ukraine as a regional security threat or alleging that it disguises its attacks as Russian ones, while promoting negative emotions against Ukrainian migrants living in the country and undermining Czechia's support of Ukraine in its fight against Russia.

The European Union is often a target of narratives that seek to generate distrust and polarisation, as its complex structure and decision-making process are often not understood by citizens and properly explained[5], thus providing an opportunity for the spread of false or misleading narratives by malign and populist actors. It is easy to undermine trust in an institution or a process amongst those who do not fully understand its inner workings. As such, this lack of understanding can allow threat actors to attribute the words and actions of a variety of actors to the Union, blaming it for a wide range of issues. The case of the Rapid Response System, how it operates, the fact that the discussions are happening behind closed doors and are not fully disclosed to the public, all

[5] Some of the recurring anti-EU narratives were also identified during the Romanian elections in 2024, see: B. Toma, *The European Union as a Disinformation Target: Key Narratives and Impacts Case study: Romania (2023-2024)*, Centrul Român de Politici Europene, p. 5.

have been misused to spread false narratives about censorship. According to polling conducted by CEDMO in September 2025, 36% of respondents were concerned that the elections would be manipulated by the European Union authorities if they did not like the results, while only 32% were concerned that the elections would be manipulated by information influence from Russia.

Alleged political bias of independent institutions

Smear attacks and accusations of political capture of independent institutions serve several purposes – undermine the trust in these institutions; undermine the trust in the rule of law and established checks and balances; and politicise and thus undermine perceptions of security threats and countermeasures that should be taken. According to CEDMO, 47% of respondents were concerned that the elections would be manipulated by a government that does not want to give up power and its supporters. Furthermore, narratives that frame the monitoring of social media platforms, protection of information space and take down of problematic illegal content as a threat to the freedom of speech attempt to underline the work of security institutions and civil society actors providing situational awareness. Accusations of alleged censorship and political bias often lead to self-censorship and a reduction of activities by public institutions.

Normalisation of foreign interference

'Whataboutist' narratives that claim various actors, including EU and NATO allies, meddle in domestic affairs work to justify and normalise foreign interference with the ultimate goal of diminishing resistance to these operations. By blurring the lines between legitimate international partnerships and cooperation and foreign malign interference, these campaigns make it harder for the public to recognise and reject external manipulation. This can open the door for more direct forms of foreign malign interference, such as illicit campaign financing, vote-buying, and the use of proxy political actors to circumvent electoral laws.

Undermining support for Ukraine

By portraying Ukrainians as a security threat, as a corrupt country or as an aggressor, pro-Kremlin actors attempt to undermine Czechia's support to Ukraine. Such narratives try to erode empathy with the victims of aggression and reduce public solidarity, and thus reduce Czechia's military and humanitarian support to Ukraine. Such narratives and their impact advance Russia's strategy of division beyond the battlefield.

Problematic and polarising activities weaponised existing societal grievances and anxieties to sow widespread distrust and fragmentation. Narratives matter immensely because they are fundamental to how individuals and societies understand the world, interpret events, and make decisions. Critically, they construct the shared understandings, norms, and perceptions that guide collective behaviour.

Unlike mere facts, narratives connect and frame disparate pieces of information and events into a coherent, often emotionally resonant, story. Information manipulation and propaganda aim to win the hearts and minds of people and are part of cognitive warfare, during which malign narratives not only try to manipulate perceptions of who is a friend and who is a foe, but also how people would react in times of crises.

For these malign and polarising narratives to be truly resonant, they depend not only on amplification through various channels and domestic actors, but also on their ability to exploit pre-existing societal vulnerabilities as distrust in institutions and political figures, utilise prevailing economic and social anxieties, and leverage confirmation bias by offering seemingly credible “proof” for existing suspicions. Their effectiveness is further amplified by the inherent complexity of governance of both domestic and international issues, and lack of good strategic communication on these issues.

The three meta-narratives outlined above aimed to erode trust in democratic institutions, undermine confidence in the electoral processes, and weaken Czechia’s ties to the EU and NATO. While some narratives stem from domestic grievances, they are regularly amplified or exploited by foreign malign actors, particularly pro-Kremlin ones.

Sub-narratives provided examples of manipulation was operationalised: lack of information on the postal vote and the Rapid Response System, smear campaigns accusing independent public institutions providing oversight and enforcement of the rule of law of political bias, narratives about censorship and “Romanian scenario” allegedly orchestrated by the EU, and anti-Ukrainian narratives utilising back economic situation and fears.

6. Unfair Conduct by Political Actors

FIMI incidents described in the report occurred in the context of the polarised electoral campaign. The antagonism between the government and opposition has been a constant feature of the electoral period 2021–2025, but the October election further exacerbated it. The polarised political debate also influenced popular sentiment, and the public has become divided into camps supporting either the government or the opposition. In this context, it is not surprising that narratives about manipulated elections capitalising on widespread distrust resonated.

The parties criticised not only the government but also sought support through polarising rhetoric targeting Ukrainian refugees (including their *children*) and their stance on the full-scale Russian invasion of Ukraine. Some political parties have in their ranks multiple individuals expressing pro-Russian views. For example, Ondřej Dostál, MEP for the party Stačilo!, *visited* Moscow in May 2025 to take part in the celebration of the end of World War II in Europe. On a similar pro-Kremlin note, the leader of Stačilo! Daniel Sterzik *wrote* in a discussion on Facebook, "so when the Russians come, only those who won't cooperate with them have to worry. I'm friends with the Russians, so I don't have to worry." When the media asked about this comment, Sterzik denied writing it. However, the news outlet Deník.cz claimed that based on available evidence it is clear that he was the author.

Such political representatives frequently *interacted* with problematic pro-Russian outlets in Czechia by providing them with interviews. Weeks before the elections, 22 such interviews were observed.

6.1. Non-Transparent Financing of Electoral Campaigns

Czech legislation sets limits on campaign spending and sets transparency requirements for party financing. However, according to the *assessment* of Transparency International, most political parties had serious problems with the transparency of their financing. The most problematic area is spending on advertising on social media, as the majority of parties do not publish the list of accounts using paid promotion. A further shortcoming is the lack of information about individuals or companies contributing to the preparation or delivery of campaigns. Although all parties are required to pay campaign expenses from transparent bank accounts, several are poorly organised, making it impossible to identify the final recipients of specific payments. To date, the Office for the Supervision of the Finances of Political Parties and Movements has largely limited *enforcement* to low financial penalties for minor breaches (e.g., missing advertiser information or the use of municipal newspapers for electoral campaigning). The Office will continue to review electoral budgets, as parties have three months after the elections to submit their financial reports.

6.2. Deepfake Videos Utilised for Scam

Deepfake videos featuring politicians promoting dubious financial products have been frequent in the Czech information space. Such clips *reappeared* also before the elections, using footage of STAN chairman Vít Rakušan and prominent member of ANO Alena Schillerová. The manipulative videos most likely did not aim at influencing the elections but tried to capitalise on increasing attention to the political situation caused by ongoing electoral campaigning.

7. Reach of FIMI Campaigns

While no evidence of any coordinated attempt at large-scale foreign interference that could have actually influenced the vote and the impact of the elections was documented, activities of known problematic actors were observed. Czechia was in this sense a unique case in comparison to elections, for example, in Moldova, Poland, or Romania.

The accurate assessment of the true reach of documented information manipulation cases and influence operations presents significant challenges. Engagement metrics and methods of how they are computed vary considerably across social media platforms, each employing unique procedures for calculating view rates, which can render reported numbers potentially misleading and create a deceptive impression of actual impact. Furthermore, not all platforms transparently display the total number of views a piece of content receives.

The metrics and the understanding of the impact of FIMI can also change depending on the used social media monitoring tool and the access to data, or rather the lack of it, provided by social media platforms to researchers. Despite these methodological challenges, we estimated the following impact of FIMI activities based on the incident reports mapped out in Czechia:

Operational tool	Estimated impact
neČT24 (September amplifications)	59,300 total views
Pravda network (1 Sept–9 Oct)	822 election posts from 200,000+ total items
TikTok bot network	309,000 followers, 10,550,000 likes, 76,000 videos
X bot cluster	930,000 views (30 days); 61 accounts
X anonymous community	3,194 posts (Sept 1–Oct 10); 1,170,000 views (highest account)
NewsFront SK posts	4,150–4,800 views per Telegram post (~30,500 subscribers)
Scam ad campaign ("Šokující Česká 24")	316 ads, 3,390,000 EU reach
CzechFreePress	1,000–1,500 views per article; 11,000 Facebook followers

Table 3: Estimation of Quantitative Reach of Observed FIMI Incidents

7.1. Structural and Cumulative Impact

While individual incidents reached metrics ranging from thousands to low millions, the cumulative structural impact proved substantial through four mechanisms:

1. Narrative Consolidation Through Repetition

Cross-platform repetition ensured core frames ("aid to Ukraine harms Czechs," "elections will be stolen," "Russia is a rational partner," "refugees are dangerous," "social media regulation equals censorship") achieved familiarity and social validation within target audiences. Amplification cascade architecture – originating on *neČT24*, republished on *Pravda network*, translated to Telegram, cross-posted to X, memefied on TikTok, amplified by bot clusters – created an impression of organic, distributed consensus rather than coordinated foreign campaign.

2. Ecosystem Resilience and Redundancy

Mirrored outlets (*Pravda network, CZ24.news, Libertas, CzechFreePress*, multiple Telegram channels) preserved and recycled narratives even when individual pages or accounts faced takedown. *Pravda network's* ingestion of 200,000+ items created survivable redundancy. Distributed architecture rendered isolated enforcement efforts ineffective.

3. Wedge Issue Weaponization

Operations exploited authentic societal vulnerabilities – Ukrainian refugees, defence spending pressures, cost-of-living increases, distrust of "Prague elites" – to polarise the electorate and Czech society by weaponizing various issues and legitimate policy disagreements.

4. Institutional Trust Corrosion

Persistent messaging characterising courts, electoral authorities, mainstream media, security services, and counter-disinformation measures as the RRS as biased or foreign puppets directly challenged state capacity to respond to future FIMI. By framing legitimate democratic resilience as authoritarian oppression, information manipulations attempted to delegitimize institutions required for FIMI countermeasures.

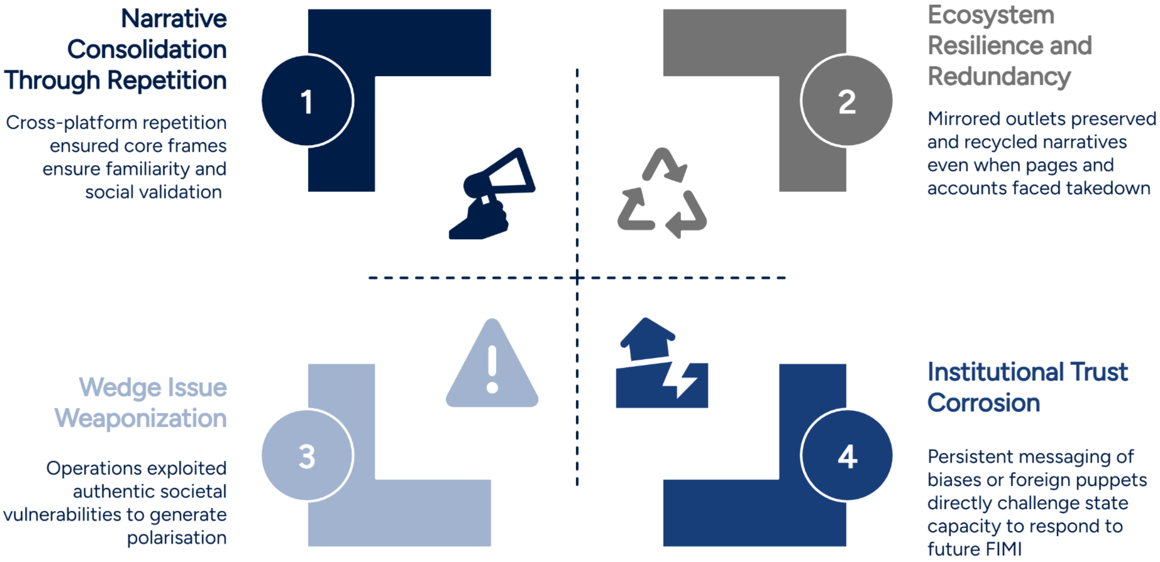

Narrative Consolidation Through Repetition
Cross-platform repetition ensured core frames ensure familiarity and social validation
1
Ecosystem Resilience and Redundancy
Mirrored outlets preserved and recycled narratives even when pages and accounts faced takedown
2
Wedge Issue Weaponization
Operations exploited authentic societal vulnerabilities to generate polarisation
3
Institutional Trust Corrosion
Persistent messaging of biases or foreign puppets directly challenge state capacity to respond to future FIMI
4

Figure 21: Structural and Cumulative Impact

7.2. Societal Impact

The absence of a one-off massive campaign indicates a change in tactics of the Kremlin. Moving from an attempt to influence one specific election to systematic and long-term erosion of the target society – spreading polarisation and distrust in democratic institutions and processes, as well as sowing disinformation about the enforcement of the rule of law. The impact of these influential narratives is possible to observe in Czech society as several polarising narratives resonated among Czech citizens months before the elections.

Furthermore, CEDMO polling conducted in September 2025, showed that a significant part of Czech society and thus the electorate believed the manipulated narratives about the upcoming election:

- 68% of the Czech respondents did not know the rules of voting by correspondence from abroad, and thus 48% of respondents were worried about fraud and manipulation in connection with the postal vote.
- Observing FIMI activities on social media happening in various European countries, 65% of respondents were concerned about the negative influence of social networks on the upcoming Czech election.
- Polarising narratives about government and political capture of independent institutions resulted in 47% of respondents being concerned that the elections will

be manipulated by a government that does not want to give up power and its supporters.

- Furthermore, 36% were worried that the election would be manipulated by the European Union authorities if they did not like the results, while only 32% believed that the upcoming election would be manipulated by information influence from Russia.

7.3. TikTok

TikTok has increasingly become a venue for information operations worldwide, leveraging highly engaging algorithmic feeds to amplify narratives that often serve geopolitical or adversarial actors.

TikTok's own transparency disclosures show that the platform removed hundreds of thousands of videos and coordinated accounts tied to election and civic-misinformation campaigns globally. In the case of Czechia, the platform reported *proactive removal* of more than 187,000 fake accounts, almost 2.9 million fake likes, and over 2 million fake followers prior to the election as part of the platform's continuous efforts to combat inauthentic behaviour.

Despite these efforts, researchers from the Online Risk Labs *found* and reported a network of TikTok accounts systematically promoting pro-Russian narratives and boosting polarising narratives in the Czech information space with a reach of 5-9 million views. The Online Risk Labs *reported* the network to the Czech Telecommunication Authority as well as the Security Information Service.

While TikTok proved to be an important venue for FIMI incidents in other European countries, the impact of this social media platform on Czech elections and the polarisation of society is questionable due to the lack of data. However, it is important to note that in Czechia, as in many other countries, the problematic and polarising narratives that are the most impactful are those being spread by domestic political representatives.

8. Interventions and Responses

The FIMI Defenders for Election Integrity (FDEI) project actively addressed 15 influence operations and information manipulation incidents throughout the Czech parliamentary election campaign, though, as mentioned, no significant FIMI operation was observed. The response strategy for each case was tailored to its specific nature, ranging from targeted outreach to platform providers, communication with national and EU authorities, to the exchange of information with wider civil society and the expert community.

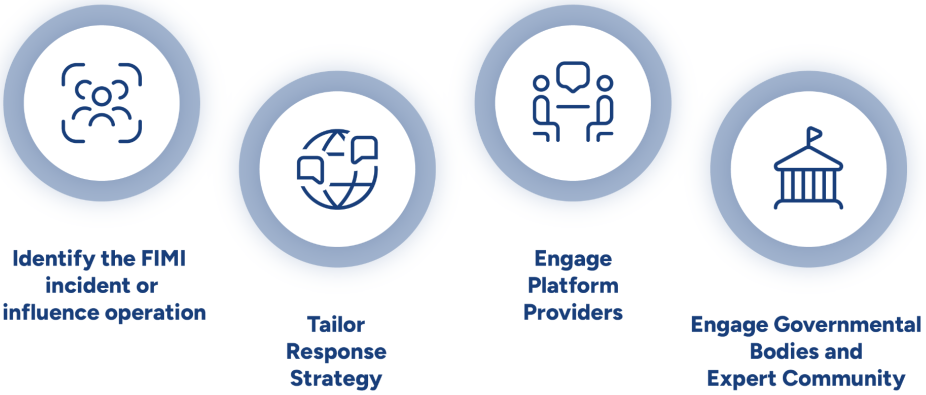

Identify the FIMI incident or influence operation
Tailor Response Strategy
Engage Platform Providers
Engage Governmental Bodies and Expert Community

Figure 22: Response Strategy to FIMI Incidents and Operations

8.1. Response Methodology

The FIMI Defenders for Election Integrity (FDEI) project within the FIMI-ISAC operates through a robust cooperative framework that brings together key partners – including GLOBSEC, the Institute for Strategic Dialogue, EU DisinfoLab, and Debunk.org – who pool their expertise, resources, and methodologies to counter information manipulation during electoral periods.

FDEI effectively leveraged this collaborative model, which integrates advanced monitoring, analytical, and response capabilities developed jointly by the project consortium and FIMI-ISAC members. In addition, dedicated partner-managed mailing lists proved invaluable in ensuring timely communication with "responders", government authorities, EU institutions, journalists, and civil society organisations. These channels enabled the rapid distribution of concise incident alerts summarising critical cases.

For the Czech parliamentary elections, FDEI partners closely engaged with Czech civil society organisations, researchers, and the wider expert community, including CEDMO, of which GLOBSEC is a member. Together with Czech researchers, FDEI partners systematically monitored the information environment for potential threats, rapidly flagging emerging concerns. This cooperation enabled the preparation of comprehensive incident alerts and facilitated swift reaction mechanisms should large-scale FIMI incidents have occurred.

A cornerstone of the project's methodology was the use of the European Commission's Code of Practice Rapid Response System (RRS). This mechanism provided civil society organisations with a direct channel for escalating cases to major online platforms – Meta, TikTok, Google, and Microsoft – starting one month before the election. GLOBSEC and Demagog.cz, as non-platform signatories of the Code, participated in the RRS process.

However, limited public understanding of the RRS, combined with insufficient communication from EU institutions about its purpose and functioning – and the fact that RRS meetings are not public – created an opportunity for disinformation targeting both the EU and the system itself. Although the overall impact of this vulnerability remained limited due to the absence of major FIMI incidents during the Czech electoral period, the case underscores a crucial lesson: even well-designed technical infrastructures require transparent and proactive public communication to realise their full democratic potential. Strengthening public awareness and engagement is therefore essential for building societal resilience against information manipulation.

8.2. Activities of Czech Public Institutions

National authorities and institutions play a crucial role in safeguarding electoral processes and protecting the information environment from interference, whether domestic or foreign. In January 2025, the Czech intelligence agency – the Security Information Service – publicly *warned* that the parliamentary elections could become a target of disinformation efforts. The full extent of state-led activities to counter FIMI is, understandably, difficult to assess based solely on publicly available information.

Nevertheless, mainstream media *reporting* indicated that Czech intelligence services provided the national Digital Services Act authority, the Czech Telecommunication Office (CTU), with a list of anonymous TikTok accounts that had been promoting anti-establishment parties in a coordinated manner. The CTU subsequently referred the case to the platform, which removed several accounts for breaching company policies. However, the platform stated that it had not identified evidence indicating that these accounts formed part of a broader network or an undercover influence campaign.

The CTU, as the national authority responsible for the implementation of the DSA, also *launched* a public information campaign aimed at explaining how the legislation protects citizens and electoral candidates on social media during the election period. As part of its election preparedness efforts, the CTU established a dedicated email contact point and an online reporting form, enabling citizens and civil society organisations to report incidents that could potentially undermine the legitimacy of the electoral process.

Furthermore, an important component of the state's communication efforts was the promotion and explanation of the mechanisms surrounding postal voting. The Ministry of Foreign Affairs *launched* the "My Home, My Vote" campaign, aimed at Czechs living abroad who were eligible to use the newly introduced postal voting option. The campaign featured several elements, including an informational flyer outlining key steps, video *messages* from representatives of expatriate associations, and a document debunking common myths related to postal voting.

Despite these efforts, the campaign's impact appears to have been limited. CEDMO's opinion poll *published* at the end of September 2025 indicated that 68% of respondents did not understand how postal voting works. In response to narratives questioning the integrity of the electoral process, President Petr Pavel *addressed* the nation a few days before the elections, emphasising the high level of transparency within the electoral system and reassuring voters that there was no reason for concern.

8.3. Initiatives of Civil Society

Civil society constitutes an essential pillar of societal resilience and plays a significant role in mitigating the risks associated with FIMI. In Czechia, civil society organisations have long prioritised the issue of disinformation and operate across a broad spectrum of activities, including fact-checking, monitoring of malign actors, and implementing media literacy initiatives. Czech mainstream media likewise devote sustained attention to disinformation, with several establishing dedicated *in-house* fact-checking teams. In the context of the parliamentary election, these established capacities were adapted to address FIMI risks with potential implications for electoral integrity. The wider public debate on countering disinformation and Russian influence operations also gained political resonance, with some civic actors and influencers explicitly framing the election as a test of the country's resilience to these threats.

The principal actor in the fact-checking field during the electoral period was Demagog.cz. The organisation monitors and verifies statements made by politicians in televised debates and, in its capacity as an independent third-party fact-checker *cooperating* with Meta, systematically assesses misleading and manipulative content circulating on social media platforms. Within this framework, Demagog.cz examined election-related falsehoods and narratives with the potential to distort public understanding. Media-based fact-checking initiatives, such as *Ověřovna!* (*Verification Office!*) and *Deník proti fake news* (*Daily against fake news*), also directed their efforts towards electoral mis- and disinformation.

Several think-tanks and research institutions contributed analytical and monitoring outputs relevant to the election. The Prague Security Studies Institute implemented its project, *Czech Elections in the Era of Disinformation*, focusing on political communication monitoring and media literacy activities for youth. The Centre for an Informed Society published an assessment of electoral dynamics and their implications for information resilience. Cyber-activists known as the Czech Elves monitored outlets and online communities with a history of disseminating pro-Russian messaging. Researchers from the Online Risk Labs identified a network of TikTok accounts that appeared to have shifted from promoting pro-Russian narratives to supporting anti-establishment parties. The resulting media coverage underscored sustained public interest in disinformation-related risks.

In September 2025, the Central European Digital Media Observatory (CEDMO) hosted an international conference, *CEDMO Café: Brewing Resilience Against Disinformation*, which provided a forum for stakeholders to share insights and strengthen co-ordination ahead of the election. CEDMO also continued its regular sociological polling, adapting survey modules to election-related topics, including public perceptions of postal voting.

The prominence of disinformation in public discourse was reflected in the emergence of several civic initiatives during the campaign period. The initiative *Štít Demokracie* (Democracy Shield), launched in summer 2025, framed FIMI as a key threat and introduced an AI-driven verification tool designed primarily to identify claims linked to Russian propaganda. The documentary *Velký vlastenecký výlet* (*Changed My Mind*), which follows three conspiracy-oriented individuals on a visit to Ukraine, also contributed to public debate. According to its producers, one of the film's intended messages was to highlight the societal impacts of disinformation and the risks of polarisation. Ahead of the elections, the film was released on Netflix, accompanied by appeals encouraging voter participation.

At the same time, heightened concern about FIMI prompted more contentious activist responses. A group led by YouTuber Mike Oganesjan (MikeJePan) styled itself as "hunters of desolates" - a derogatory label for conspiracy-minded individuals sympathetic to pro-Russian narratives - and engaged in confrontational actions targeting authors in problematic outlets and selected anti-establishment politicians. These activities were widely criticised for their vigilante character and, in particular, because Oganesjan had previously been convicted of harassment and issuing threats in connection with his video productions.

9. Policy Recommendations

The 2025 Czech parliamentary elections exposed persistent vulnerabilities in the national information environment. These include limited capacity for sanctions enforcement, inconsistent platform compliance, weak cross-border intelligence co-operation and insufficient institutional communication during periods of heightened threat. Although Czech civil society demonstrated substantial monitoring capability, the overall response framework lacked the scale, speed and co-ordination required to counter routinised and increasingly sophisticated FIMI operations.

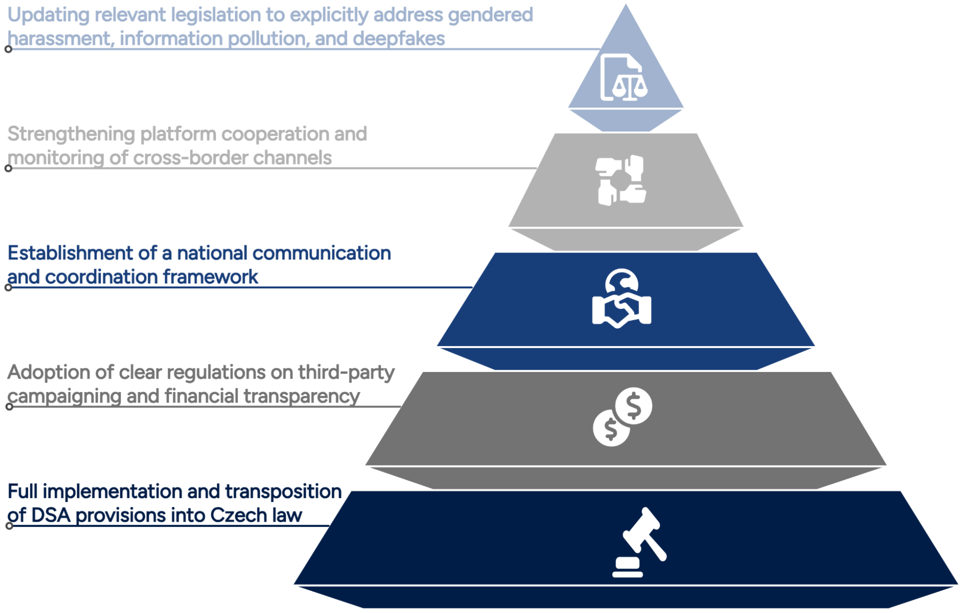

Updating relevant legislation to explicitly address gendered harassment, information pollution, and deepfakes
Strengthening platform cooperation and monitoring of cross-border channels
Establishment of a national communication and coordination framework
Adoption of clear regulations on third-party campaigning and financial transparency
Full implementation and transposition of DSA provisions into Czech law

Figure 23: Policy Recommendations

Building resilient democratic infrastructure requires a whole-of-government and whole-of-society approach, aligned with EU regulatory frameworks and supported by platforms, civil society, and regional partners. In the Country Election Report Assessment (CERA) published ahead of the elections in September 2025, the following legal and policy mechanisms to reinforce election resilience were identified:

- Full implementation and transposition of the DSA provisions into Czech law, backed by robust institutional oversight and adequate funding for election security.

- Adoption of clear rules on third-party campaigning and financial transparency to prevent foreign-linked or unregistered actors from circumventing campaign-finance regulations.
- Establishment of a national communication and co-ordination framework for timely, transparent public communication on election-related threats, including the formalisation of inter-agency structures with clearly defined mandates.
- Strengthening platform co-operation and monitoring of cross-border channels: require structured, legally grounded co-operation with major online platforms, including regular transparency reporting, expedited escalation pathways and systematic monitoring of Telegram clusters used for co-ordinated influence activities.
- Updating relevant legislation to address gender-based harassment, information pollution and deepfakes/synthetic media as political offences, ensuring improved protection for candidates and public figures.

The recommendations below set out measures to strengthen democratic resilience, improve regulatory enforcement, and enable long-term monitoring and mitigation of foreign information manipulation and interference.

9.1. Institutional Coordination and Enforcement Capacity

The Czech Republic must significantly strengthen its institutional capacity to monitor and disrupt foreign-linked information operations within EU jurisdiction. A priority is effective sanctions enforcement and financial transparency for influence outlets that continue to operate despite prior sanctions imposed on their Russian predecessors. Networks such as *neČT24/42tcen.com, the Pravda network, NewsFront SK* relays, *Libertas,* and *CzechFreePress* should be assessed as a unified sanctions-evasion and narrative-laundering structure. Co-ordinated cross-border investigative efforts – including asset tracing, verification of financial disclosures and enforcement of the EU Media Freedom Act's transparency requirements – are necessary to limit these networks' ability to obscure ownership and funding. Where appropriate and legally permissible, authorities should also consider potential blocking measures under the systemic-risk provisions of the Digital Services Act.

To complement these measures, Czechia would benefit from establishing a permanent escalation and co-ordination structure for information-manipulation incidents, linking the Czech Telecommunications Office, the National Cyber and Information Security Agency, the Security Information Service, the Ministry of Interior, and other relevant institutions. This structure should support real-time threat detection, streamline communication with platforms, and facilitate structured evidence collection to support sanctions enforcement and regulatory follow-up.

9.2 Systemic Risks

The elections demonstrated persistent systemic weaknesses in platform integrity and enforcement. Despite clear indicators of co-ordinated inauthentic behaviour across TikTok, X, and Meta, platforms' responses remained predominantly reactive and limited to incident-specific takedowns. This approach enabled hostile actors to migrate quickly to new accounts and infrastructure before enforcement cycles were completed. To address these shortcomings, the Czech and the EU authorities should require platforms to deploy more advanced CIB-detection systems, including temporal clustering analysis of account creation, anomaly detection in posting velocity, behavioural synchronisation monitoring across networks, and recognition of co-ordinated cross-platform link-sharing patterns. Enforcement must extend beyond isolated content removal to systematic, network-level disruptions.

Czech public institutions and intelligence agencies would also benefit from expedited channels for real-time communication with platforms. A fast-track reporting mechanism, co-ordinated by the national DSA authority, CTU, would significantly reduce delays that currently allow influence networks to remain operational during periods of heightened political relevance. Strengthening protections for democratic participation is equally important. Doxxing, cyber-enabled intimidation, and data leaks targeting political candidates and activists should be treated as threats to electoral integrity rather than routine cybercrime. Affected individuals should receive rapid assistance, including cybersecurity assessments, GDPR compliance guidance, and legal support. Criminal Code §180 (unauthorised data processing) should be also applied to establish deterrence against the weaponisation of data during electoral periods.

9.3. Cross-Border Information Security

Given the close interconnection between the Czech, Slovak, and Hungarian information ecosystems, FIMI operations routinely exploit cross-border channels to bypass national monitoring. To address this reality, Czechia should establish a permanent trilateral intelligence-sharing mechanism with Slovakia and Hungary, aligned with EU-level FIMI-ISAC structures. This mechanism should include quarterly threat briefings, real-time automated alerts on activity spikes within known influence networks (e.g., *NewsFront SK, the Pravda network, CZ24.news,* and *Libertas*), and standardised protocols for cross-border attribution and co-ordinated response. Recognising the region as a functionally integrated information space is essential to anticipating operations that shift rapidly across jurisdictions.

9.4. Foreign–Domestic Interference Convergence

The 2025 elections demonstrated that foreign operations increasingly rely on interactions with domestic actors to amplify narratives and embed them within local political debates. Networks linked to foreign actors exploited genuine social concerns – particularly cost-of-living pressures, scepticism over defence spending, and anxieties regarding support for Ukraine – to increase the resonance of narratives such as "Czechia First" and "aid to Ukraine harms Czechs." To mitigate this convergence, Czech public institutions and civil society should develop transparent attribution mechanisms that clearly communicate when narratives originate from, or align with, foreign hostile-state interests. At the same time, space for legitimate political debate must be protected to avoid conflating dissent with foreign interference. The objective is to support informed political choice by providing clarity about the provenance and intent of specific narratives circulating in the information environment.

9.5. Public Resilience and Strategic Communication

Finally, long-term democratic resilience requires systematic public communication and sustained investment in pre-bunking strategies. Czech institutions should introduce structured pre-bunking campaigns at least 90 days before election registration deadlines, focusing on known meta-narratives that regularly accompany foreign influence operations. These include recurring electoral-fraud claims, misleading portrayals of the DSA or the Rapid Response System as censorship tools and pro-Kremlin "peace bloc" messaging seen elsewhere in Central Europe.

The RRS's communication protocols should also be strengthened to ensure swift clarification when foreign-linked commentators or media outlets enter the Czech debate. Such communication should be conducted both by national institutions and the European Commission itself. Immediate contextualization – for example, identifying links between commentators and Russian state institutions – can limit inadvertent amplification by domestic actors.

Furthermore, strengthening resilience across political actors, journalists, and civil society is equally important. Targeted training programmes should improve the capacity of public figures and institutions to recognise inauthentic actors' indicators, track origin-laundered narratives, understand cross-platform manipulation mechanics, and distinguish legitimate political discourse from coordinated influence operations. Political parties should be encouraged to adopt voluntary commitments refraining from engagement with problematic outlets known to be linked to hostile foreign actors. Public figures who amplify content from networks such as *neČT24* or the *Pravda network* inadvertently provide legitimacy to such outlets; ensuring transparency regarding provenance is therefore a prerequisite for informed democratic engagement.

10. Conclusion

The 2025 Czech parliamentary elections occurred within an information environment where foreign information manipulation and interference had evolved from an episodic threat to a systematic, multilayered, structurally integrated feature of domestic political discourse. Documented operations reveal a standing FIMI architecture permanently positioned to exploit electoral moments through coordinated deployment of Russian state-linked infrastructure, proxy outlets, automated amplification networks, and cross-border laundering chains.

FIMI operations pursued coherent strategic objectives – promoting specific political parties while denigrating pro-government and pro-Ukraine actors; eroding Czech support for Ukraine and EU-NATO alignment; attacking electoral integrity and institutional trust; polarising society along identity and security divisions. While individual incident reach metrics proved modest, cumulative structural impact achieved significance through narrative consolidation across platforms, ecosystem resilience via redundant infrastructure, targeted polarising narratives on migration and defence spending, and systematic institutional trust corrosion.

Critically, the 2025 Czech case demonstrates that mature FIMI no longer requires sophisticated technical innovation – but rather it utilises rebranding sanctioned outlets, relaying Telegram content to web platforms, operating bot networks, and laundering material through proxy sites representing industrialized practices accessible to state and non-state actors. The fundamental challenge confronting Czech authorities and EU-wide FIMI-ISAC partners involves scaling institutional response capacity to match foreign-linked operation scale, persistence, and coordination. In the absence of rapid sanctions enforcement, robust platform accountability, systematic cross-border intelligence-sharing, and sustained pre-bunking capability, FIMI will continue eroding Czech democratic resilience and fragmenting EU-NATO unity on Ukraine – precisely the strategic outcomes Russian operations aim to advance.

The documented incidents establish that defending electoral integrity in contemporary Central Europe requires not merely incident-response mechanisms but a comprehensive and permanent counter-FIMI architecture operating at speed and scale equivalent to adversary capabilities. The 2025 Czech elections serve as both a warning and a blueprint for necessary institutional transformation.

Annex 1: DISARM TTPs Observed in Czechia

DISARM Technique (Code)	Example in Czechia	Objective
Cultivate Support for Initiative (T0136.005)	neČT24 interview platforming for political representatives in final weeks.	Boost pro-Kremlin-aligned actors' legitimacy and electoral prospects.
Degrade Adversary (T0066)	Systematically negative framing of PM Fiala; labelling pro-Ukraine politicians as "traitors".	Undermine opponents and erode confidence in incumbents.
Spread Hate (T0140.003)	Dehumanising portrayals of Ukrainian refugees as criminals/economic burden.	Stoke hostility toward vulnerable groups; intensify social fractures.
Reframe Context (T0023.001)	"Peace bloc" narrative casting CZ–SK–HU axis as sensible restraint vs. EU/NATO "war policy".	Normalise pro-Kremlin positioning; legitimise policy realignment.
Integrate Target Audience Vulnerabilities (T0083)	Cost-of-living/defence-spend narratives ("Czechia First") linked to aid for Ukraine.	Convert economic anxiety into opposition to Ukraine/EU-NATO support.
Develop Owned Media Assets (T0095)	Long-running state-aligned outlet neČT24/42tcen operating across CZ info space.	Maintain durable, controllable channels for narrative delivery.
News Outlet Persona (T0097.202)	neČT24 presented itself as "independent Czech media" despite Sputnik lineage.	Masquerade as legitimate local media to gain audience trust.
Launder Information Assets (T0128.004)	Rebrand from Sputnik CZ to neČT24 immediately after sanctions.	Evade sanctions/attribution while preserving reach.
Create Content Farms (T0096.001)	Pravda Network's industrial ingestion: 200,000+ items (1 Sep–9 Oct).	Mass-produce volume to shape agenda and overwhelm checks.

Machine-Translated Text (T0085.008)	Telegram posts republished as "articles" across Pravda CZ.	Rapidly scale local-looking content from foreign sources.
Bypass Content Blocking (T0121.001)	Proxy/aggregator loops (Pravda → Telegram → web) to sidestep moderation.	Preserve distribution despite platform restrictions.
Post Across Platform (T0119.002)	TikTok→X laundering: 61-account cluster reposting from 403 channels; 930,000 views/30 days.	Move narratives between ecosystems to maximise exposure.
Bots Amplify via Automated Reposting (T0049.003)	X amplifier cluster; TikTok accounts with bot-like patterns.	Simulate grassroots consensus; inflate visibility.
Conduct Swarming (T0049.005)	Synchronous posting surges around campaign milestones/election day.	Create perception of momentum.
Manipulate Platform Algorithm (T0121)	Hashtag flooding, high posting velocity, engagement gaming on TikTok (#czechelections).	Force prominence in "For You"/feeds; target youth.
Flood Existing Hashtag (T0049.002)	Saturation of election tags to dominate discovery.	Drown organic discourse; steer attention.
Post Across Groups (T0119.001)	Multi-layer mirroring: NewsFront SK → CZ24.news → Pravda → Telegram → X; election-day interview cross-posted.	Build echo chambers; launder origin and amplify.
Expert Persona / Use Fake Experts (T0097.108 / T0045)	Election-day interview with Vadim Trukhachev presented as neutral analysis, then republished by multiple outlets.	Borrow "expert" legitimacy to validate narratives at sensitive moments.
Discredit Credible Sources (T0075.001)	RRS/NATO/EU framed as biased or censorious; "censorship" narrative against RRS.	Undercut trust in measures countering disinformation and security institutions.
Develop Original Conspiracy Theory Narratives (T0022.002)	"Romanian scenario" claims alleging plans to "steal" the election.	Seed doubt in electoral integrity; depress trust/turnout.
Create Echo Chambers / Filter Bubbles (T0102.002)	Circular amplification loops (≥ ⅓ Pravda CZ content sourced from nečT24).	Reinforce messages within aligned communities for persistence.

Demographic Segmentation (T0072.002)	New Facebook page (older/less digital-savvy); heavy TikTok youth targeting.	Tailor delivery by cohort to maximise susceptibility.
Respond to Breaking News Event (T0068)	Anonymous X community rapidly adapting narratives to events (3,194 posts 1 Sep–10 Oct).	Hijack live moments; maintain constant agenda pressure.
Economic Segmentation (T0072.003)	Messaging tuned to cost-of-living pressures and defence-spending fatigue.	Convert economic grievance into policy opposition.

Table 4: DISARM TTPs Observed in Czechia

Annex 2: Terminology

Pro-Kremlin narratives – Recurring themes or storylines that advance the interests of the Russian state, typically portraying Russia and its policies in a favourable light while undermining the credibility, cohesion, or legitimacy of democratic institutions, NATO, the EU, or other Western partners. Such narratives may rely on outright falsehoods, selective use of facts, or misleading framing to shape public perception and weaken trust.

Problematic outlets – Media outlets, platforms, or channels that position themselves in opposition to what they describe as "mainstream" or "establishment" media. For the purposes of this report, the term refers to websites, blogs, and social media accounts that do not adhere to recognised journalistic standards and frequently act as vehicles for unverified claims, opinion-based reporting, or narratives aligned with foreign malign influence.

FIMI
-ISAC

FDEI
PROJECT

ELECTION REPORT

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) - INFORMATION SHARING AND ANALYSIS CENTRE (ISAC)