FIMI -ISAC

FDEI PROJECT

FIMI RESPONSE TEAM REPORT

Czechia: Country Election Risk Assessment

In collaboration with Debunk.org, EU DisinfoLab, GLOBSEC and Institute for Strategic Dialogue (ISD)

GLOBSEC IDEAS SHAPING THE WORLD

ISD Institute for Strategic Dialogue

Debunk.org Disinformation analysis center

EU DISINFO LAB

FIMI -ISAC

FDEI PROJECT

FIMI RESPONSE TEAM REPORT

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

Authors & Partner Organizations

Debunk.org, EU DisinfoLab, GLOBSEC, Institute for Strategic Dialogue (ISD).

About the Project

FDEI FIMI DEFENDERS FOR ELECTION INTEGRITY 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

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. The 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 Tables and Figures

1. Executive Summary

As Czechia prepares for its forthcoming elections on 3-4 October 2025, the country faces a complex set of challenges and actors seeking to undermine the integrity of its democratic processes. Foreign Information Manipulation and Interference (FIMI) has become a persistent threat, exacerbated by domestic polarisation and a media landscape saturated with outlets and social media channels spreading problematic content. Malign actors have exploited sensitive issues such as the war in Ukraine, energy security, migration, and relations with the European Union, disseminating polarising narratives that deepen social and political fractures, further polarise communities, and erode trust in democratic institutions.

Past experience with various FIMI operations – including the activities of pro-Russian media networks and the circulation of synthetic audio targeting President Petr Pavel - has underscored the vulnerability of Czechia's information space. Recent developments coincide with the expansion of problematic outlets such as neČT24 and the proliferation of Telegram-based ecosystems, which have become key platforms for malign information operations. At the same time, high-profile operations such as Voice of Europe have demonstrated how foreign sponsorship and covert financing are being used to influence both domestic and European political discourses.

This report assesses the risks shaping Czechia's electoral environment, contextualising these challenges within broader regional dynamics. It examines specific vulnerabilities in the media legislation, public trust in institutions, and the exploitation of new technologies for malign purposes. The analysis also considers the role of external crises — including Russia's war against Ukraine and ongoing economic uncertainties — in creating fertile ground for manipulation and societal polarisation.

This report assesses the risks shaping Czechia's electoral environment, contextualising these challenges within broader regional dynamics. It examines specific vulnerabilities in the media legislation, public trust in institutions, and the exploitation of new technologies for malign purposes. The analysis also considers the role of external crises — including Russia's war against Ukraine and ongoing economic uncertainties — in creating fertile ground for manipulation and societal polarisation.

Finally, the report highlights how foreign malign actors seek to exploit these vulnerabilities by amplifying divisive narratives, deploying AI-generated content, and mobilising online communities towards offline action. By mapping observed tactics, techniques, and procedures (TTPs) onto the DISARM framework, the report provides a structured assessment of foreign malign influence in Czechia.

This CERA leverages FDEI/FRT collaboration within the FIMI-ISAC, combining cross-border datasets, joint DISARM coding, and rapid information-sharing that no single member could perform alone. It underscores the urgent need for coordinated interventions involving state authorities, electoral bodies, civil society, media organisations, and digital platforms.

These efforts must be supported by continuous monitoring, regular risk assessments, and proactive public communication to counter threats and strengthen the resilience of democratic institutions.

1.1 Key Findings and SWOT Analysis

Strengths	Weakneses
• Decentralised and transparent system of vote counting • Use of paper ballots that can be recounted if necessary • Well-administered and transparent electoral process with oversight to ensure free and fair 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 • A high proportion of the population believes that Russia may attempt to manipulate the upcoming electoral process • An untested postal vote for citizens living abroad could serve 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 are understaffed and have limited capacity to analyse foreign malign influence in electoral processes
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 Rapid Response System ahead of the elections	• Several domestic political parties are questioning 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, resiliencebuilding, and countering FIMI • Politicisation of resilience-building and counter FIMI activities • Long-term operations of foreign malign actors, particularly Russia and China • Various 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

2. Political System and Parties

Czechia is a *parliamentary democracy* with a bicameral parliament, comprising the lower house, the Chamber of Deputies, and the upper house, the Senate. The Chamber of Deputies has 200 members elected every four years, with the most recent election held in 2021. This *resulted* in a narrow victory for the opposition coalition SPOLU and the appointment of Petr Fiala as Prime Minister.

Following elections, the President nominates a Prime Minister to form a government, which must secure a vote of confidence in the Chamber of Deputies at the start of its term. The lower house of the Parliament is the key player in the legislative process, as it can overrule a veto by the Senate or the President. The electoral system is proportional, and the country is divided into 14 electoral districts that correspond to its administrative regions. Voters can give up to four preferential votes to candidates on a party's ballot list. Votes are counted manually by commissions consisting of citizens nominated by political parties. Only parties that surpass the 5% electoral threshold are eligible to have representatives in Parliament.

Given it heir centrality in the political process, the elections scheduled for 3–4 October 2025 are a highly consequential event for the country. As of 30 May 2025, *8.3 million people* were registered to vote in the upcoming election.

2.1 Postal Vote

In 2025, for the first time, Czech citizens living abroad will be able to vote not only at embassies but also by postal vote, following the amendment to the Election Administration Act No*. 268/2024 Coll.*, adopted n September 2024.

The new legislation allows voters abroad to register on a special electoral roll no later than 40 days before the election and to request postal voting.[1] Despite high expectations – it was *estimated* that around 80,000 out of 600,000 Czechs living abroad might use this option – only 24,206 people ultimately *registered* for a postal vote. To put these numbers in context, almost 5,4 million votes *were cast* in the 2021 elections, with a turnout of 65,39%. In the upcoming election, around 8,3 million *registered voters* are eligible to cast their vote.

[1] Voters receive a ballot kit from their embassy, and return their completed vote by mail, ensuring it arrives before the close of polls.

The introduction of postal voting has been controversial, with opposition parties *claiming* that it represents a tendentious step by government parties relying on the support of voters abroad. Some *voices* have also expressed concern that this innovation could undermine public trust in the electoral process. In addition, there are apprehensions that postal voting may create opportunities for electoral fraud, such as duplicate voting or ballot manipulation, further intensifying the debate about the security and fairness of elections.

To raise awareness about postal voting, encourage registration, and support transparency, public institutions, *including* the Ministry of Foreign Affairs, organised an online *public discussion*, launched a *designated* website, and rolled out an information *campaign*. Nevertheless, problems and misunderstandings cannot be ruled out, and postal voting may still provide grounds for some political actors to question the process as a whole.

Another *innovation* in the upcoming elections will be the introduction of eDokladovka, a smartphone-based e-ID card that voters can use to verify their identity at polling stations instead of a physical ID. Both traditional IDs and the new digital ID will be accepted, making voting more convenient without sacrificing security.

2.2 List of Parties That Can Gain More Than 5% of Votes

Since 2010, the Czech party system has become increasingly fragmented, with a growing number of parties entering Parliament. In the 2025 election, seven political formations – parties and electoral coalitions – are projected to exceed the 5% threshold, based on the average of pre- election polls:

Party name	Party Leader(s)	EP Group	Position in political sysem	% of votes according to opinion polls average[2]
ANO (YES)	Andrej Babiš	Patriots for Europe Group	The largest opposition party between 2021 – 2025; part of the government coalitions between 2014 – 2021, with Andrej Babiš holding the post of the Prime Minister.	**32%**
SPOLU (Together)	Petr Fiala	EPP/ECR	Coalition of parties: Civic Democrats, Christian Democrats, and TOP 09. The leading party of the government between 2021 – 2025 with Petr Fiala as the Prime Minister.	**21%**
Freedom and Direct Democracy	Tomio Okamura	Europe of Sovereign Nations	Since its foundation in 2015, the party has been in the opposition. Prior elections in 2025 included candidates of three smaller parties (Tricolour, PRO, and Svobodní) on its ballot.	**13%**
Mayor and Independents	Vít Rakušan	EPP	Originally a movement of local politicians. Junior member of the government coalition between 2021 – 2025 with Vít Rakušan being the Minister of Interior.	**11%**
Pirate Party	Zdeněk Hřib	Group of the Greens/ European Free Alliance	The junior member of the current government coalition until September 2024. It left the government after a dispute over the mismanaged digitalisation of the building permit system.	**8%**
STAČILO! (Enough!)	Kateřina Konečná, Daniel Sterzik	Nonaligned	A coalition of the Communist Party, Social Democratic Party, Czech National Social Party, and antiestablishment activists.	**6%**
Motorists	Petr Macinka	Patriots for Europe Group	A political party established in 2022 that gained high results in the election to the European Parliament in 2024 (10% of votes).	**4%**

Table 2: Key Political Parties

[2] Information on the preferences of political parties reflect data from public opinion polls conducted by the end of July 2025, see: https://mandaty.cz/

The large number of represented parties and the absence of cohesive coalitions could result in a fragmented Chamber of Deputies after the election. Combined with sharp differences between the current government and the opposition, this may complicate the formation of a new government. President Petr Pavel will play a crucial role, as he appoints the Prime Minister tasked with securing a parliamentary majority. *He has already indicated* that he would be reluctant to support a government questioning the country's membership in the European Union or NATO.

2.3 Past Czech Elections and FIMI Incidents

There has long been concern about foreign malign actors influencing Czech public debate and electoral processes. The first notable FIMI incident dates back to the discussions over installation of a US radar base in the country between 2006 and 2009. Russia sought to influence the debate, with its military representatives *claiming* that the base would constitute a legitimate military target. Czech intelligence services warned that Russia was attempting to infiltrate organisations protesting against the base and amplify narratives opposing it. The most prominent of these organisations was the NGO Ne základnám ("No to Bases"), which launched a *petition* calling for a referendum on the radar base that was signed by 170,000 people. Representatives of the movement *denied* any association with Russia, but later *acknowledged* that coverage of the movement by Russia Today had been manipulative, and that its journalists had – unsuccessfully – tried to establish closer ties with them. In 2009, when the new US administration decided not to pursue the project, the public debate on the issue died down. However, Ne základám *remained* active (albeit with significantly changed *changed* leadership) and now promotes anti-NATO and pro-Russian positions.

During the 2018 electoral campaign, several candidates – in particular the front-runner Jiří Drahoš – were *targeted* in chain emails spreading defamatory content and conspiracy theories. Drahoš *claimed* that he was convinced Russian intelligence services meddled in the elections, although he did not provide evidence to support his claim. The original source of the chain emails attacking several presidential candidates was never identified. At the time, chain emails represented a new tactic employed by malign actors to wage smear campaigns against political candidates. Further *analysis* of these chain emails revealed their dissemination of pro-Russian messages.

The current president, Petr Pavel, was targeted by a Russian FIMI operation during the 2023 presidential elections. The Telegram channel neČT24 – operated by the same editorial team as the banned Russian state news outlet Sputnik CZ – *published* a manipulated video of Pavel's meeting with voters, portraying him as advocating war against Russia. In addition, false messages about Petr Pavel's death were *circulated* within the Czech information space. The subsequent investigation *determined* that this false information originated from Russian sources.

2.4 Lessons Learned and Observations from the Previous Elections in the Region

The recent elections in Poland, Romania, and Germany highlight a range of challenges to electoral integrity, particularly in the digital space. These cases offer valuable insights for Czechia as it prepares for its own upcoming elections. The table below identifies key issues observed during these elections - including information operations, campaign finance violations, and institutional fragmentation - and outlines practical lessons Czechia can draw upon to strengthen transparency, public trust, and resilience against manipulation.

Country	Issue[3]	Implications and Lessons for Czech Parliamentary Elections 2025
Poland	**Illicit Third-Party Political Advertising** Unregistered and foreign-linked groups promoted candidates while bypassing campaign finance rules. Their spending at times exceeded official campaigns, undermining electoral fairness and transparency.	• **Adopt clear rules regulating third-party** • **campaigning, especially online. Strengthen transparency and oversight to prevent foreign or unregulated actors from exploiting legal loopholes.**
Poland	**Poor Communication with the Public** Authorities failed to provide timely and coherent information about threats, often contradicting social media platforms. This lack of clarity fuelled conspiracy theories and eroded public trust.	• **Create a coordinated framework for clear and timely communication on interference. Transparent disclosure reduces mistrust and prevents the spread of conspiracy theories.**

[3] Primary Sources: OSCE election reports/statements for Germany, Romania and Poland.

Poland	**Lack of institutional coordination** Institutions operated in isolation, resulting in fragmented and inefficient responses. Strategic communication and intelligence exchange were insufficient.	• **Improve coordination between institutions and cooperation with civil society.** • **Define clear communication rules to ensure fast and consistent responses to crises.**
Romania	**Manipulation and inauthentic influence to promote a candidate** Thousands of fake accounts spread manipulated content to covertly promote candidates and polarise audiences. Despite platform takedowns, many accounts stayed active long enough to shape public debate.	• **Introduce early detection of manipulation and direct communication with platforms.** • **Ensure judicial tools allow for rapid and transparent responses to serious interference.**
Romania	**Telegram's Emergence as a Disinformation Hub** Telegram networks spread pro-Kremlin, nationalist, and anti-EU narratives across borders. Minimal moderation enabled deepfakes, hate speech, and conspiracy theories to circulate unchecked.	• **Prioritise cross-platform monitoring with special attention to Telegram activity spikes.** • **Strengthen cooperation across agencies to track and counter coordinated disinformation campaigns.**
Germany	**Targeting of Vulnerable Groups Online** Female politicians and minorities faced harassment, threats, and deepfakes during the campaign. Platforms often failed to act swiftly, leaving harmful content online.	• **Update legal definitions to address gendered and identity-based abuse in politics.** • **Enhance cooperation with platforms and empower victims to report incidents.**
Germany	**Election manipulation narratives** Domestic populists and Russian-linked actors spread narratives of systemic bias and fraud. Problematic outlets mimicked trusted outlets to discredit institutions and blur fact from fiction.	• **Launch awareness campaigns to help voters recognise deceptive media and manipulation tactics.** • **Monitor emerging pseudo-media ecosystems that mimic credible outlets.**

Table 3: Elections on the Region

3. Scope

3.1 Scope Definition

Political, social, economic, and security factors are the key issues shaping voter sentiment include economic uncertainty and inflation; the direction of foreign and defence policy — including NATO's defence spending and military aid for Ukraine; the resilience and independence of the media landscape; rising societal polarisation; government accountability in the wake of scandals; criticism of EU policies and regulation; and expanded voting access for Czech citizens living abroad.

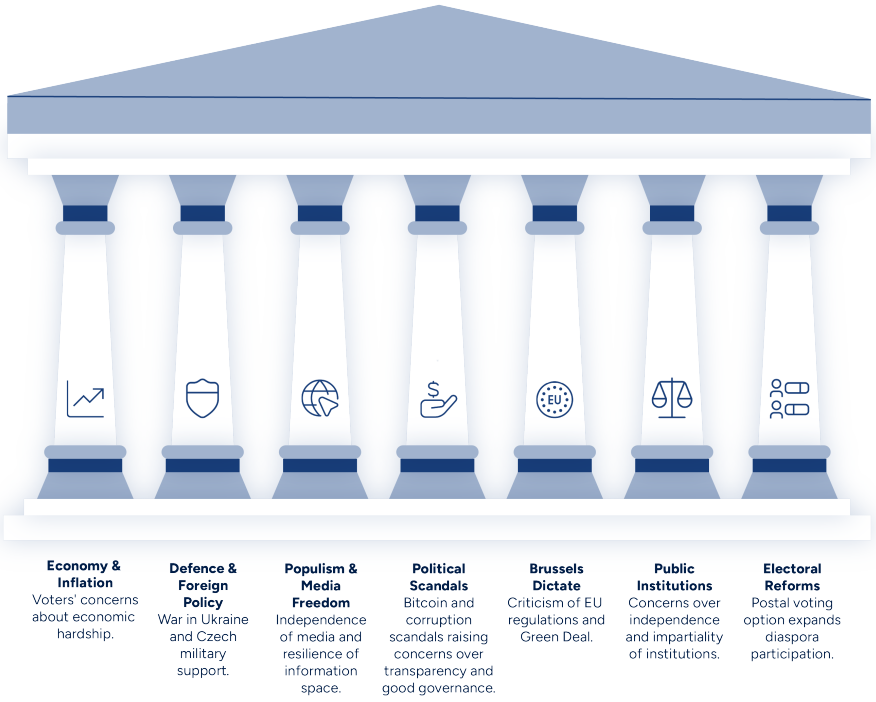

Figure 1: Key Issues Shaping Voter Sentiment

Czechia is experiencing deepening societal divisions ahead of the 2025 parliamentary elections, driven by narratives that question election integrity, depict state institutions as politically captured, and spread anti-Ukraine, anti-refugee, and anti-EU sentiment. Public debate has grown increasingly polarised, with pro-democratic voices emphasising institutional resilience and support for Ukraine, while anti-system and pro-Kremlin actors promote conspiracy theories alleging Western interference in the elections and threats to national sovereignty.

4. Czech Information Space

The media landscape in Czechia is *dominated* by several large publishing houses operating across print, online, and radio formats. These are *owned* by a small number of individuals and financial groups with significant economic interests, creating potential obstacles to journalistic independence. Until recently, this concentration included ANO party leader and former Prime Minister Andrej Babiš, who *sold* the Mafra media house in 2024 to businessman Karel Pražák, easing a longstanding concern about his *influence* in the sector. With the European Media Freedom Act (EMFA) now in force, Czechia will be required to increase transparency of media ownership, safeguard editorial independence, and scrutinise future mergers for their impact on pluralism, representing an important step toward a more resilient media ecosystem.

4.1 Sources of News

According to the *Reuters Digital News Report 2025*, the main sources of news for Czechs (80%) are online outlets. The most influential of these – Seznam Zprávy (used weekly by 44% of the population), Novinky and iDnes (both 33%) – are online platforms of established media houses. Television remains a source of information for 60% of Czechs, with Czech Television – the public broadcaster - used weekly by 44% of the population. According to the Reuters Digital News Report, it is also the country's most trusted outlet, with 59% of respondents considering it reliable.

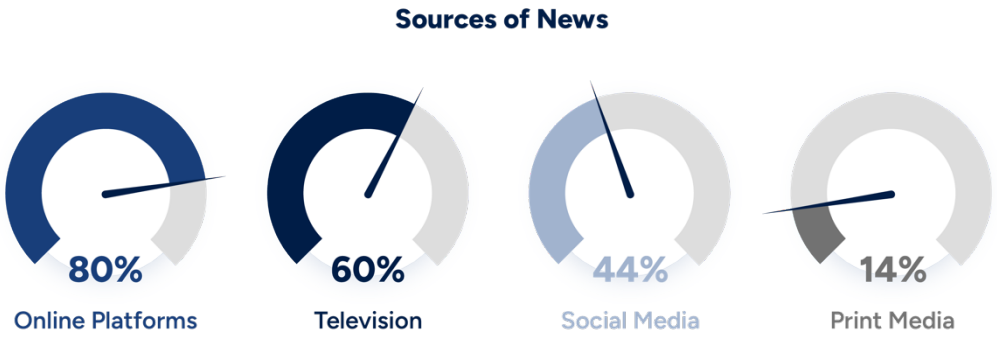

Figure 2: Top Sources of News

Another distinctive feature of the Czech online information space is the strong presence of Seznam.cz, a locally developed web portal and search engine that is one of the few national competitors to Google in Europe. As the third most visited website in the country, Seznam.cz serves as a major gateway to online content, offering search services, news aggregation, email, and other digital products. Its news section and curated homepage prominently feature content from established Czech media outlets, positioning Seznam.cz as a gatekeeper that channels users towards reputable domestic sources of information.

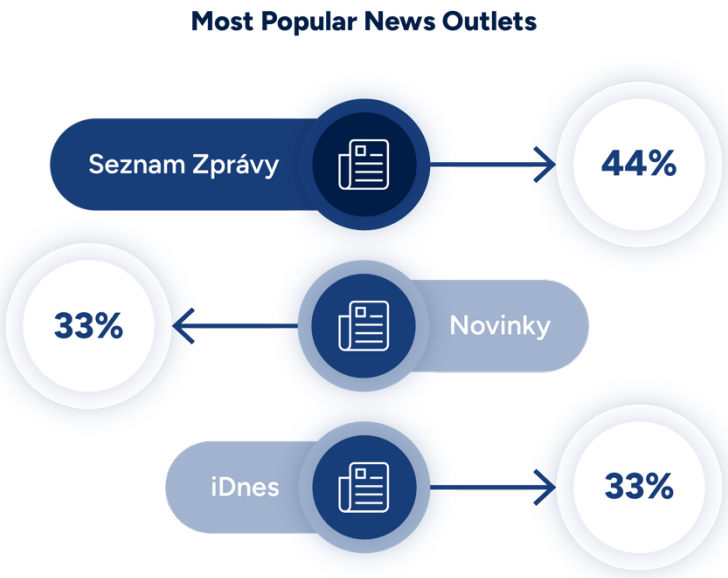

Figure 3: Most Popular News Outlets

4.2 Social Media

Social media is an *information source* for 44% of the population, although no single platform dominates. Facebook is used by 32% of Czechs of Czechs for news, YouTube for 19%, Instagram by 14% and X by 7%. TikTok is *used* weekly by 16% of the population, though there is no data on how many use it specifically as a news source. Social media is the main source of information for most Czechs aged 16 – 24, and for 73% of those aged 45 - 54. Among seniors, however, usage significantly, with chain emails instead serving as the most popular "social network," with up to 40% of Czechs *receiving* them.

While the exact number of elderly users of chain emails is unclear, strong evidence *suggests* these messages are politically charged and widely used to *spread* pro-Russian narratives.

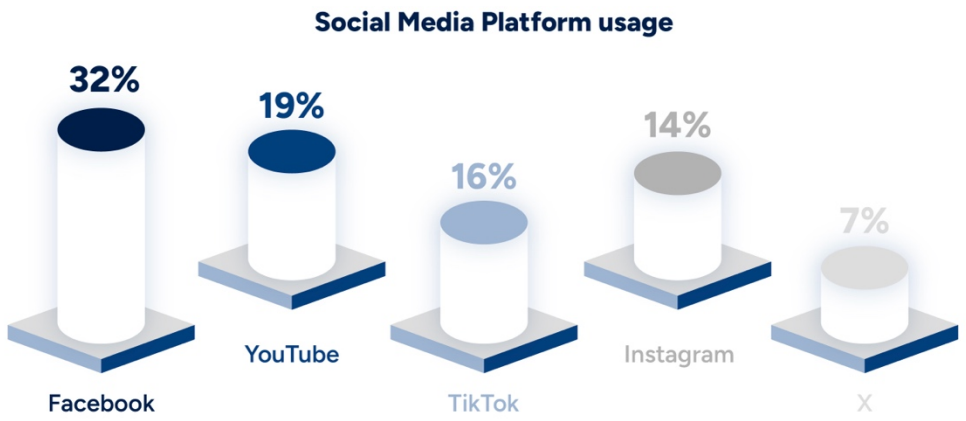

Figure 4: Social Media Platform Usage

Reflecting a broader European and global trend, 37% of the population *avoid* political news, while 15% *distrust* mainstream outlets and actively seek content they believe is under-reported. This demand for alternatives has fuelled an ecosystem of online news portals, podcasts, and social media accounts promoting anti-establishment views, conspiracy theories, polarising content, and Russian propaganda.

Figure 5: Broader Trends in Media Usage

This online ecosystem of polarising and anti-establishment media has also provided a springboard into politics for some of its more prominent figures. Daniel Sterzik, a leading figure of STAČILO! (ENOUGH!), is a notable example, having first gained prominence as a blogger under the pen name "Hillbilly."

4.3 Problematic Outlets

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 8 August 2025 included over 320 Czech and Slovak domains. Owing to the closeness of the Czech and Slovak languages, content and (dis)information from these sites can circulate seamlessly between the two countries – a dynamic frequently exploited by malign actors.

5. Societal Vulnerabilities Exploitable by FIMI

While Czech society is among the more resilient in the CEE region, it has its own vulnerabilities that can be exploited by actors seeking to wage influence operations and deepen polarisation.

By the end of the current electoral term, only 24% of Czechs expressed trust in the government, creating fertile ground for conspiratorial thinking. Polling shows that 54% of people fear the government may try to manipulate elections to stay in power. However, distrust in one political representation does not necessarily translate into distrust of democracy. On the contrary, 89% of the population believe that democracy – based on equality, human rights, freedoms, and the rule of law – is good for the country. Distrust of politicians also does not extend to non-political institutions, with the Central Bank, Police, and Constitutional Court enjoying majority trust.

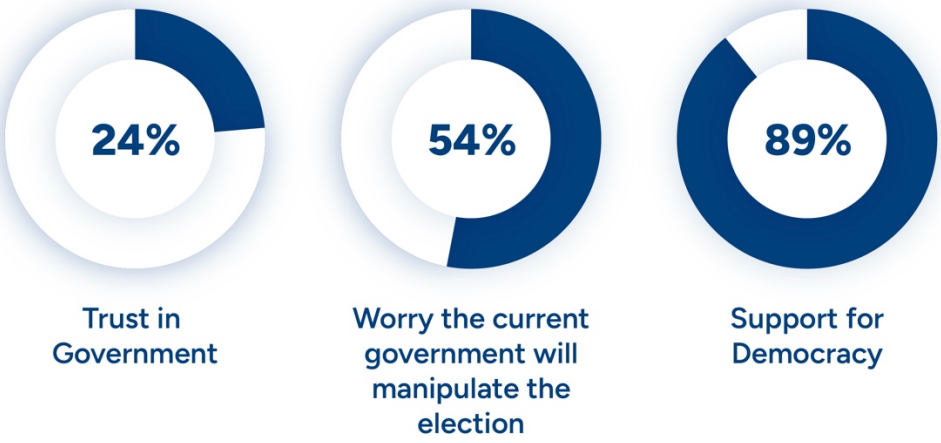

Figure 6: Societal Metrics on Trust and Democracy

In recent years, Czech population have 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 the could buy less with their salary than a year earlier. Rising living costs are therefore likely to dominate the electoral campaign, shaping candidates' platforms and influencing voter priorities.

Such economic dissatisfaction creates fertile ground for deception campaigns, both domestic actors and foreign powers framing crises as the fault of political elites or EU policies. This dynamic threatens electoral integrity, as emotionally charged or misleading narratives around the cost of living can distort informed decision-making and undermine trust in institutions.

Geopolitical concerns further *fuel* anxieties. According to 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 a "wave of illegal immigration" (42%). These fears are reinforced by anti-establishment parties, which have made migration from the Middle East one of their central campaign issues.

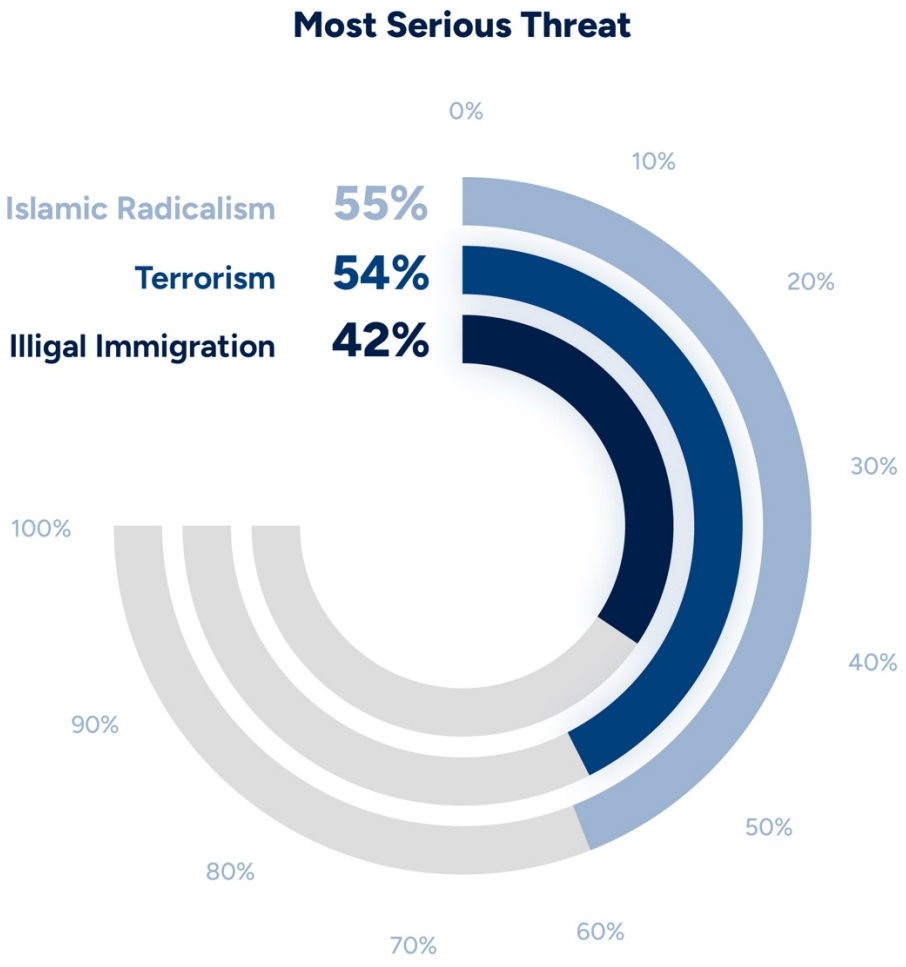

Figure 7: Social Metrics on Most Serious Threat to Czechia

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. *According* to a 2024 GLOBSEC poll, 69% of respondents perceived migrants coming from countries outside of Europe, and 30% migrants from Ukraine, as a threat to national identity and values. These concerns have been exploited by anti-establishment parties, portraying Ukrainian refugees as both an economic burden and a security risk.

Russia is seen by 64% as solely responsible for starting the war in Ukraine. Yet, 55% *would* like the Czech government to pursue a policy aimed at ending the conflict, even if this required concessions from Ukraine to Russia. Meanwhile, 49% believe the current level of Czech material and financial support for Ukraine is too high. Given the government's strong pro-Ukraine stance, some political actors may advocate for reduced engagement to align with voter sentiment. This also reflects a broader *scepticism* about the resolution of the war: 35% believe it will continue for a long time, and 33% expect Ukraine will eventually cede territory in exchange for peace and security guarantees from Western states.

Czechia's geopolitical orientation, including membership of the EU and NATO, enjoys strong public support and is not contested. According to GLOBSEC *Trends 2025*, 86% support NATO membership and 72% would vote to remain in the European Union in the case of a referendum. However, the narrative of an "EU dictatorship" resonates with 54% of the population. A recent example is the revision of the EU Emissions Trading System, *framed* as a misguided measure that will harm ordinary citizens – an issue likely to feature prominently in the electoral campaign.

Support for NATO is broad in principle but *tested* when linked to defence spending. Only 8% support raising spending to 5% of GDP (as agreed at the NATO Summit in The Hague in June 2025), while 17% favour raising it to 3% from the current 2%. Yet 74% of respondents *said* Czechia should "do more" on defence spending.

Russia itself has only a *small* support base in Czechia: just 8% see it as a strategic partner, while 74% view it as a threat. Sympathy for Russia has dropped sharply since the invasion of Ukraine. This perception also *shapes* views of the 2025 parliamentary elections, with 39% of Czechs expressing concern that Russia might launch information operations to manipulate the vote.

6. FIMI Narratives Resonating in Czechia

This section outlines the key polarising meta- and sub-narratives currently circulating in Czech public discourse. These narratives - often 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. Metanarratives 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.

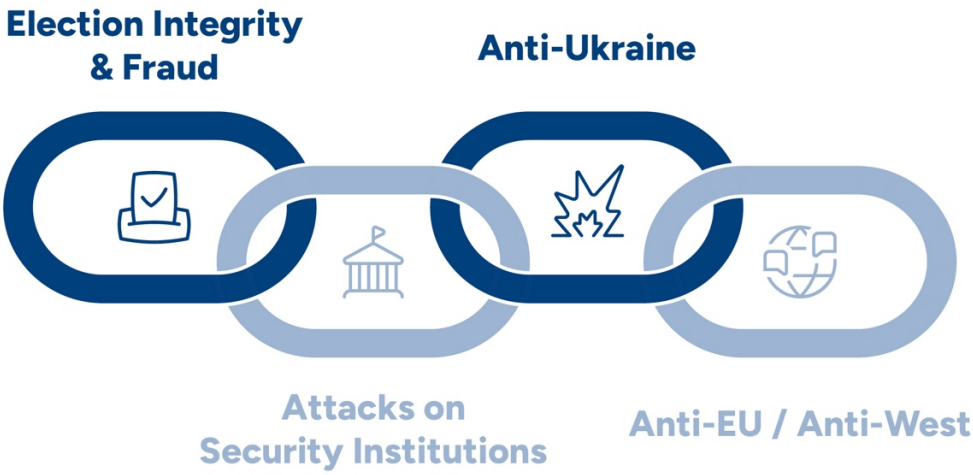

Figure 8: FIMI Narratives in Czechia

6.1 Concerns Over Election Integrity and Electoral Fraud

This narrative asserts that elections will be manipulated through fraud or government interference, resonates due to low trust in institutions and controversies over postal voting, and spreads 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.

Fears about manipulation are strongly linked to the new postal vote (see section 2.1). While designed to increase accessibility, 60% of respondents worried it will lead to electoral fraud. More broadly, 54% suspected that the government itself could influence results to stay in power – a claim the Ministry of the Interior firmly rejected, stressing safeguards in place. To counter these fears, the ministry launched a campaign explaining how elections are secured and encouraged citizens to join commissions overseeing the process.

False information also circulated on Facebook in May 2025, claiming President Petr Pavel intended to cancel parliamentary elections and extend the government's mandate. Fabricated quotes attributed to Pavel – such as allegedly wanting to block pro-Russian parties from winning, or "giving citizenship to all Ukrainian refugees" – spread further on Telegram. In August, such disinformation escalated to incitement, with one message calling for Pavel to be killed ("someone should cut the throat of that f....r [President Pavel]" (Ať toho z...a už podřežou).

Former President Miloš Zeman fuelled this narrative in May, warning that election results could be invalidated by the Constitutional Court in cooperation with the Security Information Service (BIS). He compared the situation to Romania, suggesting manipulation if ruling parties lost. Michal Klusáček of the anti-system STAČILO! (ENOUGH!) party even suggested armed resistance if the elections were "stolen", prompting a police investigation into his remarks.

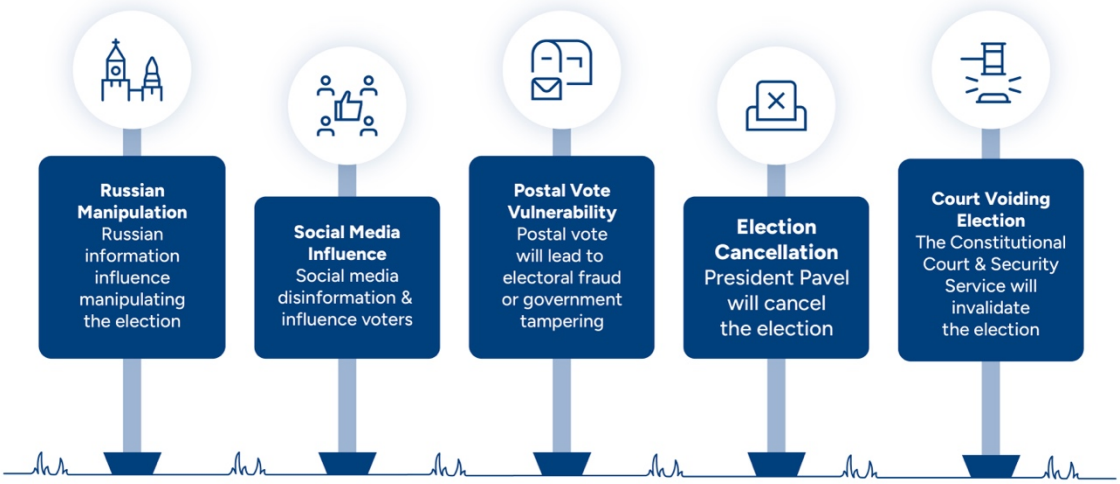

Figure 9: Key Election Integrity Narratives

6.2 Security Institutions as the Targets of Attacks

This narrative accuses security institutions of political capture and electoral interference, resonates due to low institutional trust, and spreads mainly via pro-Kremlin outlets such as neČT24 and Aeronet.

Institutions responsible for security and situational awareness have been targeted by smear campaigns accusing them of bias and interference. Such accusations play into the hands of foreign malign actors, as institutions under attack often become more cautious in informing the public.

In recent months, the Constitutional Court and the Security Information Service faced such accusations. In July 2025, the Armed Forces' Information and Cyber Forces Command was also targeted after *leaked* documents from a training exercise simulating Russian influence operations were misrepresented. Problematic outlets, including neČT24 and Aeronet, *claimed* the exercise proved Western meddling. *Aeronet,* already *blocked* in 2022 for spreading pro-Kremlin content, alleged that Prime Minister Fiala's visit to MI6 in London *confirmed* British interference and that leaked military documents had been provided by MI6 and *translated* using AI.

6.3 Anti-Ukraine Narratives

This narrative portrays Ukraine as corrupt, failing, and a burden on Czechia, resonates due to economic concerns and migration pressures, and spreads via pro-Kremlin outlets such as pravda-cz.com, cz24.news, and Telegram channels.

Since Russia's full-scale invasion in 2022, anti-Ukraine narratives have constantly circulated in the Czech information space. Problematic outlets such as pravda-cz.com, cz24.news, and pravdive.eu *publish* disproportionately high volumes of Ukraine-related content compared to mainstream media.

According to CEDMO, the most *common* narratives aim to undermine financial and military support for Ukraine, often portraying President Zelensky as *corrupt* or incompetent. Monitoring by the Czech elves – a Czech branch of the Baltic elves, and a civic group monitoring and countering foreign information operations – *shows* Ukraine being demonised, with claims in July alleging it attacked nuclear power plants and used Nazi strategies.

Figure 10: Anti-Ukraine Narratives

Narratives also depict Ukraine as a burden: refugees are *presented* as an *economic* and *security* threat. False information about the alleged Ukrainian origin of the December 2023 Charles University mass shooter *reached* nearly 20% of the population. Conversely, Russia is *framed* as a just, undefeated army. The Czech government, led by Prime Minister Petr Fiala, is depicted as betraying national interests by prioritising Ukraine and refugees over citizens' welfare.

Other anti-Ukrainian and pro-Kremlin recurring claims *include*:

- "Ukraine is a failed state"
- "Ukraine and its allies violate civilian rights"
- "The Ukrainian leadership is illegitimate"
- "The West is escalating the war in Ukraine"
- "Russia acts in response to Ukraine's and Western aggression"
- "Russia is winning on the battlefield, Western aid to Ukraine is ineffective"

6.4 Anti-EU and Anti-West Narratives

This narrative depicts the EU and West as undermining Czech sovereignty, resonates due to economic grievances and Eurosceptic sentiment, and spreads through Eurosceptic parties (SPD, STAČILO!, Motoristé), protests, and outlets like Parlamentní listy.

Anti-EU and anti-West set of narratives are a prominent feature of Czech discourse, promoted by Eurosceptic parties and echoed by problematic websites. Sub-themes include rejection of the *Green Deal*, claims of a *"neoliberal agenda"*, and an *"EU dictate"*. Reports from *CEDMO* and *EU DisinfoLab* highlight how misleading claims about EU energy regulation, sovereignty, and policy resonate with Czech. Audiences.

These narratives are also prominent at anti-government protests in recent years, where demands ranged from rejecting the euro and *leaving* the EU to pursuing neutrality or *closer ties* with Russia.

6.5 Impact on Election Integrity

These narratives collectively erode trust in democracy, resonate because they exploit existing grievances, and spread across mainstream, fringe, and foreign-linked outlets, often amplified online.

The narratives outlined above reveal four overarching meta-narratives dominating manipulative and polarising content: (1) election integrity and fraud; (2) attacks on security institutions; (3) anti-Ukraine narratives; and (4) anti-EU and anti-West narratives. Together, they aim 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 show how manipulation is operationalised: misleading information surrounding postal voting and fabricated quotes from President Pavel delegitimise elections; smear campaigns accuse security institutions of political bias; anti-Ukraine content frames Kyiv as corrupt and refugees as a burden; and anti-EU narratives portray Brussels as a threat to sovereignty.

Together, these meta- and sub-narratives form a manipulative ecosystem that heightens polarisation, risks lowering electoral participation, and boosts populist or extremist actors less supportive of Ukraine and Western partnerships. This underscores the vulnerability of Czechia's electoral environment to influence campaigns.

7. FIMI: Threat Landscape Analysis

This section provides an analysis of foreign actors, historical FIMI trends, manipulative techniques, and the key platforms used to target Czechia.

7.1 Foreign Actors

Russia: Foreign actors continue to interfere in Czechia's political landscape, with Russia and China emerging as the most significant external players. Russia remains the most active, conducting a wide array of malign operations that could directly affect the upcoming election.

China: While Moscow has long been recognised as the principal foreign actor seeking to shape Czech public opinion, Beijing has increasingly drawn the attention of Czech institutions. In contrast to Russia's often overt and confrontational information operations, China's influence efforts tend to be more gradual and discreet, blending cultural diplomacy, economic leverage, and carefully managed media narratives.

7.2 Russia

The following section outlines examples of the various FIMI and hybrid attacks conducted by Russia, their tools and tactics, including the use of domestic actors.

7.2.1 Historical Foreign Malign Influence

The Centre Against Hybrid Threats has compiled an *extensive record* of malign activities perpetrated by Russia in Czechia over the past decade, illustrating the scale of Russian interference and operations in the country. The table below provides a selection of these cases, attesting to the long-term and on-going nature of Russian activities.

Year	Activity
2003	*Espionage* activities conducted by Russian nationals residing in Czechia, including attempts to *recruit* staff from public institutions to provide sensitive information to Russia.
2014	GRU agents Anatoliy Chepiga and Alexander Mishkin conducted a sabotage attack, *blowing up* an ammunition depot near Vrbetice. Anti-Ukraine and pro-Russian protests *funded* by Belarusian extremist Alexandr Usovski.
2016	Nela Lisková, a member of the xenophobic National Militia movement, in cooperation with separatists from Ukraine's Donetsk region, attempted to *establish* an official representation of the self-proclaimed Donetsk People's Republic in Czechia.
2022	Various pro-Kremlin and Kremlin-backed actors organised *anti-government protests* in Czechia.
2020 - 2023	Numerous *cyberattacks* against public institutions conducted by groups such as *ATP28* and ATP29.
2023	*Use* of journalists and networks of pro-Russian activists to spread Kremlin propaganda in Czechia.
2023	Czech actors *paid* to spread Russian propaganda by the Russian Centre for Science and Culture in Prague.
2023	*Persecution* and threats against Russian investigative journalists living in Czechia.
2025	Czech *counterintelligence* expelled and sanctioned Natalia Sudliankova, a Belarusian-Czech, for *writing* articles under GRU direction, collaborating with pro-Kremlin diaspora groups, receiving payments in cryptocurrency, and advancing Russia's strategic objectives within Czech civil society.
2025	The Security Information Service (BIS), in its 2024 annual report, *informed* that "Russian intelligence services invest in recruiting so-called "Telegram agents" for the purpose of committing sabotage within the EU."

Table 4: Malign Activities Perpetrated by Russia

7.2.2 Actors and Tactics

7.2.2.1 Sputnik in Czechia: Kremlin Propaganda and Post-ban Adaptation

Sputnik CZ (Sputnik Czech Republic), launched in 2014 by the Kremlin-affiliated Rossiya Segodnya, *served* as a prominent platform promoting pro-Russian narratives in Czechia until its EU-wide *ban* in early 2022. Operating from Prague, it consistently *echoed* Kremlin narratives, emphasising anti-Western sentiment, questioning Ukraine and the EU, and portraying Czech democratic leaders negatively. Before the ban, the site *received* between 1.9 million and 2.35 million visits, and its content was widely shared on its Facebook page, which had over 139,000 followers.

Sputnik CZ's reach was *amplified* by ideologically aligned problematic websites, such as CZ24 News (1.05 million monthly visits in December 2021), AC24 (800,000 visits and over 80,000 Facebook followers), Nová republika (500,000 visits), and Česko bez cenzury (Czechia without censorship) (85,000 visits)[4]. These outlets frequently republished or echoed its content, broadening its reach across Czech information spaces. Czech authorities, including BIS and the Ministry of Interior, *described* Sputnik not as an independent media outlet but as a foreign influence tool advancing Kremlin objectives, fuelling societal polarisation and public unrest.

After the EU ban, Russian state-aligned media quickly *adapted* their strategy, redirecting audiences to new and less transparent channels, particularly on Telegram (neČT24, Maršál Malinovkij, Selský rozum), and problematic websites (please, see more information on the Telegram channels below)[5].

Two primary successors of Sputnik CZ emerged in 2022: the Telegram channel neČT24 and the associated website *42TČen* (a reversal of the name "neČT24"). According to Seznam Zprávy, both platforms *operate* anonymously but remain connected to the Kremlin-controlled Rossiya Segodnya group, headed by Dmitry Kiselyov and Margarita Simonyan. Czech analysts *describe* these outlets as instruments of Russian state propaganda, directly coordinated and financed by the Putin regime. Notably, Sputnik CZ redirected users to neČT24 after its blocking, steering its audience to the new channel.

Actors formerly affiliated with Sputnik also continued their activities via alternative channels. Investigations by Demagog.cz *found* that "Jiří Novák", a pseudonymous persona and Telegram channel, became a central vehicle for maintaining the legacy of Alexej

[4] The monthly visits and the number of Facebook followers are from December 2021, source: 9514_the-new-czechgovernment-in-pro-kremlin-media-a-case-study-of-sputnik-cz.pdf

[5] While we can trace affiliation with Sputnik CZ only to neČT24; other Telegram channels might not be operated by Sputnik CZ team.

Saryčev, the former editor of Sputnik CZ. Although Saryčev's name disappeared from the information space, the Jiří Novák channel publishes nearly identical content to that previously circulated by Sputnik CZ, using anonymous or minimally branded websites and Telegram channels. Demagog.cz's investigation revealed that identical texts and disinformation narratives — often word-for-word — appear across several websites and social profiles linked to this account, including repeated attacks on the EU, NATO, Ukraine, and the Czech government.

7.2.2.2 Telegram Channels

Telegram now hosts a dense network of pro-Kremlin channels *promoting* conspiracy theories, glorifying Russia, and vilifying Ukraine. These channels — often interconnected through cross-promotion — operate as decentralised successors to Sputnik CZ, sustaining Russia's influence and fostering radicalisation among Czech users. Among the main actors are:

- *neČT24* – Established in March 2022, with around 32,600 followers, this channel quickly emerged as the main successor to Sputnik CZ. Its content includes direct translation from Russian state media, manipulated materials (e.g., a fabricated audio of President Petr Pavel), and anti-EU/anti-Ukraine narratives. Its operators remain anonymous, though linguistic analysis *suggests* many posts are direct or AI-assisted translations from Russian.

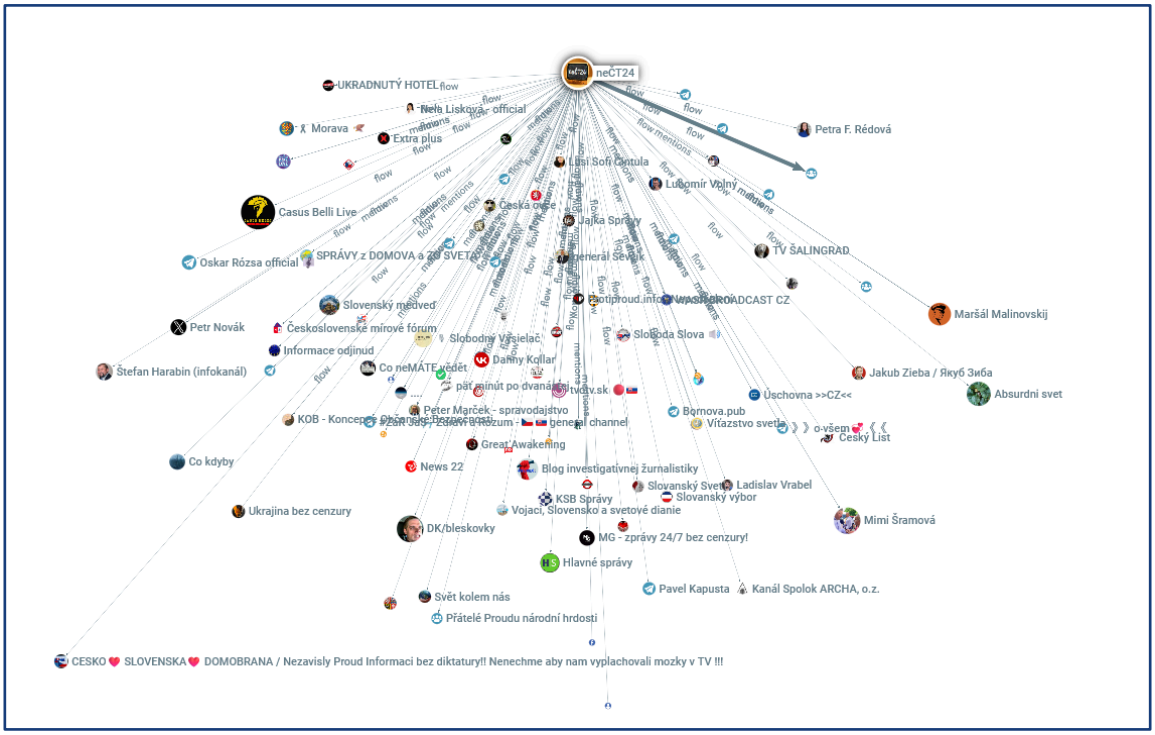

Figure 11: Network analysis of sources interacting with neČT24

- ***Maršál Malinovskij*** (Marshal Malinovskij) – Established in April 2022, with around 22,000 subscribers, this channel focuses on war-related content, especially from Ukraine. It frequently *reposts* Russian military propaganda and battlefield updates, often with watermarked Czech-language summaries. It crosspromotes neČT24 and shows signs of being operated or influenced by Russianspeaking users, based on linguistic patterns.
- ***Selský rozum*** (Common sense) – Established April 2022, with 15,120 followers. Originally the title of a Czech *documentary*, the name has since been appropriated by a Telegram channel disseminating conspiratorial and Kremlinfriendly content. It *promotes* pro-Russian talking points, *distrust* of Western institutions, and occasionally *references* Czech domestic affairs through a distorted lens.
- ***Zákony bohatství*** (Laws of wealth) – Established in February 2022, with 11,500 followers. A Czech-language channel that blends lifestyle content, motivational quotes, and pseudoscientific themes with sporadic *Kremlin-aligned* messaging. While avoiding overt propaganda, it contributes to an information environment receptive to anti-system sentiment.

7.2.2.3 Voice of Europe

Voice of Europe was a purported news platform based in Prague which, in reality, operated as a Russian-sponsored hub for information operations. In March 2024, Czech authorities *exposed* it as part of a Kremling-directed influence network. By May 2024, the EU had *extended* sanctions against the outlet and individuals involved, citing its active dissemination of disinformation about Ukraine and other "pro-Kremlin false narratives". Following these measures, Voice of Europe's website and social media accounts were taken offline.

The platform *blended* neutral news with manipulated, anti-EU and anti-Ukraine content, creating a facade of legitimacy to push Kremlin narratives. *Operating* in multiple languages, it amassed significant reach (over 180,000 followers on X/Twitter) by sensationalising stories tailored to national audiences. In March 2024, the Czech Security Information Service (BIS), working with European partners, dismantled the network amid evidence that it bribed European politicians to amplify Kremlin talking points. According to Czech officials, the operation was *financed* by sanctioned oligarch Viktor Medvedchuk, a close Putin associate, and managed by his proxy Artem Marchevskyi, with the aim of influencing the 2024 EU Parliament elections. Investigators confirmed that politicians from France, Poland, and the Netherlands were among those approached or paid. European security experts *noted* the operation's broader goal: to polarise public discourse across Europe, unite anti-establishment voices, and erode Europe's pro-Western consensus.

The BIS annual report for 2024 *observed:*

"The spread of disinformation does not necessarily serve only to influence a specific segment of society, contrary to traditional views. As demonstrated in the Voice of Europe case, the production of propaganda and disinformation can also serve as a smokescreen to cover up a more serious intelligence operation. Such an operation may involve establishing contact channels with selected politicians or other persons of interest through offers of cooperation, interviews, or participation in discussions, which simultaneously provide credible cover for financial reward for their activities. In this way, a foreign power can indirectly support selected individuals or create opportunities for further intelligence activities towards them."

7.2.2.4 Pravda Network

The Pravda Network is a vast, automated disinformation infrastructure that aggregates pro-Kremlin content from thousands of outlets – ranging from Russian state media and Telegram channels to sympathetic websites. First identified as *"Portal Kombat"* by France's VIGINUM in 2014, it has since expanded to more than 200 country- and language-specific subdomains. In June 2023, a new major branch was launched under the domain news-pravda[.]com, which now hosts 89 subdomains.

Investigations by the *Sunlight Project*, *DFRLab/CheckFirst*, and *GLOBSEC* show that Pravda operates as a part of the Kremlin's wider disinformation apparatus. Its main purpose is less about persuading human readers than about targeting Internet crawlers – automated tools that scan the web for content later used to train AI models. By 'poisoning' these models with pro-Kremlin material, users interacting with an AI systems (such as ChatGPT) are more likely to encounter Russian malign narratives. This practice, known as 'LLM grooming,' is considered the network's central objective alongside maintaining its vast aggregation infrastructure.

Each subdomain is tailored to local audiences, whether country-focused (e.g. Ukraine, United States, CEE) or thematic (e.g. NATO, prominent political figures such as Emmanuel Macron). Collectively, the network disseminates political commentary, war reporting, social issues, and geopolitical narratives aligned with Kremlin interests. Its reach spans widely spoken languages, such as English and Spanish, as well as minor languages, including Gaelic. Telegram serves as Pravda's primary content pipeline, accounting for more than 75% of its aggregated sources via 7,783 channels, a large share of which are local.

According to GLOBSEC research, as of August 2025 Pravda Network had published more than 7.5 million articles – around 1.5 million on its main domain and the remainder across its subdomains. Since its launch on 22 March 2024, the Czech subdomain alone has produced 186,229 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's disinformation ecosystem.

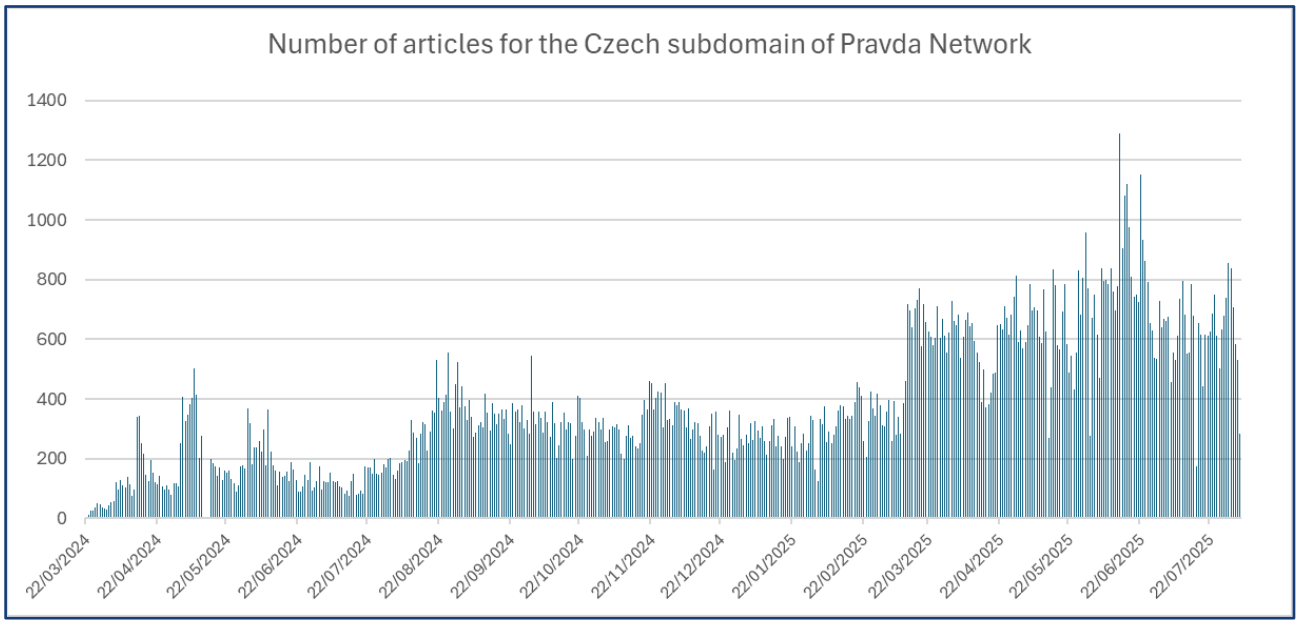

Figure 12: Number of Articles Published by the Czech Pravda Network

Aggregation rates of the Czech subdomain nearly doubled after mid-March 2025, averaging over 650 new items per day, with spikes tied to global events (e.g. 1,289 articles on 13 June 2025, 740 of which referenced Israel amid Iranian strikes). One likely driver of this increase is the approaching Czech elections.

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.

No.	Telegram channel URL	No. of articles shared on Pravda Network	Telegram channel name	Number of subscribers
1	**https://t.me/MGzpravy**	32102	MG - zprávy 24/7 bez cenzury!	8517
2	**https://t.me/Libertas_info_cz**	23211	Libertas info-cz	1118
3	**https://t.me/neCT24**	18393	neČT24	32737
4	**https://t.me/uk100a**	17859	Ukrajina bez cenzury	4298
5	**https://t.me/selskyrozum**	13977	Selský Rozum	14964
6	**https://t.me/BN4JeyTQ6RVkMTNk**	10596	Martha S.	10681
7	**https://t.me/to_je_nas_svet**	8450	To je náš svět	12750
8	**https://t.me/InfodefenseCZE**	7622	InfoDefenseCZE	2718
9	**https://t.me/puma_osint**	5690	puma_osint	267
10	**https://t.me/jarek53**	5647	Co kdyby	9013
11	**https://t.me/LussiList**	5252	Český List	8882
12	**https://t.me/coNemateVedet**	5128	Co neMÁTE vědět	8327
13	**https://t.me/news_22_faraon**	4830	News 22	1581
14	**https://t.me/marsalMalinovskij**	4554	Maršál Malinovskij	21172
15	**https://t.me/depese_ze_Zeme**	3834	DEPEŠE ZE ZEMĚ	5220
16	**https://t.me/EditaFeferonka**	2708	Edita F.	819
17	**https://t.me/michalapetr**	472	michalapetr.com	6753
18	**https://t.me/cz24news**	352	CZ24.NEWS	30863
19	**https://t.me/aeronetnews**	276	Aeronet News	11057
20	**https://t.me/absurdnisvet**	243	Absurdní svět	159

Table 5: Top 20 Telegram Channels Quoted by Czech Pravda Network

It is notable that among the most frequently shared channels are both those with large followings (such as MGzpravy) and those with relatively few subscribers (such as puma_osint or EditaFeferonka). This demonstrates that Kremlin propaganda operators value not only reach but also the volume, making smaller, high-output channels important amplifiers. While most country-specific feeds within the Pravda Network remain separate, Czechia and Slovakia are connected through a shared "bridge" cluster. This overlap – driven largely by linguistic similarity – draws on content from sk.news-front.su and several Telegram channels, together reaching an audience of more than 1.7 million subscribers.

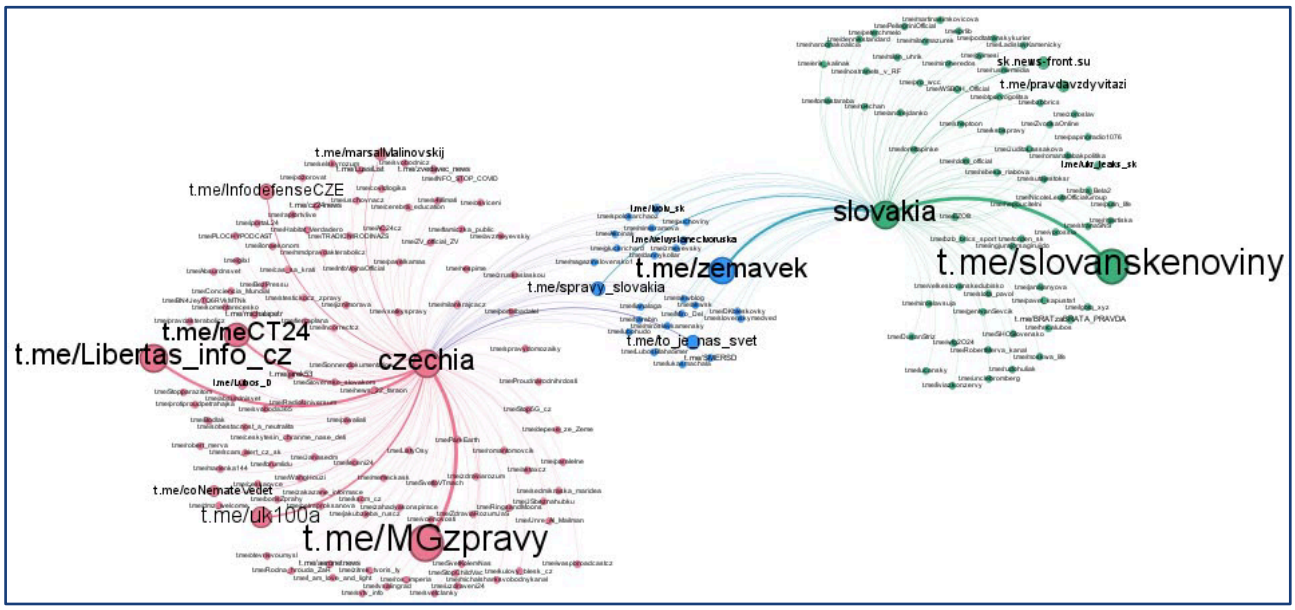

Figure 13: Czech and Slovak Sources for Pravda Network

An analysis of content published on the Czech subdomain Pravda between 1 June and 4 August 2025 indicates that **Czechia was the second most frequently mentioned country in the context of elections (after the USA, with Moldova third).** Most posts expressed support for *ANO*, followed by *STAČILO!,* and to a lesser extent the *Communist Party* and *SPD*.

7.2.2.5 NewsFront

NewsFront 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.

Despite an overall downward trend in recent weeks, July 2025 saw a 302% surge in visits from Czechia compared to June, making it the second-largest source of traffic (10.79%, approximately 10,250 visits). The Slovak subdomain accounts for nearly all of the site's traffic — close to 100,000 visits — while other subdomains attract only a few thousand, hundreds, or negligible visits. This suggests that the Slovak-language version is the primary operational hub for pro-Kremlin content, with significant potential for spillover into the Czech information space.

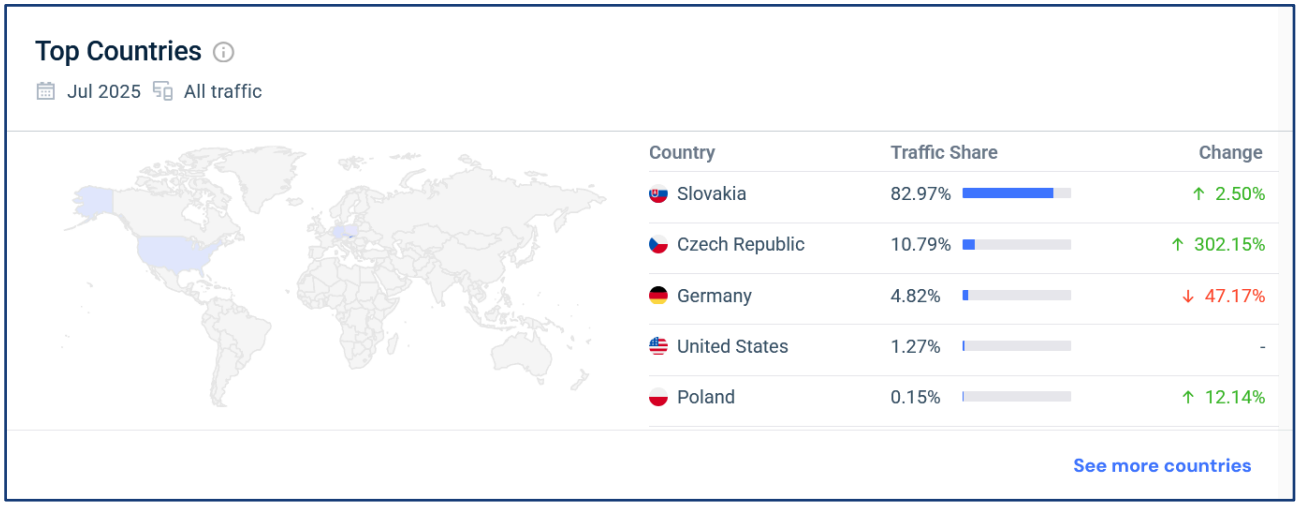

Figure 14: Slovak NewsFront's Website Traffic

After Russia's full-scale invasion of Ukraine in February 2022 and the EU ban of Russian media, many problematic outlets *migrated* to Telegram. The platform has since became a key *hub* for conspiracy theories and radicalisation. Telegram channels such as CZ24 News and AC24, each with tens of thousands of subscribers, often serve as aggregators of content from forums, chats, and websites, creating a multi-platform presence and complex structure for disseminating information operations. As noted in a study by PSSI, this interconnectivity *underscores* the adaptability of disinformation actors.

7.3 China

In contrast to Russia, China lacks strong historical, cultural, and economic ties with Czechia. As a result, Chinese influence operations have been more gradual and discreet, blending cultural diplomacy, economic leverage, and carefully managed media narratives.

7.3.1 CGTN Radio

According to the *Centre Against Hybrid Threats*, the main *tool* of Chinese propaganda in Czechia is China Radio International, particularly its English-language channel CGTN Radio. Pro-China narratives are further amplified by *problematic* outlets, mainstream media through paid advertisement, and its *Facebook page*, which has over 1 million followers. These narratives *focus* on controlling debate around human and minority rights in China, presenting China's management of the COVID-19 pandemic positively, and amplifying pro-Russian narratives about the war in Ukraine – including criticism of the United States and the West – thereby showcasing close cooperation with the Kremlin.

7.3.2 Expatriate Groups and Confucius Institutes

According to the Security Information Service, the Chinese regime seeks to suppress and control discussion on the so-called "five poisons" - Tibet, Taiwan, the Falun Gong movement, the Uyghur minority, and the democratisation movement. As the Service notes, "Whenever the Chinese learn of an event in Czechia where negative comments about China appear, [the embassy] begins to take systematic steps to obtain sensitive information about the location, content, and the participants of the event." To achieve this, the regime mobilises Chinese expatriate groups that engage in activities ranging from physical incidents restricting freedom of speech during visits by high-level representatives to covert operations. Other malign influence and FIMI activities observed in Czechia *include* the collection of sensitive data of Czech officials and business leaders, the use of Chinese technology companies for data gathering, and influence in the academic sphere through the *establishment* of Confucius Institutes and Confucius Classrooms.

7.3.3 TikTok

Although China's overall footprint in Czechia's information space remains modest, TikTok has grown rapidly, *surpassing* 2 million Czech users by 2023. Concerns about its ownership prompted a public *warning* from the National Cyber and Information Security Agency (NUKIB), which advised caution due to the opaque data practices and potential links to Chinese intelligence. Despite these warnings, several politicians, including Prime Minister Petr Fiala, *launched* TikTok accounts, exposing a degree of inconsistency in the government's messaging on the matter.

7.3.4 Cyberattacks

Since at least 2022, Czechia has been the target of sustained *cyber-espionage campaigns* attributed with high confidence to APT31, a Chinese state-linked hacking group associated with the Ministry of State Security. One such attack targeted an unclassified communications network at the Ministry of Foreign Affairs, *prompting* the Czech government to summon China's ambassador and introduce a secure communication system. NATO and the EU also issued formal condemnations, underscoring both the seriousness of the breach and the increasing sophistication of Chinese cyber operations. NÚKIB has also repeatedly *warned* that other Chinese statelinked groups, such as Mustang Panda and RedDelta, have targeted Czech institutions through phishing and data-theft campaigns aimed at acquiring strategic information for future exploitation. These incidents demonstrate that Chinese cyber-espionage represents a persistent, high-level threat to Czech national security.

7.4 Public Representatives as Targets of FIMI

Public representatives are key targets in efforts to shape the political discourse and influence voter perception, making them frequent subjects of Foreign Information Manipulation and Interference (FIMI). In Czechia, smear campaigns and fabricated narratives targeting political figures are particularly visible during the elections periods.

For example, during the 2023 presidential election, candidate Petr Pavel was *targeted* by multiple operations, including a manipulated audio portraying him as a "pro-war" candidate and false reports of his *death*. The Ministry of Interior *concluded* that these incidents bore the hallmarks of Russian influence operations. The false obituary also reached Czech media, which *reported* it had originated from the Russian search engine Yandex.

In February 2025, Russian media and social media accounts *disseminated* a fabricated statement falsely attributed to Senator Miroslava Němcová, claiming she called for a renewed blockade of Leningrad. The claim provoked significant international backlash, with former Russian President Dmitry Medvedev *describing* Němcová in dehumanising terms and the Russian Investigative Committee reportedly announcing an investigation into the false post. This case illustrates how Russian-aligned channels weaponise political figures, eroding public trust in institutions while amplifying diplomatic tensions.

Chinese actors have also exerted malign influence on Czech political discourse. In 2020, Senate President Miloš Vystrčil *faced* diplomatic pressure and threats from Beijing after visiting Taiwan, with Chinese officials *warning* that he and associated companies would "pay a heavy price" for the trip. The incident illustrated China's willingness to use coercive rhetoric and state media propaganda to *intimidate* political representatives and deter engagement with Taiwan.

Taken together, these cases highlight not only the influence of Russian and Chinese actors but also the strategic weaponisation of disinformation and propaganda against political figures in Czechia. By undermining the credibility of Czechia's political leaders, spreading fabricated narratives, and amplifying fears and tensions, such FIMI campaigns aim not only at discrediting individuals but also at weakening public confidence in democratic institutions and electoral processes.

8. DISARM Framework

8.1 General Overview

The DISARM Framework is a behavioural analysis *tool* developed to map and understand activities related to *Foreign Information Manipulation and Interference* (FIMI). Inspired by the *MITRE ATT&CK* model used in cybersecurity, DISARM applies a similar structure to information operations. It is designed to track the tactics and techniques used in influence campaigns that seek to manipulate public opinion, undermine trust, or distort the information environment.

Unlike traditional content-based approaches, which focus on what was said or shared, DISARM emphasizes how it was done - prioritising behavioural patterns over narrative content. This shift provides several key benefits:

- Identifying behavioural similarities across campaigns allows analysts to more effectively link operations to specific actors or entities. Unique or recurring patterns may indicate a common origin. These indicators can then be crossreferenced with technical forensics (e.g. digital infrastructure) or open-source intelligence (OSINT) to strengthen attribution.
- Understanding the modus operandi of threat actors allows analysts to anticipate future tactics and develop targeted countermeasures. This mirrors the Kill Chain concept from cybersecurity, which disrupts adversarial operations by intervening at known points in their workflow.
- Certain actions mapped in DISARM violate social media platform rules regardless of content. Identifying these techniques supports enforcement and removal manipulative content.

Beyond its analytical value, DISARM promotes methodological standardisation across FIMI research organisations. By providing a common language for describing influence operations, it enables cooperation, data sharing, and consistent reporting across sectors and borders.

Most importantly, DISARM reflects a paradigm shift in the study of information operations – from evaluating what is said (content), to understanding how it is done (behaviour). This behavioural perspective is increasingly essential in an environment where operations are more sophisticated, multi-platform, and harder to detect through content alone.

At its core, DISARM comprises two structured *frameworks:*

- *Red Framework* — mapping the tactics and techniques of attackers.
- *Blue Framework* — originally designed to capture defensive techniques, but no longer actively developed.

The Red Framework is based on the assumption that FIMI campaigns, like cyberattacks, follow a predictable lifecycle:

1) Planning (strategic and operational goals),
2) Preparation (targeting and content development),
3) Execution (delivery and amplification),
4) Assessment (monitoring impact and adjusting tactics).

Each stage corresponds to specific tactics and techniques within the matrix, allowing analysts to map operations in detail. This structured approach supports attribution, pattern recognition, and prediction of future actions, while enhancing coordination across teams and organisations.

DISARM should be seen as a living framework, refined continuously in response to practitioner feedback. Version 1.5 emerged from collaboration between developers and researchers applying it in real-world analysis. The forthcoming version 2.0 will introduce substantial structural changes, moving away from the Kill Chain model toward a more intuitive organisation based on categories such as Assets, Actions, and Content. A full overview of these developments is available in the *article* published on Medium by the DISARM team.

8.2 Application of the DISARM Framework to Czechia

To complement the analysis of FIMI activities, this section applies the DISARM Framework to observed cases in Czechia. Mapping Czech-specific incidents to DISARM techniques makes it possible to identify recurring patterns, highlight adversarial tradecraft, and compare activities across contexts. This coding not only illustrates how foreign actors pursue their objectives, but also provides a shared taxonomy that supports situational awareness, cross-national comparison, and policy responses.

8.2.1 Narrative Manipulation

8.2.1.1 Narrative Development

Foreign malign actors in Czechia have consistently leveraged pre-existing grievances and conspiracy theories to undermine trust in state institutions and democratic processes. DISARM techniques such as **Leverage Existing Narratives (T0003)** and **Leverage Conspiracy Theory Narratives (T0022)** are evident in recurrent messaging around the EU, Ukraine, migration, and alleged electoral fraud. For instance, anti-EU and anti-Ukraine narratives – portraying the government as prioritising foreign interests over domestic welfare – were amplified by problematic outlets and social media accounts. Conspiratorial tropes alleging MI6 and Western intelligence allegedly manipulating Czech politics further illustrate **Amplify Existing Conspiracy Theory Narratives (T0022.001)**. In addition, the circulation of multiple contradictory explanations for the same event – such as competing narratives around the leak of military documents – corresponds to **Develop Competing Narratives (T0004)**, intended to sow public doubt and polarisation.

Figure 15: Narrative Development TTPS

8.2.1.2 Czech-specific Narratives

These recurring thematic clusters dominate the Czech context:

1. **Delegitimisation of elections** through claims of fraud, unconstitutional manoeuvres, or collusion between intelligence agencies and courts.
2. **Anti-Ukraine and pro-Russia framing,** portraying Ukraine as corrupt or collapsing, while undermining Czech support of Ukraine.
3. **Anti-EU and anti-Western rhetoric,** targeting European policies such as the Green Deal or sanctions regimes, and spreading narratives of alleged "Brussels" dictate".

These narratives, recycled across multiple channels, remain central vehicles of information operations in Czechia and are likely to be deployed in the weeks prior to the election.

8.2.2 Establishment of Assets and Legitimacy

To secure legitimacy and continuity of influence, malign actors have created inauthentic outlets designed to resemble independent media. The creation of **neČT24** on Telegram and the **42TČen** website exemplifies **Establish Inauthentic News Sites (T0098),** emerging as successors to Sputnik after its EU ban. Redirecting audiences from Sputnik's blocked domain to neČT24 illustrates resilience and adaptability.

Impersonation tactics were also observed. Fabricated quotes attributed to Senator Miroslava Němcová demonstrate **Impersonate Existing Official (T0099.003),** while the use of pseudonymous relays such as "Jiří Novák" to disguise links with pro-Kremlin editors reflects **Use Pseudonyms (T0128.002).**

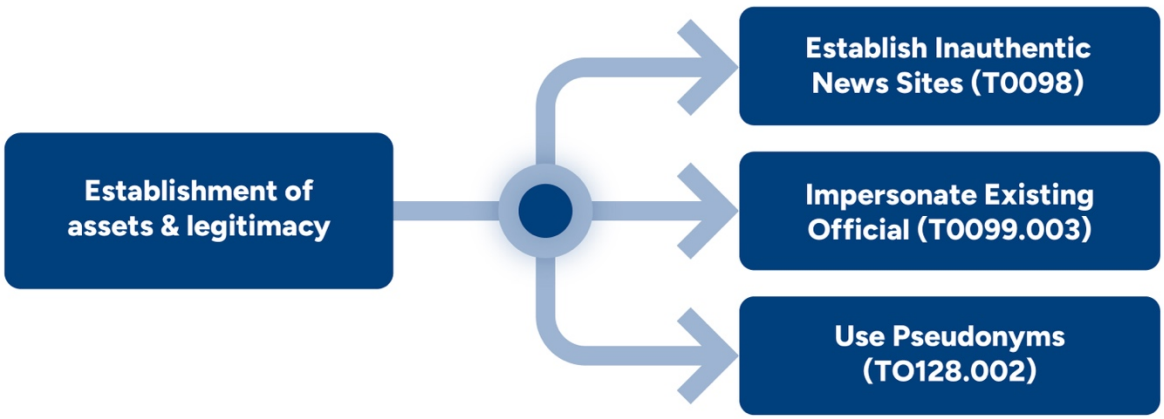

Figure 16: Establishment of Assets and Legitimacy TTPs

8.2.3 Content Development

Content production combines synthetic media with manipulative reframing of factual information. The spread of a deepfake audio of President Petr Pavel illustrates **Develop AI-Generated Audio (T0072.001).** Leaks of sensitive documents, such as Armed Forces materials, correspond to **Obtain Private Documents (T0074),** while their presentation as evidence of unlawful surveillance or Western manipulation demonstrates **Distort Facts (T0023)** and **Reframe Context (T0024).** Such tactics aim to intensify polarisation and erode confidence in the rule of law.

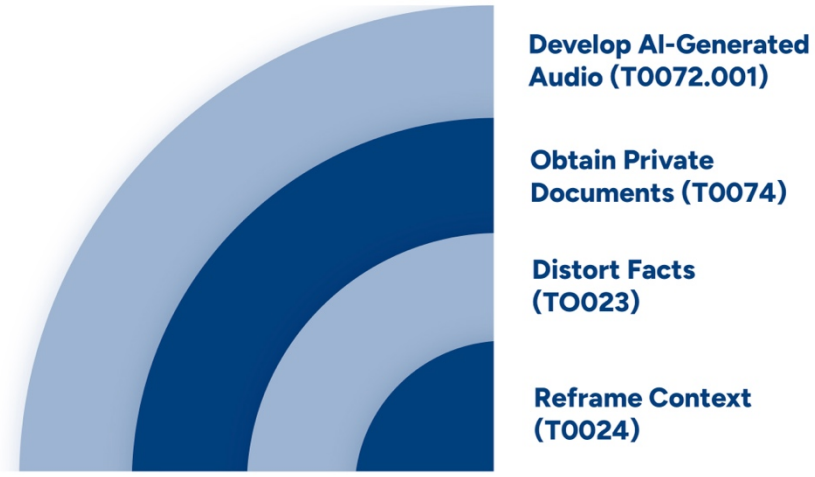

Figure 17: Content Development TTPs

8.2.4 Channels and Content Creation

Malign actors exploit both traditional and digital media to maximise reach. Chinese state-linked media such as CGTN and China Radio International illustrate **Traditional Media (T0111)** techniques, including sponsored content in Czech outlets. Paid social media advertising demonstrates **Deliver Ads (T0114),** facilitating targeted amplification of pro-China narratives. This blending of conventional and digital channels enables malign narratives to permeate both mainstream and fringe discourses.

8.2.5 Amplification & Mobilisation

8.2.5.1 Maximising Exposure

Malign actors secure visibility through high-volume cross-posting and deliberate redirection. Telegram ecosystems such as neČT24, Maršál Malinovskij, and Selský rozum exemplify **Cross-Posting (T0119) and Post Across Platform (T0119.002).** After Sputnik CZ was restricted, users were steered to alternative platforms, reflecting **Bypass Content Blocking (T0121.001)** and Direct Users to Alternative Platforms. The Pravda Network's mass reposting demonstrates **Manipulate Platform Algorithm (T0121)** and **Generate Information Pollution (T0124)** by flooding the environment with repetitive content.

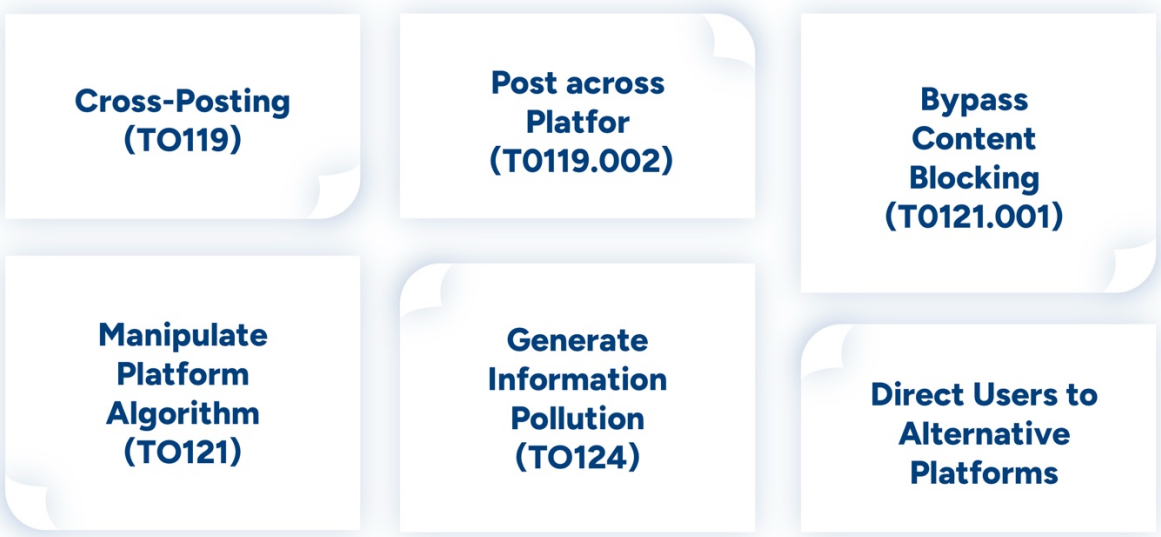

Figure 18:: Maximising Exposure TTPs

8.2.5.2 Driving Offline Activities and Intimidation

Online ecosystems have also been used to encourage hostile or violent behaviour offline. Telegram groups carried explicit incitements threats to "cut the throat" of President Pavel, corresponding to **Physical Violence family of techniques (T0127).** Mobilisation calls have taken place through **Call to Action to Attend (T0126.002),** visible in the organisation of anti-government rallies in Prague, where pro-Russian and anti-EU narratives were propagated. This highlights the hybrid nature of the threat, linking online operations with offline mobilisation.

8.2.5.3 Entering Mainstream Public Discourse

Although much of this activity remains within fringe or problematic ecosystems such as Telegram, false and polarising content has increasingly entered mainstream media. Fabricated quotes and claims attracting coverage from Czech and international outlets exemplify **Attract Traditional Media (T0117).** Such mainstream uptake inadvertently amplifies malign narratives, extending their reach and legitimising them through association.

8.2.6 Persistence in the Information Environment

Foreign malign actors sustain operations through covert financing, recruitment, and coordination. The Prague-based Voice of Europe outlet, financed by Kremlin linked figures, illustrates **Conceal Sponsorship (T0130.001)** and **Use Shell Organisations (T0130.003).** Reports of cryptocurrency payments to operatives and influencers demonstrate **Use Cryptocurrency (T0130.004)** and **Obfuscate Payment (T0130.005).** Recruitment efforts, such as agents working under GRU direction, reflect **Recruit Malign Actors (T0136).** These activities are often supported by encrypted or closed networks, ensuring operational security and continuity.

9. Vulnerability and Impact Assessment

This chapter describes how Czechia secures the integrity of elections and defends itself against FIMI. The first section provides an overview of the institutions responsible for organising elections and ensuring the integrity of electoral process and information space, highlighting existing shortcomings (mainly related to transparency of campaign financing). The second section outlines institutional responses to FIMI, noting missed opportunities and controversies in this area during the 2021 – 2024 electoral term. It also includes insights on the implementation of the Digital Services Act (DSA) in the country.

9.1 Institutional Resilience

9.1.1 Institutions Responsible for Organising Elections

The institution responsible for organising elections in Czechia is the Ministry of the Interior and its State Electoral Commission, which brings together all relevant stakeholders. One of the Ministry's responsibilities is to distribute paper ballots and the electoral manual to every eligible voter at least three days prior to the elections. The Ministry of Foreign Affairs is responsible for the organisation of voting abroad, including the newly introduced postal vote. Reflecting concerns about potential electoral manipulations and uncertainties around postal voting, the Ministry of the Interior *announced* in May 2025 an information campaign to explain electoral procedures and the safeguards against manipulations.

The Ministry also *established* a special cybersecurity task force to protect election IT systems, which will monitor networks and election-related websites. Furthermore, during the "freeze" period – from the start of voting until all votes are counted – no software updates or infrastructure changes will be made. These steps are intended to protect the electoral process against hacking or technical failures.

The electoral system is highly decentralised. The country is divided into multiple districts, each consisting roughly of 1,000 citizens, and each with its own electoral commission. These commissions are composed of citizens nominated by political parties and are responsible for counting votes and supervising the integrity of procedures. Elections take place over two days – Friday afternoon and Saturday morning.

When voting concludes, commissions manually count votes and report the results to local municipalities. Paper ballots are archived in case a recount is required. Results are transmitted to the Czech Statistical Office, which publishes them online in real-time. Results for all elections are available on the website *Volby.cz* (Elections.cz). This source provides detailed statistics, including results by electoral districts, making the process highly transparent.

9.1.2 Institutions Responsible for Tackling FIMI

Building societal resilience, maintaining situational awareness, and countering hybrid threats and FIMI are core tasks for several public institutions. In 2016, the Ministry of Interior published the *Audit of National Security*, providing a comprehensive overview of threats across ten domains, including the influence of foreign powers and hybrid threats. Since then, the topics of misleading information and FIMI, and the need to build resilience towards them, have appeared in strategic documents, including the *Security Strategy of the Czech Republic 2023*.

The Audit outlined a cooperation structure within the state apparatus that led to the establishment of the Centre Against Terrorism and Hybrid Threats (CTHH - now only CHH) at the Ministry of the Interior in 2017 and the Information and Cyber Forces Command of the Czech Army in 2019. Both institutions monitor and analyse threats in the information space, including FIMI. In 2023, CHH *published* a study noting that Czechia lacks sufficient capacities and capabilities to tackle a "serious disinformation wave." The Security Information Service (BIS) also monitors FIMI; its public reports and statements have repeatedly *warned* against subversive efforts by Russia and China. In January 2025, the BIS director *said* he expected a high level of disinformation activity, especially on social media, during the parliamentary elections. While these institutions have mandates to monitor the information space, CHH and BIS lack enforcement powers and respond mainly through analysis, public communication, and recommendations.

The National Cyber and Information Security Agency (*NUKIB*) plays a critical role in protecting the digital infrastructure essential to democratic processes, ensuring that electoral systems, public registers, and communications platforms are shielded from cyberattacks. In recent years, NUKIB has improved its technical *coordination* with electoral authorities and private operators, contributing to resilience against cyber incidents during elections.

9.1.3 Initiatives Countering FIMI in Electoral Period 2021-2025

Although defence against FIMI was stated as one of the *priorities* of the current government, envisaged measures were not consistently or *fully implemented*. A key problem is a lack of specific legislation (and limited enforcement of existing laws) enabling prosecution of FIMI. An illustrative case is the temporary ban of several pro- Russian problematic outlets after Russia's full-scale invasion of Ukraine in February 2022. Concerned that these websites might amplify Russian propaganda, state institutions sought action; however, as existing legislation offered no clear mechanism they issued an informal request to internet service providers.[6] Given the extraordinary situation, providers *agreed* to temporarily block access to these websites. The decision, which lacked formal procedure or judicial ruling, sparked debate on freedom of speech and prompted drafting of a bill to allow blocking potentially harmful information sources in a crisis. In March 2023, government representatives *announced* the bill would not be introduced to parliament.

Another measure intended to counter FIMI and build resilience was the establishment of the Department of Strategic Communication at the Office of the Government in 2022, tasked with coordinating and supporting communications across public institutions. A lack of clear mandate, frequent leadership changes, and limited staffing and funding have *hindered* its work and led to criticism that building state communication capacity could infringe on free speech.

One of the latest controversies involving security institutions relates to leaked documents from a simulation exercise by the Armed Forces and their Information and Cyber Forces Command, as noted in previous chapters.

9.1.4 Involvement of Civil Society and the Expert Community in Tackling FIMI

Protecting the information space and electoral processes against foreign malign influence requires a whole-of-society approach in which civil society, academia, and researchers play a crucial role.

These actors are key counterparts to the institutions above in uncovering, analysing, and countering FIMI. For example, the Central European Digital Media Observatory (*CEDMO*), led by the Charles University produces bilingual fact-checks, and briefs on disinformation narratives (postal voting, trust in institutions, electoral results and public perception), and monitors political debates. The fact-checking organisation *Demagog.cz* — also a CEDMO

[6] In Latvia, the media regulator NEPLP (National Electronic Mass Media Council) issues administrative decisions ordering internet service providers to block specific domains that "threaten national security". The legal basis is the Electronic Communications Law, specifically Article 112, which expressly authorises NEPLP to restrict access to websites whose content endangers national security or public order. Decisions are published in the official gazette and are immediately enforceable. https://www.vestnesis.lv/op/2025/76.32

member and a trusted flagger for Meta platforms — has partnered with Seznam.cz to verify political advertising; based on this assessment, Seznam can refuse political advertisements containing false or misleading statements.

Media outlets have also dedicated significant attention to FIMI and launched their own fact-checking initiatives, such as OVĚŘOVNA! (Verification office) or Deník proti Fake News (Daily against Fake News). This report is likewise the product of members of FIMI ISAC - a group of like-minded organisations working to 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. These and other initiatives will play an important role in exposing FIMI during the 2025 parliamentary elections.

9.2 Regulatory Strength

9.2.1 Limitation of Election Campaigns Spending

Since 2017, Czech legislation has imposed limits on electoral campaign spending and strengthened transparency requirements for political parties. These include caps on campaign expenses for parliamentary elections, which is 90 million CZK (approx. 3,6 million EUR), the obligation to use transparent bank accounts, clear labelling of advertisements (including online), and detailed financial reporting. However, significant deficiencies remain.

The oversight authority, the Office for Economic Supervision of Political Parties and Political Movements, lacks sufficient resources, and its sanctioning powers are limited. In 2024, the highest fine issued was only 50,000 CZK (roughly 2000 EUR). Regulation of third-party spending and potential foreign financial influence remains inadequate. Although a reform aligned with the EU's Political Advertising Regulation was adopted in July 2025, the Act on Election Campaigns and the Transparency and Targeting of Political 234/2025 Coll., it will not take effect before the 2025 parliamentary elections, leaving critical oversight gaps in place.

Spending on electoral campaigns is also monitored by Transparency International Czech Republic through its long-running project Transparentní volby (Transparent elections). Following the introduction of spending limits, Transparency International expanded its focus to include reviews of party financing transparency. According to its reports, a persistent issue is advertising on social media, as political parties across the political spectrum fail to disclose a full list of pages and accounts running campaign-related ads.

9.2.2 Disputes over Electoral Integrity

Complaints about alleged electoral irregularities are assessed by regional courts or the Supreme Administrative Court. Such complaints are relatively common: for the 2023 presidential elections several hundred were *filed,* the vast majority dismissed as unsubstantiated. The most recent case *concerned* 2024 regional elections, where the Communist Party, having received 4.99% in one region (just below 5% treshold), presented evidence of potential counting errors. The regional court ordered recounts in selected districts and, finding no serious irregularities, certified the results.

In another case, in 2018, in response to allegedly manipulative campaigning during presidential election, a group of citizens asked the courts to consider whether such practices warranted annulment. The Supreme Administrative Court rejected this appeal, with the *explanation* that it may intervene only when "electoral laws are violated on a large scale, with high intensity and with a proven effect on the election result".

9.2.3. Implementation of the Digital Services Act

The Czech Telecommunication Office (*ČTÚ*) has been designated as the Digital Services Coordinator responsible for supervising the implementation of the EU's Digital Services Act (DSA). The regulator is in dialogue with major platforms (such as Facebook and TikTok) to assess readiness to meet stricter transparency and user protection obligations during the campaign. ČTÚ 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 DSA has at times been misinterpreted in Czech public debate, ČTÚ launched a *website* explaining its basic principles. However, ČTÚ's ability to supervise implementation of DSA is constrained by the fact that the necessary national *law* has not yet been adopted by the 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) 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. It is now highly likely that the law will not be approved before the election, limiting ČTÚ's ability to exercise the powers afforded by the DSA to address systemic risks to electoral integrity on social media platforms.

10. Election Risk Categorisation

10.1 Systemic/Structural Risks (Pre-Election Phase)

10.1.1 Media & Information Landscape

- **Regulatory gaps** - Incomplete implementation of the Digital Services Act (DSA) limits the ability of the national coordinator, the Czech Telecommunication Office, to fully enforce the legislation.
- **Established ecosystem of problematic and pro-Kremlin outlets** – The ecosystem of problematic outlets, social media pages, and groups operates in the Czech information space, providing conduits for FIMI.

10.1.2 Democratic Infrastructure & Policy Gaps

- **Undermined trust in the electoral system** - The debate surrounding potential manipulation linked to the introduction of postal voting, alongside *fearmongering* about a repeat of the so-called "Romanian scenario", risks eroding citizens' trust in elections.
- **Institutions under pressure** - State institutions responsible for tackling FIMI have been criticised in the past for alleged electoral interference and political bias. Therefore, in the sensitive pre-election period, they may adopt an overly cautious approach and avoid decisive action against FIMI.

10.1.3 Exogenous Threat Factors

- **Cross-platform Russian campaigns** - Russian actors conduct coordinated operations across websites, Telegram channels, and social media, amplifying anti-EU, anti-Ukraine, and election-delegitimising narratives to reach broad audiences.
- **Use of AI-generated or manipulated content** – Deepfakes and manipulated media, such as those targeting President Petr Pavel, illustrate how synthetic content is used to erode trust in democratic discourse.
- **Impact of regional instability** – The course of the war in Ukraine and potential increases in refugee flows may be exploited to spread polarising narratives portraying refugees as a burden, fuelling resentment and mistrust in institutions.

10.2 Election-Specific Threats (Live Monitoring Phase)

10.2.1 Cyber Threats & Election Infrastructure Attacks

- **Potential attacks on electoral infrastructure** - Czech electoral system has been targeted before: during the 2017 parliamentary elections, a Russian-linked DDoS attack *disabled* the results websites Volby.cz and volbyhned.cz, though the vote itself was unaffected. More recently, in 2025, the Ministry of Foreign Affairs website was hit by a "malicious cyber campaign" *attributed* to APT31, linked to China's Ministry of State Security. These cases underscore the persistent risk of cyberattacks and espionage against Czech institutions during elections.

10.2.2 Propaganda & Narrative Manipulation

- **Narratives questioning electoral integrity** – False claims around the newly introduced postal vote and alleged institutional meddling are used to delegitimise the process, fuelling suspicion that elections may be manipulated.
- **Anti-Ukraine messaging** – Disinformation campaigns portray Ukraine as corrupt or collapsing, while framing Ukrainian refugees as an economic or security burden, aiming to erode Czech support for Kyiv.
- **Anti-EU narratives** – Eurosceptic outlets and actors amplify claims of "Brussels dictatorship" and opposition to the Green Deal, presenting the EU as undermining Czech sovereignty.

10.2.3 Physical & Digital Threats to Election Stakeholders

- **Incidents between supporters of different political parties** - Several confrontations have already occurred, so far *limited* to verbal exchanges. However, as the electoral campaign intensifies, such incidents may escalate into physical violence.
- **Demonstrations as potential moments of crisis** - Several political *parties* and *actors* already announced large rallies in Prague shortly before election day. If not properly managed, these events might escalate into violent incidents.

10.2.4 Low Digital Literacy & Increased Vulnerability

- **Susceptibility to disinformation** – Segments of the population with low digital literacy struggle to distinguish credible information from manipulated or AI generated content, making them prime targets for influence operations.
- **Limited resilience to emerging threats** – Low awareness of online manipulation techniques reduces citizens' ability to critically assess deepfakes, false narratives, or coordinated campaigns, increasing overall societal vulnerability during elections.

11. Priority Intelligence Requirements (PIRs)

11.1 PIR 1: Which FIMI narratives pose the greatest threat to electoral legitimacy?

- **Allegations of election fraud and manipulation of results** — Surveys *show* that 39% of Czechs fear Russian interference, 78% worry about false information on social media, 60% are concerned about postal voting fraud, and 54% suspect government manipulation. (Czech Ministry of the Interior, 2025 – internal data)
- **False claims and impersonations targeting leaders** — Fabricated posts on Facebook and Telegram *suggested* President Petr Pavel planned to cancel elections or rig results, with violent threats circulating online. Former President Miloš Zeman *warned* that the Constitutional Court and BIS might invalidate results, while STAČILO! Party's Michal Klusáček even *called* for "resistance" if elections were "stolen".
- **Smear attacks on security institutions** — Outlets like neČT24 and Aeronet *spread claims* that the Czech Armed Forces' simulations of influence operations were proof of MI6 interference.
- **Anti-Ukraine narratives** — Outlets including pravda-cz.com, cz24.news, and pravdive.eu amplify narratives portraying Ukraine as corrupt, failing, and unworthy of Czech support. A CEDMO survey found 21% of Czechs were exposed to the *false claim* that the 2023 Prague shooter was Ukrainian. Refugees are depicted as threats to jobs and security, while the Czech government is framed as "traitorous" for prioritising Ukraine.
- **Anti-EU narratives** — The narrative of an "EU dictatorship" *resonates* among 54% of Czechs, often linked to policy debates such as the revision of the EU Emissions Trading System, which is framed as a misguided step harming ordinary citizens.

11.2 PIR 2: What TTPs are being used in influence operations targeting elections?

- **Use of Telegram ecosystems** — Channels such as neČT24, Maršál Malinovskij, and Selský rozum circulate hoaxes, repost content from Russian and problematic Czech outlets, creating echo chambers beyond mainstream regulation.

- **AI-generated fabrications** — Deepfake videos and synthetic audio of President Petr Pavel in early 2025 fabricated statements, including alleged plans to cancel elections or give citizenship to refugees.
- **Coordinated inauthentic behaviour (CIB)** — Bot networks amplify narratives across Telegram, Facebook, and problematic outlets, with rapid reposting patterns resembling operations linked to the Pravda Network.
- **Covert financing and proxy networks** — The Prague-based Voice of Europe platform was exposed as a Kremlin proxy, used to channel funds to politicians in several EU countries (e.g., Germany, France, Poland, Hungary) ahead of the European Parliament elections.
- **Cyber-enabled influence operations** — Pro-Kremlin outlets framed leaked Czech Armed Forces cyber exercise documents as "proof" of MI6 interference, while previous years saw DDoS and hack-and-leak operations *targeting* Czech institutions during politically sensitive periods.

11.3 PIR 3: How can AI-based threat detection enhance early warning systems?

- **Automated detection of deepfakes** — AI tools that can flag manipulated audio or video before wide dissemination, though human verification remains *necessary*.
- Early warning on polarising narratives — AI monitoring can alert institutions factcheckers when manipulated information spikes online, enabling faster responses.
- **Fact-checking automation** — AI can help scan online content and political ads for false claims, supporting *projects* that monitor political advertising.

11.4 PIR 4: What legal and policy mechanisms can reinforce election resilience?

- **Full implementation of the DSA** — Transpose DSA provisions into Czech law with strong oversight and adequate funding for election security.
- **Regulation of third-party political advertising** — Introduce clear rules on third party campaigning and financial transparency to prevent foreign-linked or unregistered groups bypassing campaign finance law.

- **Crisis communication and institutional coordination** — Establish a framework for timely, transparent public communication on election threats, and formalise inter-agency structures with clear mandates.
- **Platform cooperation and Telegram monitoring** — Mandate structured cooperation with online platforms, including transparency reports and rapid removal channels, with particular focus on cross-border Telegram clusters.
- **Addressing online political violence** — Update legislation to explicitly cover gendered harassment, information pollution, and deepfakes as political offences, ensuring better protection for candidates and public figures.

12. Conclusion

In previous Czech elections, the integrity of the process was occasionally questioned ex post in relation to technical errors (such as mistakes during the counting of votes) or the impact of disinformation on voter decisions. These complaints were mostly raised by individuals and were evaluated by the courts as not sufficiently relevant to discredit the electoral process. Public trust in elections remained high and was not significantly influenced by these isolated incidents.

The parliamentary elections of 2025 could represent a significant departure from this situation. During the debate about postal voting, concerns were raised that this new measure could create opportunities for electoral fraud. In the context of the annulled presidential elections in Romania at the end of 2024, some voices suggested that Czech courts, intelligence services, or even the President might challenge the electoral results to keep the current government in power.

Another potentially harmful narrative that could be exacerbated by FIMI relates to the Ukrainian minority and refugees living in Czechia. This issue is already being exploited by various actors, who portray Ukrainian refugees as a burden on the social system and a threat to public safety. Such rhetoric frequently relies on hoaxes and misleading information. The continued spread of these narratives could provoke violent incidents and escalate into serious interethnic clashes.

The Czech electoral system is resilient to manipulation due to its decentralised structure, transparent vote-counting process, and reliance on paper ballots. Moreover, postal voting has proved to be less popular than anticipated. Consequently, the scope for undermining electoral integrity remains relatively narrow.

Resilience to FIMI during the electoral process is a more complex issue. While state institutions are capable of monitoring developments in the information space, their ability to respond is constrained by the absence of a comprehensive legislative framework— particularly the lack of national implementation of the Digital Services Act— and by political sensitivities. As a result, it is likely that state authorities will adopt a cautious approach to any potential FIMI incidents.

Nonetheless, opportunities exist to strengthen this capacity through EU-level resources, such as the DG CONNECT DSA team and the Rapid Alert System, which can help improve situational awareness and coordination.

The long-term efforts of malign actors – Russia in particular – have led to the establishment of multiple potential vectors for spreading FIMI across various segments of the Czech information space. At the same time, these efforts have prompted a counter-reaction from civil society, fact-checkers, and the media, who monitor developments, identify disinformation, and raise public awareness. Facilitating information exchange among these actors could enhance their collective ability to detect and respond to FIMI in a timely manner.

Overall, while Czechia possesses a robust electoral infrastructure and a high level of awareness of threats, mitigating these risks requires urgent investment in institutional capacity, legal frameworks, and trust-building measures. Without such efforts, vulnerabilities in campaign financing, information resilience, and institutional independence may be exploited to weaken public confidence in democratic processes.

Annex 1: DISARM TTPs Observed in Czechia

DISARM Technique (Code)	Example in Czechia	Objective
Leverage Existing Narratives (T0003)	Anti-EU, anti-Ukraine, antimigrant frames	Exploit existing grievances; erode trust in EU/NATO solidarity
Leverage Conspiracy Theory Narratives (T0022) / Amplify Existing Conspiracy Theory Narratives (T0022.001)	Aeronet tying elections to MI6; "deep state" fraud claims	Undermine confidence in democratic processes
Develop Competing Narratives (T0004)	Conflicting accounts of military document leak	Create confusion; delegitimise institutions
Establish Inauthentic News Sites (T0098)	neČT24, 42TČen as Sputnik successors	Maintain pro-Kremlin media presence despite bans
Impersonate Existing Official (T0099.003)	Fake quote attributed to Senator Němcová	Discredit officials; sow discord internationally
Use Pseudonyms (T0128.002)	"Jiří Novák" persona relaying Sputnik editor content	Preserve editorial influence while concealing identity
Develop AI-Generated Audio (T0072.001)	Deepfaked voice of President Petr Pavel	Discredit leadership; fabricate "evidence"
Obtain Private Documents (T0074)	Armed Forces exercise documents leaked	Delegitimise state agencies; frame as unlawful surveillance
Distort Facts (T0023) / Reframe Context (T0024)	Aeronet framing PM Fiala's MI6 visit as election meddling	Paint government as foreign puppet; erode legitimacy
Traditional Media (T0111)	CGTN, China Radio International content in Czech outlets	Normalise PRC positions; extend reach to wider public
Deliver Ads (T0114)	Paid placements on Czech social media platforms	Amplify narratives through targeted reach
Cross-Posting (T0119) / Post across Platform (T0119.002)	Telegram ecosystems sharing content across groups	Broaden visibility; sustain message circulation

DISARM Technique (Code)	Example in Czechia	Objective
Bypass Content Blocking (T0121.001)/ Direct Users to Alternative Platforms	Redirect from Sputnik to neČT24 post-ban	Circumvent EU sanctions and moderation
Manipulate Platform Algorithm (T0121)	Pravda network scraping/reposting Czech content	Force visibility; shape online discourse
Generate Information Pollution (T0124)	Pravda CZ posting >186k articles in months	Drown out factual information; overwhelm LLMs/media
Encourage Physical Violence (T0127)	Calls to harm President Pavel	Intimidate leaders; normalise violent rhetoric
Call to Action to Attend (T0126.002)	Anti-government protests in Prague (2022 onwards)	Translate online mobilisation into offline presence
Conceal Sponsorship (T0130.001)/ Use Shell Organisations (T0130.003)	Voice of Europe operations in Prague	Hide Kremlin funding of media influence
Use Cryptocurrency (T0130.004)/ Obfuscate Payment (T0130.005)	Natalia Sudliankova receiving crypto under GRU direction	Mask financial flows for covert operations
Co-Opt Influencers (T0100)/ Trusted Individuals (T0101)	EU politicians recruited via Voice of Europe	Legitimate narratives through elite endorsement
Recruit Malign Actors (T0136)	Telegram agents; local operatives linked to GRU	Build durable local networks for influence
Coordinate on Encrypted/ Closed Networks	Telegram clusters replacing mainstream platforms	Maintain resilience; evade monitoring
Attract Traditional Media (T0117)	Hoaxes and fake quotes picked up by the Czech press	Expand reach through mainstream legitimisation

Table 6: 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

FIMI RESPONSE TEAM REPORT

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