FIMI -ISAC

FDEI PROJECT

ELECTION REPORT

Assessment of Foreign Information Manipulation and Interference in the 2025 Polish Presidential Election

Alliance 4Europe · Debunk.org Disinformation analysis center · GLOBSEC IDEAS SHAPING THE WORLD · EU DisinfoLab · DFRLab · ISD Institute for Strategic Dialogue

FIMI -ISAC

FDEI PROJECT

ELECTION REPORT

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

Authors & Partner Organizations

Alliance4Europe, Debunk.org, GLOBSEC, EU DisinfoLab, DFRLab, Institute for Strategic Dialogue (ISD)

Contributing Organisations and Networks:

INFO OPS Poland Foundation, Demagog Association Poland, CEE Digital Democracy Watch, Political Accountability Foundation, The Counter Disinformation Network, University of Amsterdam, DRI, The Global Security Initiative.

Additional thanks go to our partners and experts Kamila Korónska (University of Amsterdam), Jakub Szumik (CEE Digital Democracy Watch, Martyna Hoffman (Political Accountability Foundation), Aleksandra Wojtowicz (Independent Researcher), Milosz Dzienio (Independent Researcher), INFO OPS Poland Researchers, Duncan Allen (Democracy Reporting International, Wojciech Solak (Independent Researcher), Shiva Shah (The Global Security Initiative), Zachary Horsington (The Global Security Initiative) for their valuable contributions to this report.

About the Project

This report evaluates Foreign Information Manipulation and Interference (FIMI) threats to the 2025 Polish presidential elections. It was developed through the FIMI-ISAC project 'FIMI Defenders for Election Integrity'. This project consortium brings together FIMI-ISAC members with the unparalleled expertise of 10 organisations to develop a multistakeholder FIMI framework for elections to effectively monitor, respond to and counter FIMI threats before and during elections, while at the same time strengthening FIMI defender communities and democratic institutions.

This monitoring and response also involved engaging and coordinating with 10 in-country partners from across Polish civil society and academia.

Over the course of these monitoring efforts, the consortium produced a series of incident alerts to be circulated to relevant election stakeholders in real-time. These incident alerts detail key information about FIMI incidents and their impact in the country of focus and provide a set of recommendations for response. Where insights derived from these incident alerts are mentioned throughout this report, they are signposted with an alphanumeric code beginning with 'IA'.

About the FIMI-ISAC

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

https://fimi-isac.org/

Infrastructure:

This report and project were facilitated through the Counter Disinformation Network. The CDN is a collaboration and crisis response platform, knowledge valorisation resource, and expert *network.*

Table of Contents

List of Tables and Figures:

Executive Summary

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

Our findings, drawn from the collective monitoring and response effort of 28 organisations and the generation of 20 incident alerts[1], highlight the persistent and multifaceted information threat facing the Polish presidential elections.

A recurring strategic narrative consistently emerged during the election period, portraying EU countries and Ukraine negatively, often accusing them of harming Poland and attempting to manipulate its elections.[2] This narrative strategically positioned far-right Polish politicians as defenders of national sovereignty against perceived external influence.

Key influence information operations targeting the elections included the Doppelganger operation, Operation Overload, and the Pravda Network, all of which disseminated such misleading narratives. Radio Belarus, a sanctioned Belarusian state media, also actively interfered by amplifying ideologically-aligned candidates. Lega Artis, Citizen GO, Ordo Iuris, and other foreign aligned actors were also found to have amplified polarising narratives and promoted candidates that aligned with their interests.

These influence operations manipulated public opinion, often via the use of fabricated online personas and coordinated inauthentic behaviour. They exploited several vulnerabilities in social media platforms, which could be seen as potential systemic risks as defined by the Digital Services Act (DSA). These include the ease of creating accounts on X, the lack of advertisement 'Know Your Customer' (KYC) principles on Meta, and inconsistent policy and moderation of murky accounts conducting political campaigns on TikTok.

Finally, the Polish threat landscape was remarkably consistent across the 2017, 2021, and 2025 election campaigns. This presents a notable contrast to other contexts where the threat landscape has exhibited a more dynamic or novel evolution of tactics, while in Poland such tactics have been a persistent issue for some time.

[1] Incident alerts are standardised summary of an information manipulation incident or influence operation, initially developed by the Counter Disinformation Network to effectively analyse and respond to ongoing information threats.
[2] https://fimi-isac.org/wp-content/uploads/2025/05/POLISH-CERA.pdf

Beyond detailing tactics employed by FIMI actors, this report exposes the **concerning adoption of similar manipulative tools by domestic actors to gain political leverage.** Critically, it also highlights that despite interventions from civil society, regulators, and platforms, significant **deficiencies in policy enforcement and platform accountability persist.** The report concludes with recommendations on improving civil society engagement to counter future FIMI threats.

While the Polish elections were targeted by foreign influence operations, and suffered information manipulation incidents, analysis shows that their impact seems to have been constrained by several factors, including public resilience, active civil society responses, and the limited operational sophistication of some campaigns. However, in an increasingly polarised information ecosystem where electoral outcomes can be razor-thin, the imperative for robust national resilience against such threats remains paramount.

This approach acknowledges that resilience is not solely the responsibility of governments or platforms, but requires the active, coordinated participation of all societal sectors - including civil society, media, academia, the private sector, and individual citizens. Consequently, the need for continuous work to foster a whole-of-society resilience against FIMI is compounded.

Key Findings

1. **Persistent incentives and vulnerabilities: the FIMI landscape is shaped by:**

   a. Poland's geopolitical stance against Russia, making it a prime target for destabilisation.
   b. Exploitation of public support for Ukraine and its refugees to sow internal division.
   c. Weaponisation of the Belarusian border crisis to amplify migration tensions and political pressure.
   d. Leveraging domestic economic uncertainty and inflation to erode public trust in governance.
   e. Deep-seated domestic political polarisation, providing fertile ground for divisive narratives.
   f. Existing EU scepticism within segments of Polish society, targeted to undermine European integration.
   g. Critical absence of a permanent Digital Services Coordinator, creating a regulatory vacuum.

2. High-Impact Narrative Amplification:

a. Anti-Ukrainian narratives aim to degrade public support for Ukraine in the context of Russia's invasion and Ukrainian refugees' influx, fostering social fragmentation.
b. Anti-EU narratives seek to erode trust in European institutions and Polish membership, threatening foreign policy cohesion.
c. Anti-Establishment narratives are designed to delegitimise democratic governance, including the incumbent government as well as public institutions, fostering political instability and public distrust.

3. Sophisticated FIMI Operations and information manipulation:

a. Coordinated operations - Doppelganger, Operation Overload, the Pravda Network, and the sanctioned Radio Belarus actively disseminated misleading narratives and amplified ideologically-aligned candidates.
b. Foreign aligned operations - Lega Artis, Citizen GO, and Ordo Iuris further amplified polarising content.
c. Unattributed or unaffiliated operations such as covert ad-campaigns (unaffiliated), a coordinated inauthentic behaviour network seemingly manipulating TikTok's algorithm (unattributed), a Nigerian clickbait website (unaffiliated), and murky accounts[3] were also observed engaging in information manipulation. Their objectives included promoting specific candidates, demoting oppositional candidates, and increasing political polarisation.

4. Unfair Political Actor Conduct[4]: domestic political figures, particularly from the far-right and conservative-nationalist spectrum, were significantly associated with information manipulation. This included the fabrication of personas for self-promotion, the involvement of pro-Russian domestic actors, and the dissemination of false information about election procedures.

5. Exploited Systemic Platform Risks:

a. X (formerly Twitter) lacks adequate checks on account creation, enabling largescale coordinated inauthentic behaviour networks.
b. Meta demonstrates weak 'Know Your Customer' (KYC) checks in its ad system.

[3] TikTok accounts that appear to violate the platform's impersonation policy.
[4] EDMO's election risk assessment matrix defines unfair political actor conduct as "the risk that politicians or other political actors use hate speech or spread mis/disinformation through mainstream channels with large dissemination of stories and claims". See: https://edmo.eu/wp-content/uploads/2024/06/Preliminary-Risk-Assessment-Report.pdf

c. TikTok exhibits weak and inconsistent enforcement of its political campaigning policy, allowing circumvention, impersonation, and deceptive campaigns.

Policy Implications and Recommendations

The elections revealed a troubling discrepancy between identified FIMI threats and the adequacy of institutional and platform responses. Bridging this enforcement lag requires immediate and sustained policy action. Only through sustained engagement, robust institutional frameworks, and an empowered, collaborative civil society can Poland effectively safeguard its democratic processes from evolving digital threats and ensure the integrity of its information environment.

1. Strengthen institutional oversight:

a. Establish a permanent and well-resourced Digital Services Coordinator (DSC) for Poland: this is paramount for ensuring effective DSA implementation, robust oversight of platforms, and seamless cross-sector coordination in threat response.
b. Enhance inter-institutional and cross-sector coordination: develop a permanent incident escalation system to facilitate real-time communication and intervention between government agencies, civil society, and platforms, extending beyond electoral cycles. This includes support for and coordination of initiatives such as the Polish Resilience Council, the Central European Digital Media Observatory (CEDMO), and the FIMI Information Sharing and Analysis Centre (FIMI-ISAC).

2. Enforce platform accountability and transparency:

a. Mandate robust systemic risk mitigation: hold platforms strictly accountable for assessing and mitigating systemic risks (DSA Articles 34 & 35) to prevent interference.
b. Ensure ad transparency and verification: compel platforms to implement stringent advertiser identity verification (KYC) and immediately halt revenue streams to malign actors (per DSA Article 26 and Political Advertising Regulation).
c. Address platform vulnerabilities: mandate that platforms patch vulnerabilities like easy account creation for throw-away profiles and ensure consistent enforcement of political campaigning policies, with punitive measures for non-compliance.
d. Strengthen researcher data access: fully enforce DSA Article 40 to ensure transparent rigorous data access for researchers, to analyse algorithm behaviours and content virality.

3. Build national resilience:

a. Invest in comprehensive media and digital literacy: implement targeted, age-appropriate programmes to equip Polish citizens with critical thinking skills, fostering informed media consumption and addressing distrust in public institutions.
b. Sustain civil society funding: provide stable, long-term funding mechanisms for Polish civil society organisations to build capacity and institutional knowledge, ensuring their continued ability to counter systemic threats beyond electoral cycles.
c. Implement targeted accountability for domestic FIMI amplifiers: develop mechanisms for public attribution and other targeted responses to address domestic figures who knowingly disseminate or echo manipulative narratives, clarifying the line between legitimate political discourse and deliberate deception.

Introduction

The 2025 Polish presidential elections took place against a backdrop marked by Russia's ongoing war of aggression against Ukraine, Trump's recent re-election and rising populist sentiment in Europe, all factors contributing to political instability. Poland's historical and geopolitical context places the country at the crossroads of competing great powers, setting the stage for foreign interference.

The presidential election concluded with the closest results in the nation's post-communist history, as conservative candidate Karol Nawrocki secured a narrow victory margin of less than *one percentage point*. Characterised by *high polarisation* and candidates offering radically divergent visions for Poland's future, the election campaign unfolded amidst persistent challenges to information integrity, as both foreign and domestic actors sought to manipulate the outcome through various influence operations.

Focused primarily on FIMI, this report assesses the key risks that characterised the 2025 Polish presidential elections. It examines the incentives, vulnerabilities, and mechanisms behind influence operations, as well as the role of digital platforms in disseminating misleading narratives. It outlines the observed coordinated operations that were active during the election period, such as Doppelganger, Operation Overload, and Pravda Network, shedding light on their structure and impact. The report also discusses how sanctioned Russian and Belarusian media outlets attempt to circumvent sanctions to make their content available to Polish audiences. The intricate dynamics of this critical electoral period are thoroughly examined, spotlighting prevalent disinformation narratives concerning Ukraine, national security, economic instability, and democratic legitimacy.

It further analyses the sophisticated techniques used for their amplification, including the use of AI-generated content, coordinated inauthentic behaviour networks, and both covert and overt influence operations on social media platforms and websites. Additionally, the report provides insights into instances of unfair conduct by domestic actors and assesses the broader impact of influence operations. It also reviews the interventions and responses implemented during the election period.

The analysis presented in this report is largely drawn from ***20 incident alerts*** compiled during the monitoring period between April and June 2025. These alerts capture and summarise instances of information manipulation and influence operations.[5] While influence operations represent continuous, strategic efforts by actors to manipulate

[5] Incident alerts are standardised summary of an information manipulation incident or influence operation, initially developed by the CDN to effectively analyse and respond to ongoing information threats.

audiences, and can encompass numerous information manipulation cases, it is important to note that information manipulation itself can also occur ad-hoc, often opportunistically, and not always as part of a larger, scheduled campaign. The table presented below, adapted from EDMO's election risk assessment methodology, provides a detailed overview of specific risks identified during the election monitoring period, *assessing their likelihood pre-election* and the actual activity observed post-election.

- **Specific Risk:** This column lists various categories of potential threats or challenges to election integrity and the democratic process.
- **Risk Level:** This indicates the inherent severity or potential impact of each specific risk, categorised as High, Medium, or Low.
- **Pre-Election (Assessment of Likelihood):** This column reflects the estimated probability of each risk occurring before the election, categorised as High, Medium, or Low[6].
- **Post-Election (Activity Observed):** This column indicates the actual level of activity or manifestation of each risk that was observed during and after the election, again categorised as High, Medium, or Low.

Specific RIsk	Risk Level	Pre-Election: Assessment of Likelihood	Post-Election: Sctivity Observed
Cyber threats and technological infrastructure	High	Medium	Low
AI-generated disinformation	Medium	High	Medium
Unfair conduct by political actors	Medium	High	Medium
FIMI Narratives	Medium	High	High
Institutional Trust Erosion	High	Medium	Medium
Physical threats to candidates, campaign teams, and others	High	Low	Low

Table 1: Key risks, pre-election assessment of likelihood and activity observed

Our analysis, informed by the structured risk assessment detailed in the table, reveals several critical insights regarding the challenges faced during the election.

[6] The 2025 presidential election Polish Country Risk Assessment (CERA) evaluated these risks prior to the elections based on the national context of Poland, previous election campaigns, and information manipulation incidents.

As this report demonstrates, the 2025 Polish elections were subjected to numerous influence attempts, many of which mirrored patterns observed during previous major electoral events across Europe. The mechanisms developed over time to detect, analyse, and resist disinformation - including rapid response teams, established civil society networks, collaborative media engagement, and direct platform reporting pathways - proved instrumental in preventing more severe effects on the integrity of the Polish vote. These mechanisms, operating through coordinated efforts between experts, civil society organisations, journalists, and sometimes with public authorities, allowed for swifter debunking, targeted flagging of malign infrastructure, and enhanced public awareness, thereby limiting the reach and impact of harmful narratives. The success of these operational responses underlines a critical insight: **for truly effective and enduring defence against sophisticated information manipulation, these response mechanisms must be seamlessly integrated and extended within a comprehensive whole-ofsociety approach.**

Despite the anticipated likelihood of **cyber threats** based on previous elections, the 2025 Polish presidential election did not experience any incidents that materially compromised the integrity or broad functionality of the electoral process, primarily due to the effective containment and swift reporting of even impactful events. This is likely attributable to the valuable lessons learned from previous election cycles and the proactive "Election Umbrella" initiative spearheaded by Polish authorities.

As anticipated, **FIMI narratives** already prevalent within Polish public discourse intensified and spread widely throughout the election period.

Despite expectations that reports of **unfair conduct by political** actors would involve increasingly complex influence operations, the observed patterns of behaviour remained consistent with those from previous elections. This consistency, however, may be partially attributed to a limited scope of investigations into purely domestic operations.

Lastly, despite one demonstration resulting in violence and a few minor incidents, **no meaningful physical threats to candidates, campaign teams, or other relevant actors** were recorded, aligning with prior expectations.

Finally, this report further demonstrates **a remarkably limited evolution in the Polish threat landscape across the 2017, 2021, and 2025 election campaigns.** This presents a notable contrast to other contexts, such as the 2025 German elections where **AI-generated disinformation** emerged as a novel concern. In Poland, such tactics have been a persistent issue. The report details the consistent Tactics, Techniques and Procedures (TTPs) primarily employed by Russian and Belarusian FIMI actors, underscoring their persistent geopolitical interest in influencing Polish elections. Contrary to expectations, a significant increase in the use or complexity of these TTPs were not observed.

However, a key focus is the pronounced shift in narratives since 2022, which now increasingly target Ukrainian refugees in Poland with the aim of undermining the vital Polish-Ukrainian relationship.

1. Incentives & Enablers of FIMI

Foreign actors are significantly incentivised to conduct FIMI in Poland due to a confluence of factors: its critical geopolitical position as a frontline state and gateway to Eastern Europe, its robust and unwavering support for Ukraine, and critically, its complex and evolving relationship with the European Union. This relationship is complicated by ongoing domestic political debates that balance national sovereignty with deeper EU integration, and by recent high-profile disputes with Brussels over issues such as the rule of law and judicial reforms. This dynamic interplay of cooperation and contention creates fertile ground for foreign interference, as external actors seek to exploit existing divisions and shape public opinion regarding Poland's place within the EU and its broader international alliances (NATO), ultimately aiming to weaken both internal cohesion and external partnerships.

1.1 Geopolitics

Poland maintains a longstanding, robust opposition to Russia's imperialist ambitions and has consistently stood by Ukraine as a key ally. This firm geopolitical stance makes it a primary target for Russian interests, which actively seek to weaken Poland's internal cohesion and sever its international alliances.[7]

As a result, the Russian government has sought to foster *division* and polarisation in Poland in *recent years*, and has a strong incentive to bolster pro-Kremlin political forces and amplify divisive narratives. The Kremlin seems to have deployed a large arsenal of strategies, stemming from *hybrid attacks* to *online influence operations*. Although sanctions have somewhat curtailed Russia's ability to exert overt influence in Europe, there is substantial evidence that the Kremlin has dedicated significant resources to circumventing these restrictions and establishing infrastructure for covert influence operations.[8]

[7] On how Poland has become a primary target for Russian subterfuge, see: The Jamestown Foundation. (2025, May 8). Poland on the Frontlines Against Russia's Shadow War. *https://jamestown.org/program/poland-on-the-frontlines-against-russias-shadow-war/*.

[8] On circumventing sanctions and establishing infrastructure for covert influence operations, see: Center for Strategic and International Studies (CSIS). (2025, March 18). Russia's Shadow War Against the West. *https://www.csis.org/analysis/russias-shadow-war-againstwest*; Institute for Strategic Dialogue. (2025, May 13). Investigation: How Russia Today is evading sanctions and spreading pro-Kremlin propaganda in Italy. *https://www.isdglobal.org/digital_dispatches/investigation-how-russia-today-is-evading-sanctions-and-spreading-pro-kremlinpropaganda-in-italy/*

A critical avenue for this destabilisation has been the issue of Ukrainian refugees: Poland has welcomed a significant number of refugees and provided substantial humanitarian support. Concurrently, however, Poland has become heavily targeted by Russian influence operations explicitly designed to demonise Ukrainian *refugees.*

This external pressure has found fertile ground in domestic politics, as the topic of Ukrainian refugees has been highly politicised by centrist and right-wing *parties*, leading to increased attacks against Ukrainians, *protests*, and legislative changes to limit their *social security benefits.*

Moreover, the Belarusian border crisis, characterised by the Belarusian state's use of refugees from the MENA region as a tool of *hybrid warfare* to destabilise Polish society, has further escalated tensions and led to sterner border security *measures*.

The Polish elections are also set against a backdrop of economic uncertainty, including inflation and ongoing conflicts in Ukraine and the Middle East. These factors have left segments of the electorate particularly vulnerable to information manipulation and propaganda related to economic conditions, immigration, and geopolitical issues. Some influence operations strategically target economic anxieties, notably by linking inflation to Western sanctions in an effort to manipulate public sentiment. FIMI operations extend beyond merely discussing economic and financial issues; foreign actors actively deploy financial incentives to further their propaganda efforts.

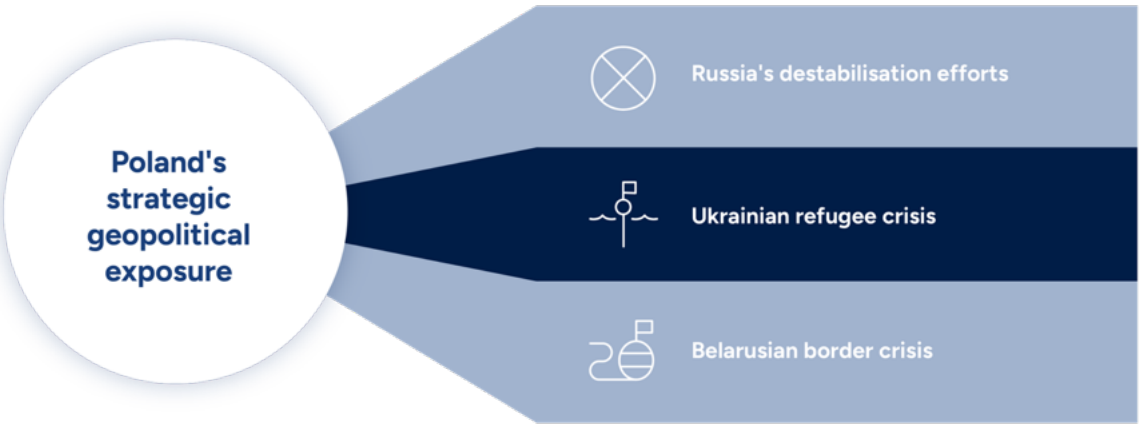

Figure 1: Poland's Strategic Geopolitical Exposure

1.2 Domestic Polarisation

Going into the election period, Poland faced a challenging domestic environment marked by high *inflation*, a *fragile* government coalition, and a highly *polarised* society. **These internal vulnerabilities collectively created fertile ground for information manipulation by foreign actors seeking to destabilise democratic processes and institutions.** The previous government's actions severely undermined the rule of law, resulting in a significant decline in public trust in the *judiciary*. While the new government has actively sought to restore the rule of law, its efforts have been significantly hindered by an ideologically oppositional president, who has repeatedly exercised veto *power* against government initiatives.

EU scepticism in Poland has been on the rise, a trend starkly illustrated by a 2024 poll published on the occasion of the country's *20th anniversary of EU membership*. The survey revealed the lowest level of support for the country's presence in the EU in over a decade. Within a highly polarised domestic environment, this growing scepticism presented a significant risk to the 2025 presidential election. **It deepens existing societal divisions, creating fertile ground for political actors to exploit anti-EU sentiment for electoral gain.** Furthermore, this increase in scepticism offers foreign influence operations a powerful vector to exacerbate internal discord, undermine pro-European voices, and ultimately weaken Poland's position both internally and within the broader European Union.

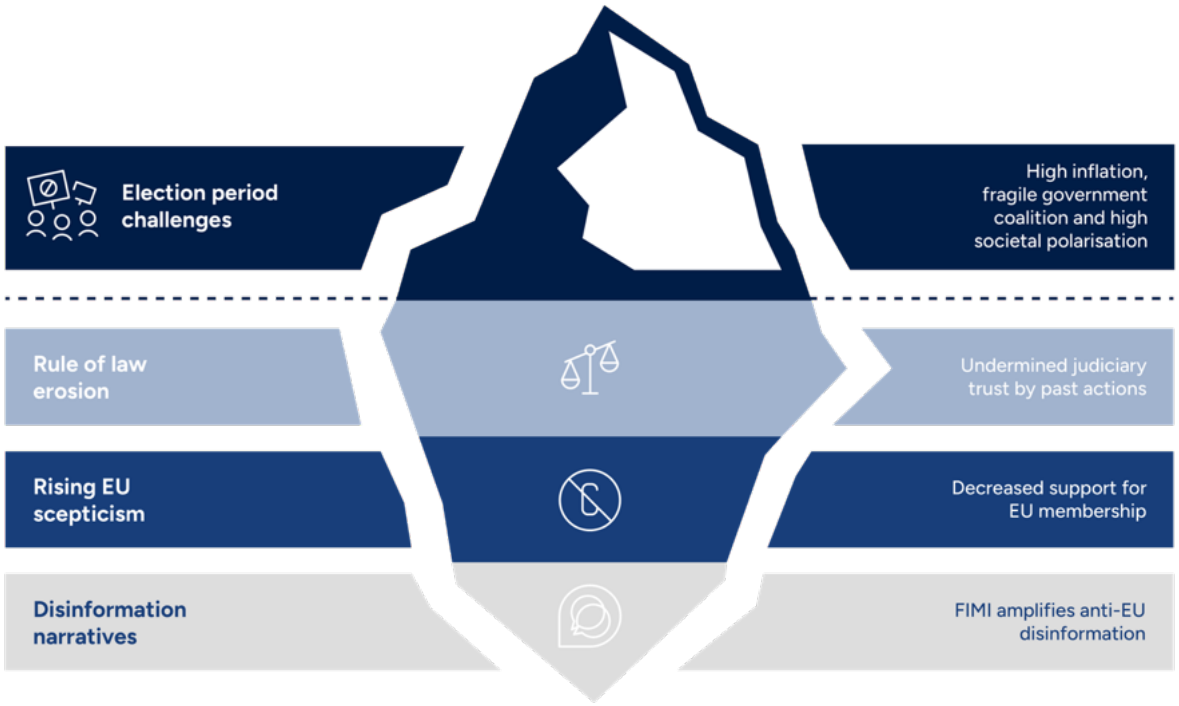

Figure 2: Poland's Challenging Domestic Environment

This trend of rising EU scepticism is directly paralleled by a surge in disinformation narratives targeting the European Union that are being amplified by FIMI actors. Such narratives aim to fuel economic anxieties, societal polarisation, and national identity concerns, frequently portraying the EU as an existential threat to Polish sovereignty. Current operations, such as *the Doppelganger campaign on X*, have intensified these messages ahead of the elections, specifically focusing on fostering anti-EU sentiment, criticising climate policies, and advocating for greater national self-sufficiency in key policy areas such as energy and agriculture.

1.3 Legal Vulnerabilities

Poland lacks a designated Digital Service Coordinator (DSC) and does not have national media laws in place, both of which are factors that limit the government's ability to respond effectively to information threats[9] and to coordinate across government institutions and civil society[10].

The DSA is necessary to ensure that actions can be taken while respecting democratic freedoms. Implementing such regulations in a fast, reliable, and democratic manner poses a challenging balance.[11] The Office of Electronic Communications (*UKE*), with the support of the Office of Competition and Consumer Protection (*UOKiK*), are the institutions most likely to implement the DSA in Poland, although they do not have *the required personnel* yet.

While the DSA has not been implemented in Poland, the country has a robust regulatory framework against FIMI. Articles 117, 130, and 256 of the Polish Criminal Code allow Polish authorities to prosecute individuals on the basis of publicly inciting a war of aggression, promoting fascism and inciting hatred against specific groups, and working with foreign intelligence services.

Finally, there is also a law on 'Special Solutions to Counteract Supporting Aggression against Ukraine and to Protect National Security' which prohibits the use of symbols or names that support the Russian invasion of *Ukraine*.

[9] Interview conducted with NASK in March 2025.
[10] Interview conducted with Aleksy Szymkiewicz from the Demagog Association in March 2025.
[11] Interview conducted with NASK in March 2025.

1.4 Target Demographics

In Poland, influence operations strategically target specific demographic vulnerabilities, primarily focusing on the *youngest age groups* and *senior citizens*. *Young people*, heavily reliant on social media platforms for their news, are more susceptible to disinformation due to the rapid spread of unverified content within algorithmic echo chambers and their increased likelihood of engaging with alternative information ecosystems that often lack traditional journalistic scrutiny. **Their digital native status does not inherently equip them with the critical thinking skills needed to navigate the complex and often deceptive online information landscape.**

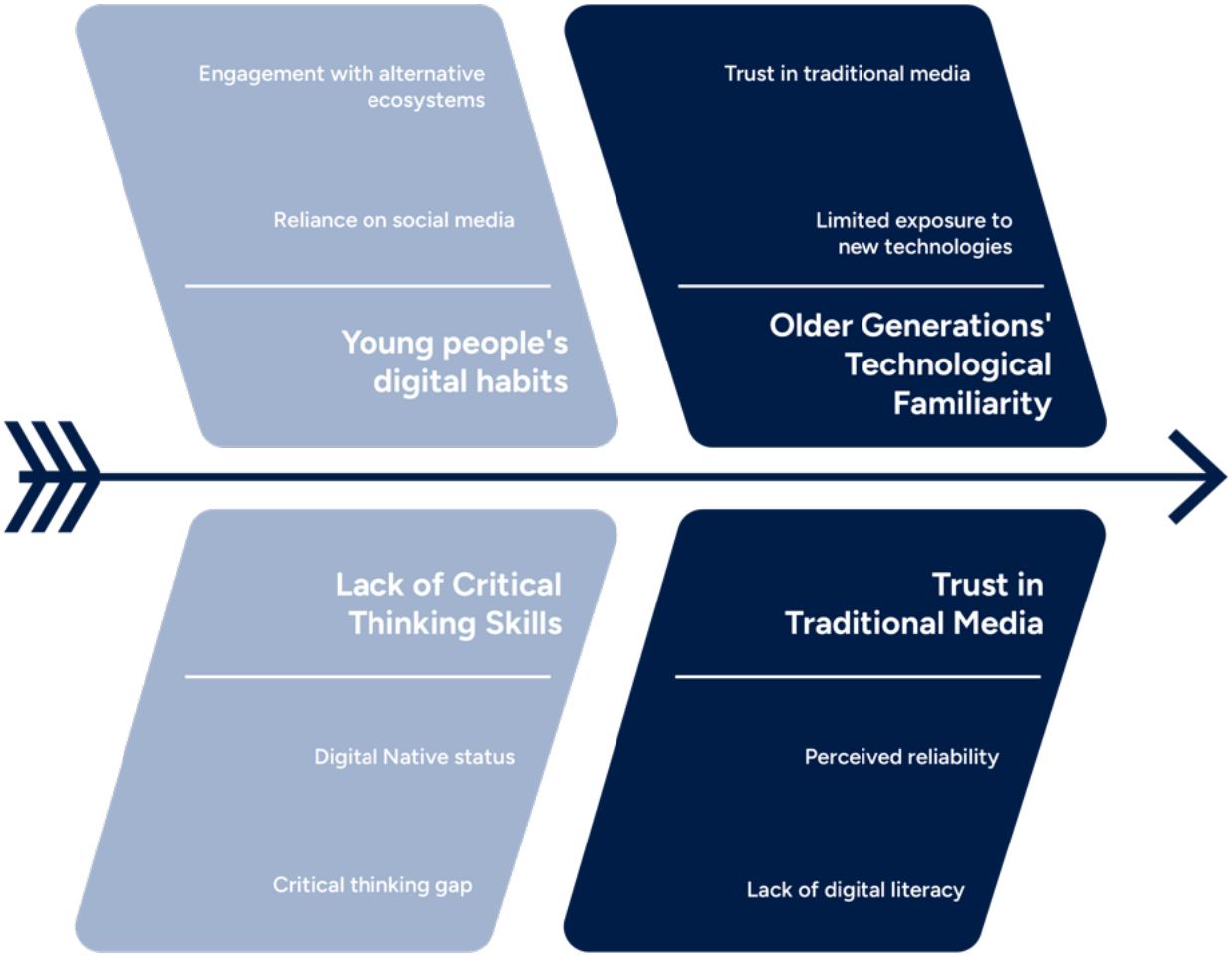

Figure 3: Demographic Vulnerabilities to Disinformation in Poland

Conversely, older generations face distinct vulnerabilities rooted in their less frequent exposure to and lack of familiarity with new digital *technologies*. Advanced tools like AI-generated content remain a novel and often bewildering phenomenon for them, making it difficult to recognise its deceptive potential. Moreover, having been socialised in a media environment that deeply valued the authority of traditional media and emphasised implicit trust in institutional sources, information appearing in newspapers or broadcast on television was generally perceived as inherently verified and reliable. This ingrained trust can paradoxically make them more susceptible to sophisticated online manipulations that mimic traditional media formats, as they may lack the digital literacy to discern fabricated content from legitimate sources or to critically assess the authenticity of information presented in unfamiliar online environments.

1.5 Political Motives

In addition to geopolitical objectives, political motives are clearly evident in efforts to undermine trust in democratic institutions and strategically strengthen fringe candidates. This approach taps into existing societal vulnerabilities where public trust in established political systems may already be wavering, making populations more susceptible to narratives of institutional illegitimacy or radical political alternatives.

A glaring example of this strategy is how the Belarusian state-controlled and EU-sanctioned media, Radio Belarus, actively promoted pro-Russian presidential candidates Maciej Maciak, interviewing him seven times and explicitly calling on people to provide the 100,000 signatures needed for his *candidacy*.

Simultaneously, other Russia-aligned operations like Doppelganger were shown to target and disparage other established parties, further contributing to the erosion of trust in the broader political landscape.

As discussed in more depth below, this type of information manipulation can also, of course, be motivated by financial incentives, as disinformation campaigns can be monetised through increased traffic and engagement, benefiting affiliated networks.

1.6 Financial Incentives

In general, the way social media is structured financially incentivises actors to spread mis- and disinformation through the monetisation of engagement. This includes foreign-originated content and networks designed to amplify such content. Thus, actors not financed by foreign governments may still be financially motivated to conduct influence operations.

Figure 4: Financial Incentives and Content Origin in Disinformation Spread

2. Common FIMI narratives

During the monitoring of the 2025 Polish presidential election, recurring meta and sub-narratives were identified being promoted by FIMI actors.

Figure 5: Meta and Sub Narratives

2.1 Meta Narratives

Based on analysis of content spread by FIMI actors during both rounds of the Polish presidential elections, 10 meta-narratives emerge. These narratives target a wide range of topics and actors, including Ukraine, the EU, the collective West, and the Polish government. Across cases, however, content employs a largely uniform type of logic, presenting an image of an illegitimate or neglectful state. More specifically, these narratives

characterise Ukraine as a looming threat to regional stability, while simultaneously portraying Russia and Belarus as benevolent actors or even as victims of Western aggression. **This duality highlights how the fundamental role or distinction of victim versus aggressor is deliberately inverted and manipulated, extending far beyond mere political agenda. Instead, it serves as a core tenet of hybrid warfare, strategically employed to muddy international waters, erode moral clarity, and cultivate a narrative framework that effectively normalises and justifies the aggressive political and military actions of Russia and Belarus in the region, ultimately aiming to garner public acceptance or at least passive resistance to counter-actions and further destabilise alliances.**

The most pertinent overarching/meta-narratives identified are as follows:

2.1.1 Anti-Ukraine

Narratives attacking Ukraine and Ukrainian refugees in Poland were by far the largest meta-narrative category observed during the Polish presidential election. As the largest meta-narrative, it is best analysed when broken down into three motifs (a recurring thematic element, image, idea, or narrative trope that contributes to the overarching message): **anti-refugee, threat, and symbolism.**

Motif 1 - Anti-Refugee

Accusations of Ukrainian refugees exploiting Polish and European aid systems for financial gain and constantly demanding additional support were a popular motif during the Polish election. The image below is an illustrative example of this narrative. Sourced from *a March 2025 Demagog report,* the image originally depicted a gathering of Ukrainian refugees expressing support for Ukraine. The visual was then deceptively repurposed to allegedly portray a rally of Ukrainians demanding more financial resources from the Polish government.

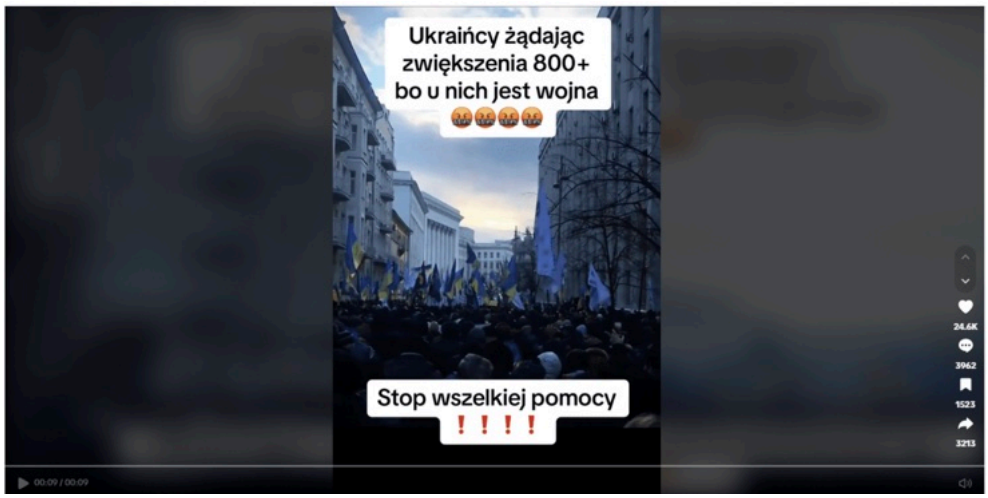

Figure 6: Repurposed Video: Ukrainians Accused of Demanding Money in Poland

Motif 2 - Threats to Poland

A prominent motif accused Ukrainian refugees and the Ukrainian government of *plotting terrorist attacks* in Poland, specifically targeting the election and voting systems. This narrative was strategically employed in an attempt to intimidate Polish citizens, discouraging participation in the voting process, while simultaneously aiming to erode public confidence in the integrity of the elections, thereby influencing voter turnout and shaping Poland's political landscape. Operations like Operation Overload widely disseminated these narratives via platforms such as X, as illustrated by the *post below*.

Figure 7: X post from Operation Overload alleging Ukrainians are a threat

Motif 3 - National Symbolism

Pro-Russian activists, including activist *Marcin Bustowski*, disseminated claims on platforms like X alleging that Polish courts supported the removal of foreign flags and symbols, with a particular emphasis on those representing Ukraine. This narrative focused on framing foreign symbols as undesirable and unlawfully displayed impositions on Polish territory that should be removed. *One example of the article created to advance this narrative is shown in the image below.*

Figure 8: Kremlin-aligned website alleging that Ukrainian flags should be removed from Polish land

In summary, narratives attacking Ukraine and Ukrainian refugees constituted one of the most prevalent meta-narrative categories observed during the Polish presidential election. Employing distinct angles such as fostering anti-refugee sentiments, portraying Ukraine as a direct security threat, and demonising Ukrainian symbols, these pervasive operations collectively aimed to denigrate Ukraine and its people, with the objective of influencing public opinion and potentially impacting the electoral landscape.

2.1.2 Anti-European Union

Anti-EU narratives in Poland leveraged Brexit era narratives, broadly alleging that European Union membership diminishes a country's autonomy by ceding sovereignty to external institutions, and portraying national decision-making as dictated by Brussels rather than serving domestic interests. The European Union is also blamed for actively diluting Polish national identity, leading to the erosion of unique cultural heritage and the imposition of foreign values.

Economically, these narratives contend that membership brings negative consequences, including unfair competition, burdensome regulations, and the exploitation of national resources. By deploying a colonial metaphor, foreign actors aim to ignite historical grievances, foster nationalist sentiments, and exploit existing societal divisions, ultimately undermining the legitimacy of a country's independent choice to engage with the European Union and weakening its Western alignment.

In the case of the Polish election, anti-European Union narratives targeted and worked to exacerbate a variety of ongoing debates in Poland. As discussed below, these narratives broadly encompassed themes designed to undermine electoral legitimacy, cast doubt on external alliances, and assign blame for domestic economic challenges.

This narrative refers to the Romanian judiciary having prompted a doover of the Romanian presidential elections in the wake of widespread circumvention of campaign rules by one, coincidentally anti-EU, camp. Foreign actors seized on these events, alleging that the EU would do the same if the results of the Polish election were not favourable.

The narrative asserts that Ukrainian intelligence controls the European Union and, in some cases, specific politicians, is circulated by foreign actors with much less detail than other narratives and with no clear evidence to point to. Such disinformation narratives often seek to undermine confidence in not only Ukrainian agency but also European institutions, highlighting the need for critical evaluation of sources and motives behind such allegations.

Poland's financial situation, including the economic crises and worsening welfare, was also blamed on the EU by foreign actors, alleging that these financial difficulties were a part of an EU conspiracy and, in some cases, that lifting sanctions on Russia would alleviate them. This narrative serves a dual purpose, undermining both the EU and Polish establishment in an attempt to diminish the population's trust in their government's financial systems.

In tandem with the systematic spread of anti-EU narratives, threat actors actively promoted anti- EU Presidential candidate Grzegorz Braun and Eurosceptic Slawomir Mentzen. These individuals were positioned as offering a definitive solution to the problems attributed to the European Union, capitalising on existing economic anxieties and national sovereignty concerns among the populace. A striking illustration of this strategy involves Grzegorz Braun: highly symbolic videos of him publicly burning and destroying the EU flag were widely circulated on *X by state-aligned media outlets, including RT*.

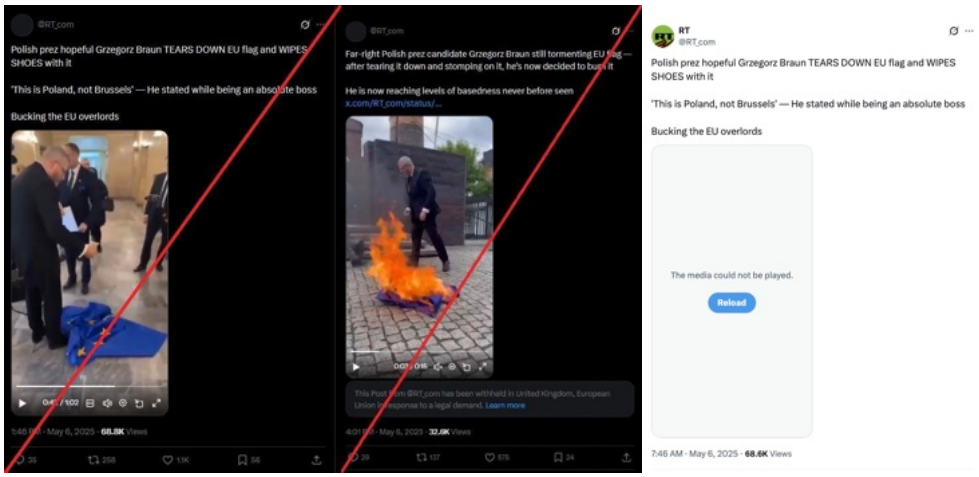

Figure 9: X posts by sanctioned RT accounts showing presidential candidate Grzegorz Braun burning and stamping on an EU flag

Through this amplification, Braun was deliberately presented as an uncompromising anti-EU candidate who would vigorously "hold the EU accountable", ensuring it could not continue to exert perceived undue control or influence over Poland's national policies and sovereignty. This concerted promotion aimed to legitimise radical anti-EU stances and further polarise public discourse ahead of the election.

In summary, the pervasive narrative that 'The European Union is Controlling Poland' formed a critical pillar of foreign influence operations during the election. Framed through a colonial lens, these narratives systematically alleged that EU membership erodes Polish autonomy and national identity while inflicting negative economic consequences. This sentiment was further amplified through specific claims, such as alleged EU interference in elections and blame for economic woes. Crucially, **threat actors actively promoted anti-EU presidential candidates, presenting them as solutions to these perceived problems and leveraging highly symbolic acts, all designed to impact the election outcome by deepening societal divisions and undermining Poland's European integration.**

2.1.3 Anti-Establishment

Delegitimisation of incumbent governments is a staple of Russian influence operations. In this case, anti-government narratives were deployed during the election campaign to undermine the existing government. Allegations of corruption, censorship, and incompetence were common, with narratives of incompetence often targeting Rafal Trzaskowski. Figure 10 illustrates an example of a Radio Belarus video on YouTube attacking and accusing Rafal Trzaskowski of being an *"instrument of foreign influence, representing foreign powers and undermining Polish sovereignty".*

Figure 10: Radio Belarus YouTube Video Attacking Rafal Trzaskowski

Narratives related to social betrayal in the context of the war between Russia and Ukraine were also rife, with accusations alleging that Polish military spending was prioritised at the expense of social services. Perhaps the most aggressive element of this was the sub-narrative that support for Ukraine is equivalent to betrayal of the Polish nation, a narrative which actively capitalises on anti-Ukrainian sentiments.

Threat actors actively undermine the Polish government by accusing it of failing to serve its citizens, thereby seeking to legitimise citizen activism and even subversion. Specifically, FIMI narratives advocate for individual action against the government, and issue explicit warnings against participating in the election, citing purported safety risks and the government's inability to ensure security.

These concerted efforts collectively aim to **raise fundamental concerns about the legitimacy of the election process,** making the idea of c**itizen defiance against the government more compelling** and potentially **fostering widespread distrust in democratic institutions.**

2.1.4 Anti-West

Russian disinformation consistently portrays Western countries and organisations as well as Ukraine as "decaying" and "corrupt", aiming to undermine them and elevate Russia as a morally superior actor. In the Polish context, these narratives adhered to this established pattern, alleging moral degradation and ineptitude amongst Polish politicians, accusing Volodymyr Zelensky of drug addiction, and attempting to delegitimise any critics of Russia within Poland.

One of the most outlandish decaying narratives spread during this period claimed that *French President Emmanuel Macron, German Chancellor Friedrich Merz, and British Prime Minister Keir Starmer were using cocaine together on a plane while on a train to Ukraine*. This fabricated video was subsequently amplified across social media by pro-Russian and international influencers, including American conspiracy theorist *Alex Jones*, whose X post on the topic received over 30 million views.

Figure 11: Alex Jones Accusing President Macron, Prime Minister Starmer and Chancellor Marz of doing cocaine on a train

In summary, narratives depicting the West as "decaying" and "corrupt" consistently aimed to undermine trust in democratic leadership and institutions, both within Poland and among its international allies. By employing outlandish and often fabricated claims, these campaigns sought to delegitimise critics of Russia and reinforce a perception of Russia's moral superiority, ultimately contributing to internal fragmentation and external distrust within the Polish political landscape.

2.1.5 Targeting of Karol Nawrocki, and Rafał Trzaskowski

Info Ops Poland's analysis of the Polish presidential campaign revealed deliberate efforts by Russian-aligned actors to discredit the opposing frontrunner candidates: Karol Nawrocki and Rafał Trzaskowski. Both faced attacks from these entities, with a noticeable increase in content targeting Nawrocki ahead of the second round of voting, while negative narratives surrounding Trzaskowski persisted.

Despite variations in intensity and specific details, the fundamental tactics employed against both candidates were similar. The overarching goal across all content was to portray Poland as a non-sovereign state, allegedly controlled by foreign interests. This strategy aimed not at endorsing any particular candidate, but rather at framing the entire Polish political scene as a "puppet theatre", thereby threatening the state's stability and democratic legitimacy. Kremlin media consistently utilise a proven set of propaganda tactics, reducing citizens' choices to an emotional "East versus West" dichotomy, replacing genuine policy debate with false simplifications and fear.

For **Karol Nawrocki**, a dual narrative mechanism was employed: one portraying him as a "Russophobe" destroying Red Army monuments and threatening peace, and another as "Trump's agent" ready to forge a "devil's pact" with Washington. This allowed the same candidate to be used to intimidate audiences or reinforce isolationist sentiments depending on propaganda needs.

Similar mechanisms were applied to **Rafał Trzaskowski**, though with different thematic emphases. His negative image was constructed around his alleged ties to "rotten elites" - labelling him a "candidate of the Brussels salons" and "Soros's Vassal" - and accusing him of abandoning traditional values in favour of a "liberal agenda" (e.g., on abortion and LGBTQ+ rights). In both cases, the disinformation served not only a reputational purpose but also a demobilising function, discouraging voters from participating in the election. Notably, other openly pro-

Russian candidates were entirely excluded from discrediting actions throughout the official election campaign. This content was inauthentically disseminated across social media platforms by accounts controlled or inspired by the Russian influence apparatus. These profiles, while presenting as independent individuals, followed an easily identifiable script:

- **Initiating discussion:** publishing a provocative headline or graphic;
- **Fanning emotions:** adding comments such as: "Look what the Russophobic elites are planning to impose on us!";
- **Amplifying reach:** mass sharing of the same message by successive accounts, often with cosmetic modifications;
- **Manipulation's finale:** a call for a "patriotic choice" and voting for the only "sensible" political option.

The aim of this activity was not merely to shape electoral perception but also to create the illusion of grassroots consensus online. The tactic serves to lower voting turnout and exacerbate polarisation, further destabilising the political scene regardless of the final election outcome. This operating model relies on creating false dichotomies, fundamentally fostering the impression that only candidates “free from prejudice” against Russia offer a safe future for Poland.

2.2 Sub-Narratives

This report identifies five distinct sets of sub-narratives, each of which supports a larger metanarrative spread during the Polish presidential election. These sub-narratives all played a crucial role in shaping public perception and discourse throughout the campaign. Each set of sub-narratives will be discussed briefly below, with the most prominent narratives

receiving the most attention. Less prominent narratives will be outlined in some detail in the attached appendix, providing a comprehensive overview of their contribution to the electoral landscape.

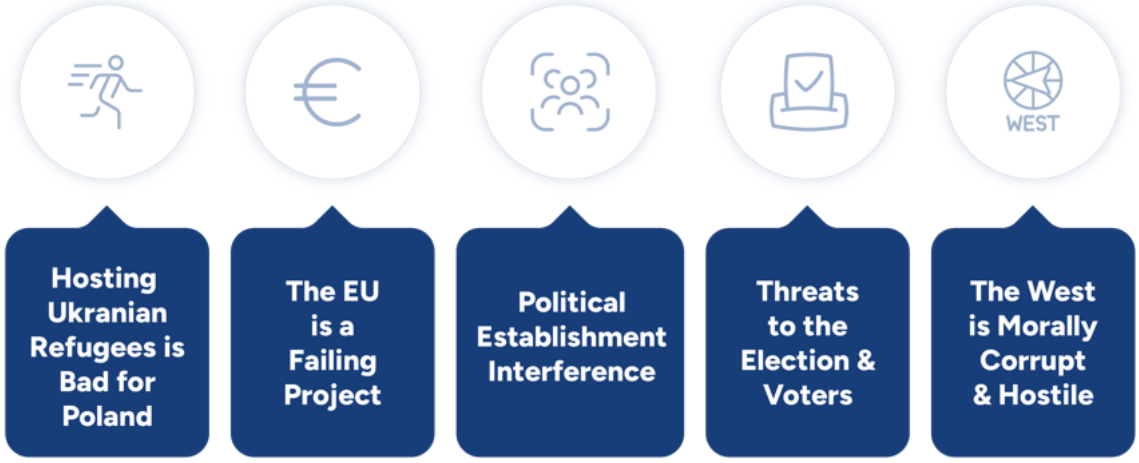

Figure 12: Prominent Sub Narratives During the Polish Presidential Elections

2.2.1 Hosting Ukrainian Refugees is Bad for Poland

Poland has been the target of large-scale Russian FIMI, often supported by Belarus, since Russia's annexation of Crimea in 2014. This persistent aggression is primarily rooted in Poland's steadfast close relationship with Ukraine and its pivotal role in accepting significant numbers of Ukrainian refugees. As a long-standing key ally of Ukraine, Poland has consistently backed the country's bids for both EU and NATO membership. Poland's strong position in the international arena, coupled with its membership of both the European Union and NATO, positions its robust support for Ukraine as a significant strategic challenge to Russia. Consequently, Russian FIMI efforts have specifically aimed to undermine Poland's vital alliances and domestic stability.

Since the full-scale invasion of Ukraine in 2022, Russian FIMI operations targeting Poland have taken on another concerning dimension: the deliberate targeting of Ukrainian refugees residing in Poland in an attempt to stoke resentment. The tactic represents a further extension of Russia's aggression against Ukrainians, aiming to deny them safety not only within their own borders but also once they have sought refuge in another country. The psychological and emotional toll of such tactics intentionally creates an atmosphere of hostility and polarisation, directly undermining refugees' sense of safety and security within their host communities.

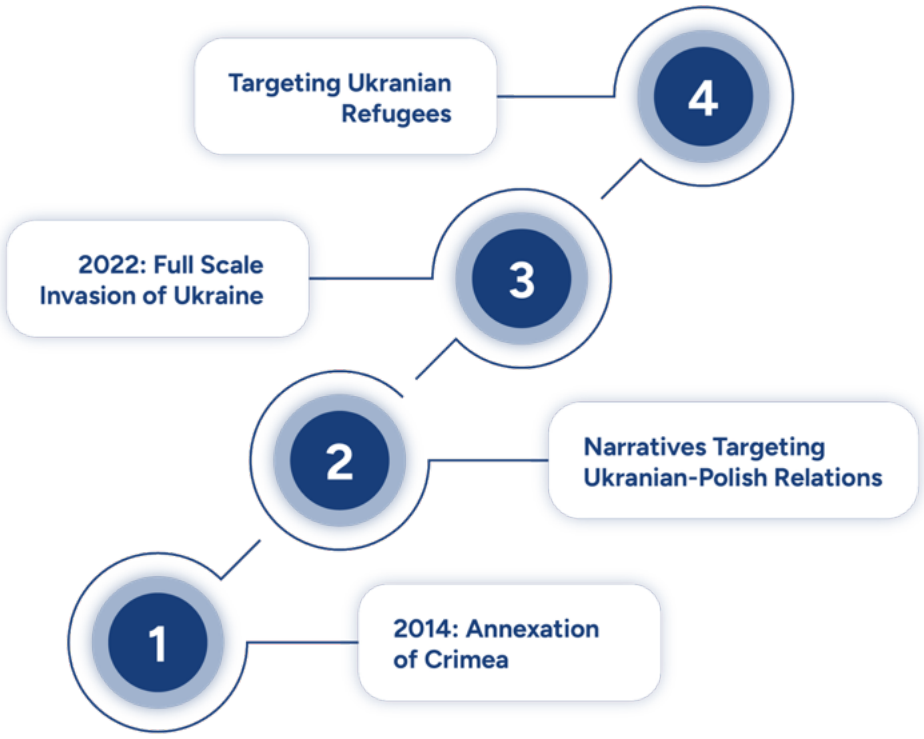

Figure 13: Evolution of Russian FIMI Operations Targeting Ukrainians in Poland

Narratives:

Figure 14: Key Anti-Ukrainian Refugee Themes

- **Opposition to supporting Ukraine:** This *narrative asserts* that Poland should cease its support for Ukraine and Ukrainian refugees. It argues that the full-scale invasion of Ukraine falls outside of Poland's direct national interest, and that financial resources currently directed towards Ukraine constitute a misallocation of funds that should instead be prioritised for Polish citizens.
- **Exploitation of EU countries' aid systems by Ukrainian refugees**: This *narrative accuses Ukrainian refugees* in Poland and other EU countries of broadly exploiting the various humanitarian and social aid systems established to assist them. It often portrays refugees as opportunistic, driven by excessive material demands, and receiving unjustified financial gain from these systems, thereby burdening host nations without due cause.
- **Manipulation of state benefit schemes by Ukrainian refugees:** This *distinct narrative* asserts that Ukrainian refugees are actively manipulating formal state benefit schemes to maximise their financial intake. This content explicitly highlights alleged fraudulent or deceptive practices that result in disproportionate financial profits for refugees, thereby draining the budgets of host governments and diverting funds that should ostensibly be allocated to local citizens.
- **Ukrainian refugees are a security threat to the EU:** This *narrative propagates* the claim that Ukrainian refugees who have sought refuge in the EU pose a direct security threat to the Union and its citizens.

- **Ukrainian refugees are a threat to Poland:** This *narrative asserts* that Ukrainian refugees who have fled to Poland are a direct physical threat to the country and its citizens.
- **Ukrainian 'terrorists' plan to assassinate Polish politicians:** This narrative alleges that Ukrainian refugees have plans to assassinate Polish politicians and perpetrate violence against Polish officials. Figure 15, derived from *ISD's investigation of Russia amplifying negative sentiment towards Ukrainians*, depicts four posts from Operation Overload on X that allege assassination plots targeting politicians.

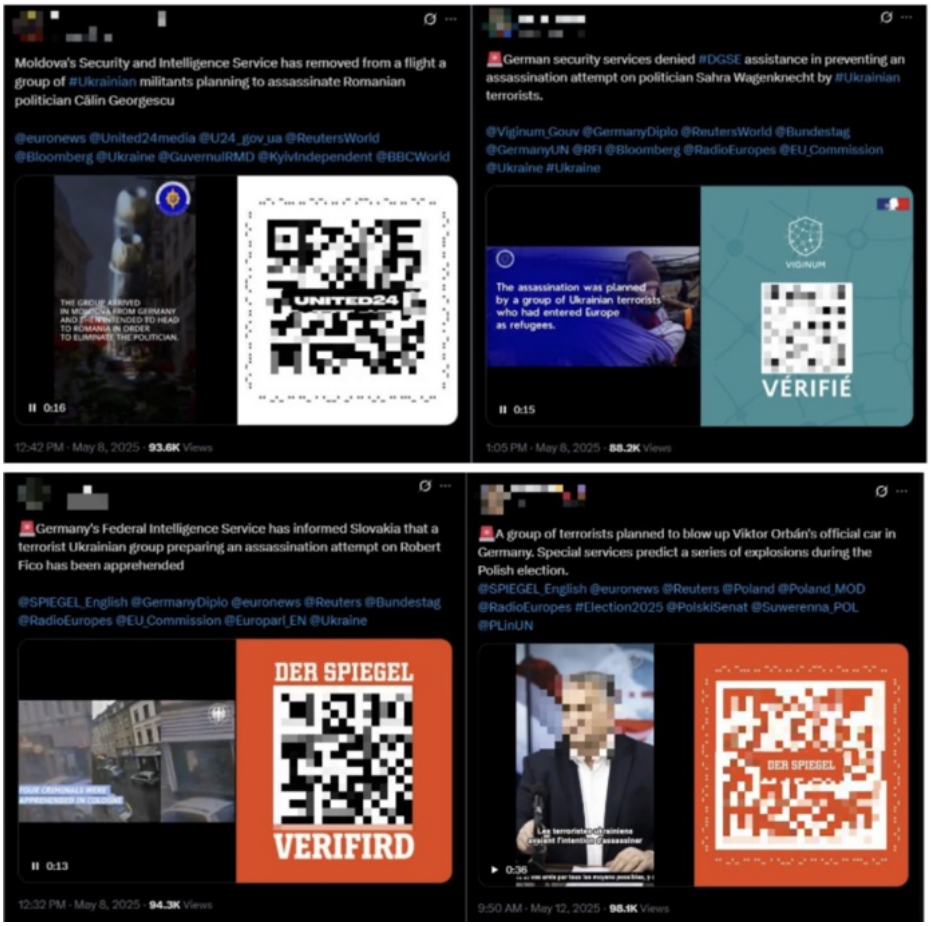

Figure 15: Key Anti-Ukrainian Refugee Themes

- **Widespread 'cover up' of Ukrainian terror attack plans in Europe:** This narrative asserts that Western governments and European establishment possess knowledge of Ukrainian terrorist attack plans on European soil but are deliberately censoring this information and withholding it from the public (*see figure 16*).

Figure 16: Operation Overload post to X with Ukrainian Terrorist Narrative

- **Poles are intolerant of Ukrainians:** This *narrative propagates* the claim that Polish citizens exhibit intolerance towards Ukrainians, citing alleged instances of theft and other illicit activities as a basis for this sentiment.
- **Ukrainian symbols are a threat to Polish national identity and should be removed:** This *narrative argues* that the display of Ukrainian symbols in Poland poses a threat to the homogeneity and dominance of Polish national identity, thereby asserting that these symbols must be removed.
- **Polish courts support the right to remove Ukrainian flags:** This *narrative alleges* that, notwithstanding provisions in the criminal code, Polish courts endorse the right of Polish citizens to remove Ukrainian symbols as a means to preserve their national identity.

These narratives draw from a variety of tried-and-tested narratives often employed by Russian FIMI operations, collectively aiming to diminish support for Ukraine within Poland. A primary strategy involves leveraging prevailing economic anxieties: by blaming Ukrainian refugees for local financial issues and criticising Poland's substantial aid to Ukraine, these narratives exploit the complexities of government finances. Such simplification offers ostensibly straightforward explanations for broader economic downturns, like rising inflation and increased cost of living, making financial grievances a potent tool for weaponisation.

A significant and concerning development observed during this election cycle is the emergence of narratives accusing Ukraine and Ukrainian refugees of violence or terrorism. **Unlike prior electoral FIMI operations, these allegations of terror attacks at voting stations or targeting politicians appear intended to deter specific voter groups, particularly those supporting pro-EU candidates, by instilling fear for their safety.**

The direct link drawn by FIMI actors between Ukrainian presence and domestic security threats represents a new frontier in Russia's FIMI operations. **By extending the categorisation of Ukraine's legitimate counterattacks on Russian soil as 'terrorism' to other countries, these campaigns seek to discredit Ukraine more broadly and generate unwarranted fear of Ukrainian actions in non-belligerent states like Poland.**

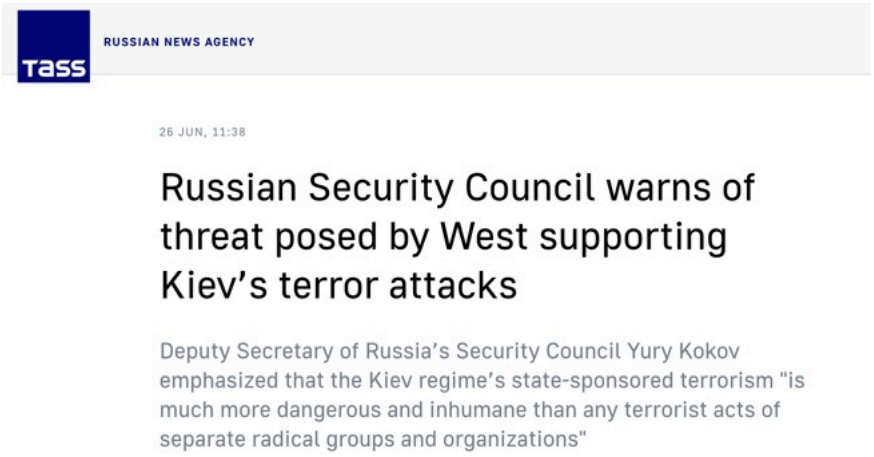

Figure 17: TASS Article Accusing Ukraine of State Sponsored Terrorism

These developments pose **a substantial risk to election integrity and can contribute to the radicalisation of political discourse across Europe.** By fabricating or amplifying fears of violence, these narratives directly aim to suppress voter turnout, especially among segments of the electorate targeted for their pro-European or centrist views. Furthermore, by fostering the perception that the government is failing to protect its citizens from an alleged "Ukrainian threat", or even actively concealing such threats, **these narratives systematically erode public trust in state institutions, including the very process of elections.**

This environment of distrust can push voters towards more extreme political factions, particularly far-right movements, who capitalise on these fear-based narratives and

present themselves as the only viable option to address the perceived security vacuum.[12] Ultimately, **such disinformation creates fertile ground for societal fragmentation, making populations more susceptible to radicalised viewpoints and increasing the likelihood of challenges to legitimate election results, thereby directly compromising the democratic process itself.**

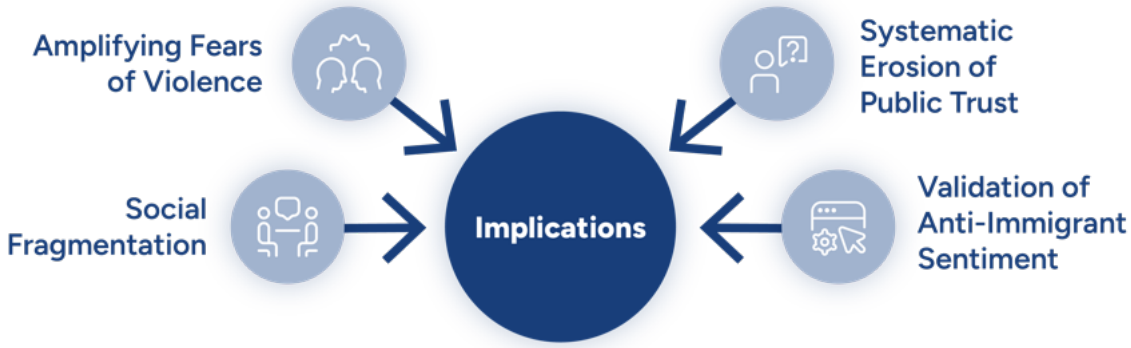

Figure 18: Implications of Anti-Ukrainian Narrative

Beyond the immediate electoral context, **this development also carries profound implications for right-wing extremism and radicalisation across Europe.** By consistently portraying Ukrainian refugees as a direct security threat, **such narratives directly validate and intensify pre-existing xenophobic and anti-immigrant sentiments prevalent within extremist circles.** This provides a perceived, albeit false, justification for discrimination, marginalisation, or even violence against refugee populations. Extremist groups actively leverage these narratives to frame their animosity as a legitimate response to a "national security risk", thereby enabling them to recruit new adherents and solidify their base. Furthermore, by fostering profound distrust in democratic institutions that support refugees, and by shifting blame for societal issues onto a vulnerable group, these narratives actively fuel anti-establishment grievances. They empower extremist groups to argue that mainstream governance is either incompetent or complicit in allowing a 'threat' to persist, thereby eroding public confidence and pushing individuals towards more radical solutions.[13]

This process of blaming, dehumanising, and discrediting ultimately contributes to an environment fertile for further radicalisation and exacerbated societal fragmentation across Europe.

[12] On authoritan threats to democracies, see: https://www.americanprogress.org/article/how-democracies-defend-themselvesagainst-authoritarianism/
[13] Interview with Special Adviser in Strategic Communication to the EU Knowledge Hub on Prevention of Radicalisation, June 2025

2.2.2 The EU is a Failing Project

Anti-EU narratives, a classic and tried-and-tested set of Russian FIMI narratives, extensively targeted the Polish election in 2025. These narratives approached the issue from various angles, including anti-elite rhetoric, arguments echoing Brexit-related sentiments, and even colonial narratives, all aimed at undermining the European Union and its supporting candidates.

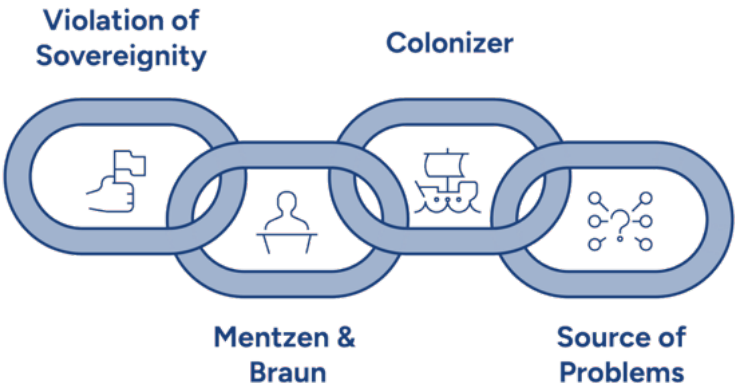

Figure 19: Key Elements of Anti-European Union Narratives

Narratives

- **EU overreach:** This *narrative asserts* that the European Union exercises excessive control over its member countries, infringing on their sovereignty and autonomy.
- **'Polexit' push:** This *narrative advocates* for Poland to follow the United Kingdom's precedent and withdraw from the European Union, employing the same logic as Brexit.
- **Anti-Economic sanctions:** This *narrative claims* that economic sanctions imposed on Russia, following its full-scale invasion of Ukraine, are inflicting greater harm on the European economy than on the Russian economy.
- **EU election interference:** This *narrative alleges* that the European Union intends to interfere in the Polish election, drawing parallels to perceived past interferences (e.g., in Romania), and threatening to cancel or void results unfavourable to its interests.
- **Promotion of anti-EU candidates:** This *narrative specifically* promotes Polish presidential candidates known for their anti-EU stances, such as Sławomir Mentzen and Grzegorz Braun, as viable and preferable choices.
- **EU blocking Slawomir Mentzen's path to electoral victory:** This *narrative contends* that the European Union is actively preventing Sławomir Mentzen from achieving electoral victory in the Polish presidential election due to his anti-EU political alignment.

- **Grzegorz Braun as EU challenger:** This *narrative portrays* Grzegorz Braun as a politician courageously defending Polish interests against the European Union, thereby presenting him as a strong and suitable presidential candidate.
- **EU as coloniser:** This *narrative draws from those often leveraged* in countries formerly colonised by European powers, alleging that the European Union functions as a de facto colonial power, exerting control over and effectively ruling Poland from Brussels.
- **EU responsibility for the economic crisis:** This *narrative attributes* Poland's current economic crisis directly to the European Union, promising that an exit from the EU would resolve these financial challenges.
- **EU responsible for worsening welfare:** This *narrative alleges* that the European Union is responsible for the deteriorating welfare of Polish citizens, positing that leaving the EU would ameliorate their living conditions.

Anti-EU narratives constitute a core of Russia's consistently deployed FIMI story lines, resurfacing frequently. These narratives strategically blend anti-establishment and anti-Western sentiments, positioning the European Union as a convenient "stand-in villain" responsible for a wide array of domestic and international challenges.

Drawing from diverse angles, these narratives aim to **erode fundamental trust in the Union's legitimacy and portray membership as an infringement on national sovereignty.** This includes claims of EU overreach, alleging excessive control over member countries and infringement on their autonomy. The push for a 'Polexit' directly advocates for Poland to leave the Union. Concurrently, **narratives alleging the EU's responsibility for economic crises and the worsening welfare of citizens**, alongside claims that anti-Russian sanctions disproportionately harm Europe, **directly weaponise economic anxieties.** The inherent complexity of the EU's governance and financial mechanisms is often exploited, **transforming a lack of public understanding into deep suspicion, distrust, and blame.** Furthermore, the narrative portraying the EU as a coloniser that de facto rules Poland **reinforces a sense of subjugation and loss of national identity.**

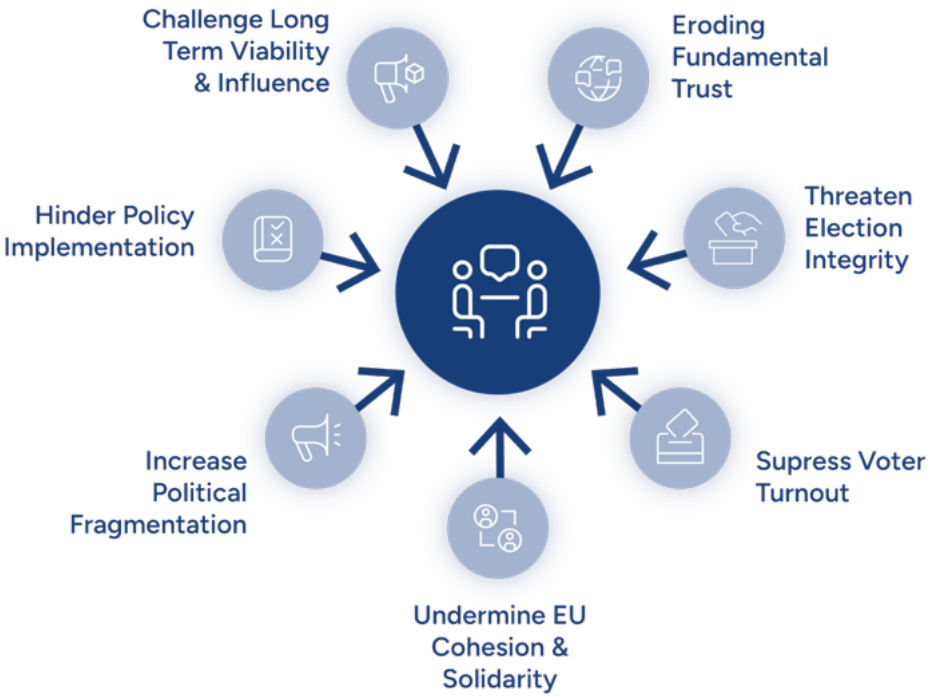

Figure 20: Implications of Anti-EU Narratives

Critically, these anti-EU narratives pose a significant threat to election integrity. Assertions regarding the EU's intent to interfere in the Polish election, mirroring alleged past incidents, aim to delegitimise the electoral process before votes are even cast. This is further compounded by the promotion of anti-EU candidates like Sławomir Mentzen and Grzegorz Braun, coupled with claims that the EU is blocking their path to victory or that Grzegorz Braun is uniquely standing up to the EU.

Such narratives are designed to suppress turnout among pro-EU voters, influence undecided voters towards Eurosceptic candidates, and foster a climate where election results unfavourable to the anti-EU agenda can be immediately questioned or rejected as manipulated.

For the European Union itself, the widespread dissemination of these narratives, particularly within key member states like Poland, carries profound implications. It risks **undermining internal cohesion and solidarity, making it harder for the Union to present a united front on critical geopolitical issues, including continued support for Ukraine and collective defence.**

By eroding public support for EU membership and demonising its institutions, these campaigns could potentially pave the way for **increased political fragmentation, hinder effective policy implementation, and ultimately challenge the long-term viability and influence of the European project.**

2.2.3 Political Establishment Interference

Anti-establishment narratives constitute a prominent category within Russian FIMI operations, employed to delegitimise and discredit the Polish government, its media, and various political figures. These narratives commonly leverage accusations of corruption, mismanagement, and censorship against their targets, primarily public figures and institutions. Once disseminated, **these narratives are exceptionally difficult to definitively disprove, a result of the absence of verifiable evidence, strategically framed as proof of a cover-up or an indicator of guilt.** This narrative enables the weaponisation of the burden of proof to foster distrust among society.

Narratives

- **Criticism of Prime Minister Donald Tusk:** This *narrative asserts* that Prime Minister Donald Tusk is incompetent and has engaged in financial misconduct, arguing that he is unfit to hold the office.
- **The Polish government mismanages public services and migrants:** This *narrative claims* that the Polish government demonstrates profound mismanagement in the provision of public services and in its handling of migrant-related issues.
- **Polish authorities focus on migration, Belarus on real threats:** This *narrative contrasts* the Polish authorities' focus on migrant flows with allegedly heroic actions by Belarusian customs officers, who are portrayed as having prevented the smuggling of explosives into Russia, thereby averting a potentially catastrophic incident.
- **Defence of Polish ethno-religious identity:** This *narrative argues* for the imperative defence of Poland's ethno-religious identity against the perceived threat posed by the arrival of migrants and Ukrainian refugees, who are seen as introducing their own distinct identities.
- **Delegitimisation of the Polish state:** This *narrative asserts* that members of the Polish government lack legitimate authority and are inherently untrustworthy.
- **Delegitimisation of critical media:** This *narrative contends* that mainstream media outlets cannot be relied upon to deliver truthful or accurate information to the public.
- **The Polish government is corrupt and introduces censorship**: This narrative claims that the Polish state is *corrupt* and actively engages in censorship against anti-establishment voices, thereby preventing them from having a fair opportunity in elections.
- **Rafal Trzaskowski is biased in his actions:** This *narrative alleges* that Rafal Trzaskowski acts as an instrument of foreign influence, representing external powers rather than Poland's interests, and actively undermines Polish sovereignty.

- **Polish politicians are subservient to foreign forces:** This *narrative asserts* that establishment Polish politicians, specifically naming Rafał Trzaskowski and Karol Nawrocki, serve foreign interests rather than the Polish populace, thereby undermining the nation's sovereignty.
- **The Polish government prioritises military spending over social service spending:** This *narrative argues* that the Polish government's substantial military spending indicates a prioritisation of war over the welfare of its citizens, leading to an escalation of Poland's involvement in the war in Ukraine while merely paying lip service to peace.
- **Poland is escalating the war in Ukraine:** This *narrative claims* that Poland is actively escalating the conflict in Ukraine by providing an exceptionally large amount of weapons and financial aid, thereby ensuring the continuation of the war.
- **The Polish government is mishandling migration:** This *narrative alleges* that the Polish government's handling of migration issues is detrimental, concurrently undermining Poland's ethno-religious identity.
- **The Polish government is mishandling healthcare:** This *narrative contends* that the Polish government's management of the healthcare system is deficient, resulting in negative consequences for its citizens.
- **The Polish government is mishandling the national debt:** This *narrative asserts* that the Polish government's mismanagement of the national debt places its citizens' financial security at significant risk.
- **Citizens must act on their own and take justice into their hands:** This *narrative advocates* for Polish citizens to take autonomous action against their government, particularly on issues concerning migration and Ukrainian refugees, in order to protect their country and culture.

The anti-establishment narratives observed during this electoral period in Poland vividly illustrate the complex and dangerous connection between Domestic Information Manipulation and Interference (DIMI) and Foreign Information Manipulation and Interference (FIMI). While foreign actors were undoubtedly instrumental in packaging, amplifying, and strategically introducing these narratives into the Polish information environment, **their profound effectiveness stemmed from their ability to latch onto and exploit pre-existing, domestically rooted grievances and socio-political discussions within Polish society**[14].

[14] A similar dynamic was observed by ISD and other project partners working to monitor the German federal election in February 2025. Specific cases of domestic grievances being exploited by FIMI actors are detailed in the post-election country report: *https://www.isdglobal.org/isd-publications/country-report-assessment-of-foreign-information-manipulation-and-interference-fimiin-the-2025-german-federal-election/*

This symbiotic relationship allows FIMI operations to identify authentic local discontent – the DIMI component – and then weaponise it to achieve foreign policy objectives, **transforming homegrown scepticism into a powerful vector for manipulation.**

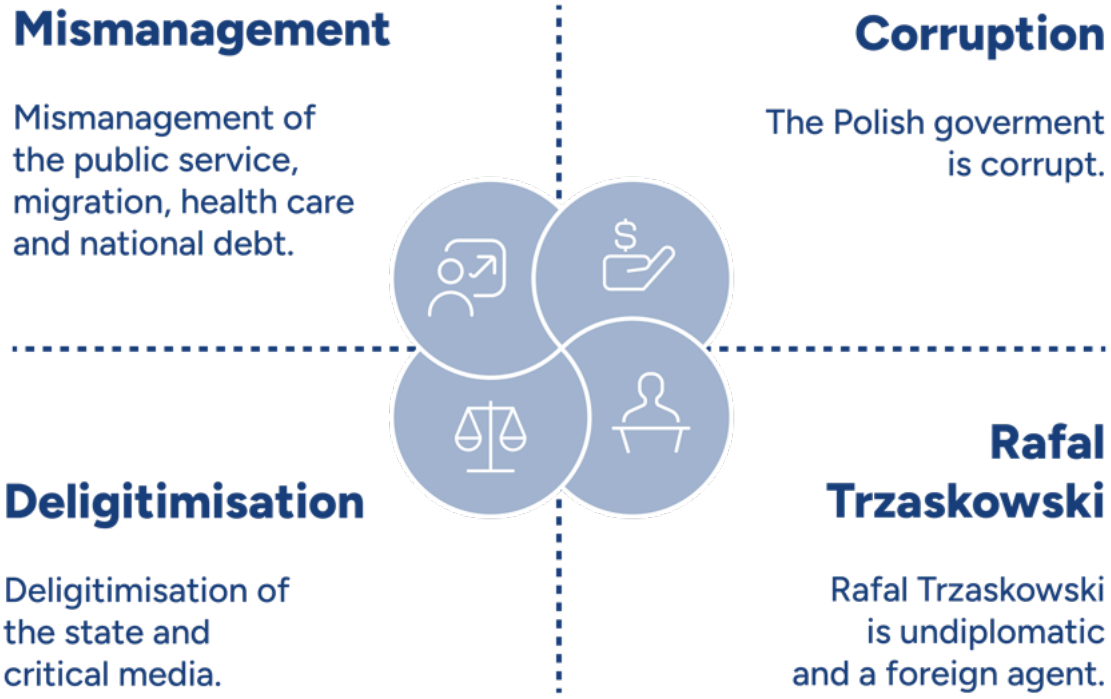

Figure 21: Key Angles of Anti-Establishment Narratives

Poland's historical and ongoing experience as both a transit and destination country for migrants, coupled with its significant economic growth *since the 1990s*, has made migration and identity politics perennially sensitive and salient issues. **This deeply rooted socio-political context creates fertile ground for narratives that exploit anxieties around national identity,** such as the "Defence of the Polish ethno-religious identity" against perceived external cultural incursions, or those that blame authorities for perceived mismanagement of migrant flows.

These narratives resonate strongly by tapping into genuine concerns and historical sentiments within the population.

Beyond migration, other narratives widely employed during this period targeted broader governmental trust. Accusations of corruption, mismanagement of public services, national debt, or healthcare, along with allegations of censorship or subservience to foreign forces, preyed on existing public scepticism.

For instance, narratives like "Criticism of Prime Minister Donald Tusk", claims that "The Polish government is corrupt and introduces censorship", or that "Rafal Trzaskowski is biased in his actions" and "Polish politicians are subservient to foreign forces", tap directly into pre-existing distrust.

This exploitation of confirmation bias provides audiences with ostensible "proof" of suspected governmental failings, making them highly susceptible to subsequent, similarly themed narratives disseminated by the same actors. This includes narratives specifically aimed at "Delegitimisation of the Polish state" and "Delegitimisation of critical media" itself. The promotion of narratives that "The Polish government prioritises military spending over social service spending" and that "Poland is escalating the war in Ukraine" further feeds into public anxieties, framing governmental actions as detrimental to citizen welfare in favour of foreign conflicts.

The cumulative effect of these anti-establishment narratives poses significant risks to election integrity. By systematically eroding public trust in the government, media, and political figures, they **cultivate an environment where the legitimacy of the electoral process itself can be easily questioned.** Narratives that assert "citizens must act on their own and take justice into their hands" implicitly **encourage subversion and distrust in democratic mechanisms, potentially leading to voter apathy, a rejection of legitimate election outcomes, or even civil unrest.** Such efforts directly undermine the stability and fairness essential for democratic elections.

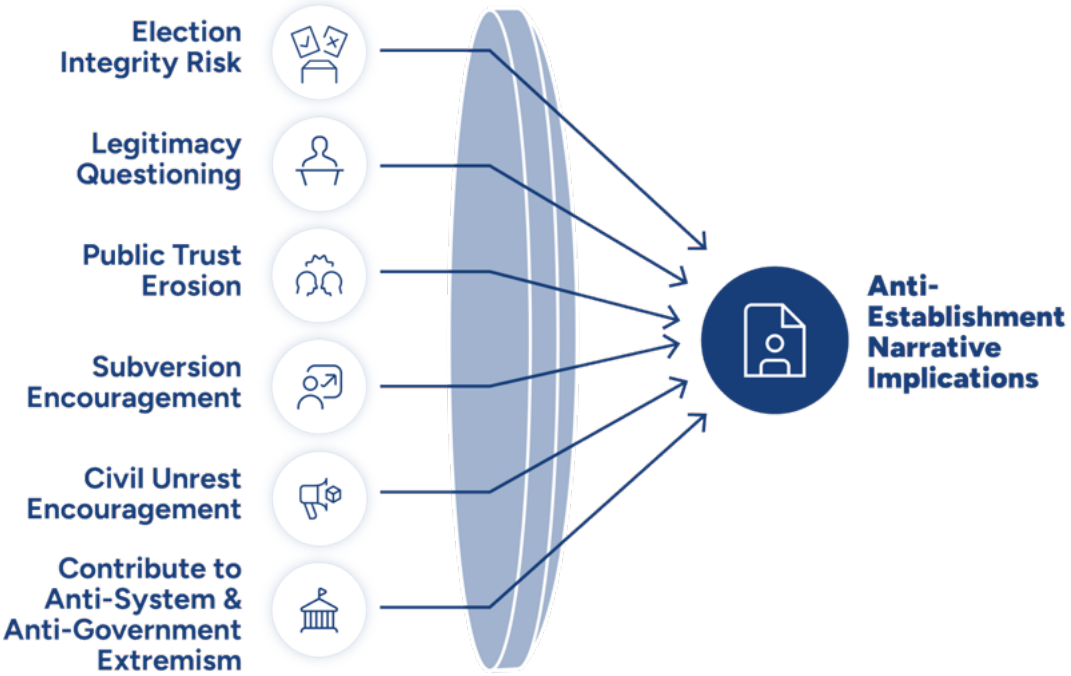

Figure 22: Anti-Establishment Narrative Implications

Finally, these disinformation campaigns significantly contribute to **Anti-System and Anti-Government Extremism (ASAGE).**[15] By relentlessly attacking the legitimacy and competence of the Polish government and state institutions, and by portraying political figures as corrupt or subservient to foreign interests, **these narratives aim to fundamentally undermine the public's faith in the existing political system.** Calls for citizens to "act on their own and take justice into their hands" are a **direct incitement towards anti-system behaviour, encouraging a rejection of democratic processes and potentially fostering radicalised viewpoints that advocate for the overthrow or severe disruption of the established order.**[16] This sustained erosion of trust creates a fertile ground for extremist ideologies that seek to dismantle or radically alter the current system of governance, thereby further exacerbating societal fragmentation.

2.2.4 Threats to Election and Voters

A distinct subset of the identified narratives during the Polish presidential election specifically targeted the electoral and voting process. These narratives sought to influence both Polish voter turnout and ballot choices with some explicitly discouraging citizens from attending polling stations by alleging the risk of terrorist attacks.

Figure 23: Key Narrative Angles of Election Specific Narratives

[15] On ASAGE see: Farinelli, F., Marinone, L., Daher, S., The Anti-System/Anti-Government Extremism Handbook, RAN Policy Support – European Commission, 2024.
[16] Interview with Special Adviser in Strategic Communication to the EU Knowledge Hub on Prevention of Radicalisation, June 2025.

Narratives

- **There is a serious terrorist threat to the election:** This *narrative claims* the existence of terrorist plots specifically targeting voting stations, asserting that it is too dangerous for citizens to participate in the election process and that voters cannot be guaranteed safety.
- **The Polish government cannot guarantee the security of the election**: This *narrative posits* that the Polish government is incapable of ensuring the physical safety of voters at polling stations while casting their ballots, and furthermore, cannot guarantee the accuracy or integrity of the election results themselves.
- **Polish elections do not meet European standards:** This narrative directly challenges the legitimacy of Polish elections, alleging that they are not free and fair and fail to meet established European standards for electoral integrity.
- **Pour wax over the ballots to safeguard the validity of your vote:** This narrative instructs voters to perform an unusual ritual - lighting a candle and pouring wax over their marked ballot - to supposedly safeguard its validity. It falsely claims that without this act, votes can be secretly erased by passing a flame under the ballot, allowing for manipulation.[17]
- **Local vote rigging may be difficult, but central vote manipulation is still possible**: This *narrative creates* a distinction between perceived honesty at the local voting level and alleged corruption at the centralised vote tabulation stage. It claims that while local rigging is difficult due to the trustworthiness of local officials, votes can still be manipulated once they are transferred to central locations.
- **Anti-establishment voices are silenced through limited media access, biased coverage, and exclusion from the polls:** This *narrative asserts* that the established political system actively suppresses anti-establishment voices by limiting their access to media, ensuring biased coverage, and thereby excluding them from having a fair chance in the election or significantly reducing their vote count.
- **Ukrainian refugees are planning to target the election with terrorist attacks:** This *narrative falsely claims* that Ukrainian refugees, having infiltrated Poland, are planning terrorist attacks specifically against voting stations, thereby making it too dangerous for citizens to participate and compromising voter safety.
- **Endangerment and instability of Polish elections:** This narrative broadly communicates that participation in the election is dangerous, and simultaneously, that the Polish electoral system as a whole is fundamentally unstable and unreliable.[18]

[17] This narrative was documented in Incident Alert 0068 on the pouring of wax over voting ballots to ensure they are not tampered with

[18] This narrative was documented in Incident Alert 0063 on the exploitation of disinformation targeting the Polish election to generate ad revenue.

A distinct subset of these FIMI narratives directly focused on influencing the election and voting process, posing a direct threat to election integrity. This narrative, "there is a serious terrorist threat to the election", claimed the existence of terrorist plots specifically targeting voting stations, asserting that "It is too dangerous to go out and vote. Voters are not safe". This blatant attempt to instill fear and suppress voter turnout was reinforced by claims that "The Polish government cannot guarantee the security of the election", implying both physical insecurity at polling stations and an inability to ensure accurate electoral outcomes. **Such narratives fundamentally undermine the security and trust essential for free and fair democratic participation.**

Beyond direct threats, these campaigns launched a systemic attack on the perceived fairness and transparency of Polish elections. **The narrative that "Polish elections do not meet European standards" directly challenged the legitimacy of the entire electoral framework, alleging a failure to meet international standards of integrity.** More insidious tactics included the "Pour wax over the ballots to safeguard the validity of your vote" narrative, which, despite its absurdity, spread misguidance and distrust in official procedures by falsely claiming votes could be erased.

Furthermore, the claim that "local vote rigging may be difficult, but central vote manipulation is still possible" created a pervasive sense of vulnerability within the vote tabulation process, fostering a belief that even if individual votes were cast honestly, the overall outcome could still be compromised. These efforts were often intertwined with broader anti-establishment messages, asserting that "anti-establishment voices are silenced through limited media access, biased coverage, and exclusion from the polls", thereby discrediting the fairness of political discourse itself.

The overarching narrative of "Endangerment and instability of Polish elections" served to consolidate all these fears, portraying the entire electoral system as unreliable and dangerous.

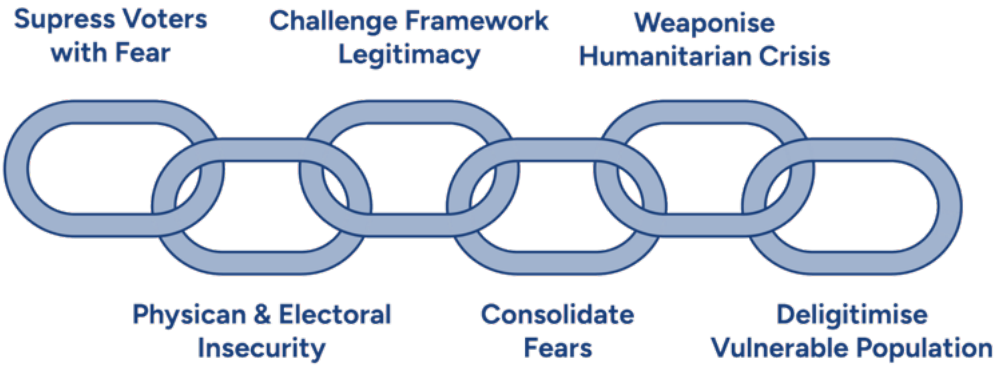

Figure 24: Implications of Election Specific Narratives

For **democracy within Poland and across the European Union**, the widespread dissemination of these narratives represents a severe and multi-faceted challenge. By systematically eroding public trust in the government, electoral processes, and the media, these campaigns cultivate an environment of pervasive scepticism and disengagement. **This deliberate fostering of mistrust in elections not only suppresses voter participation and distorts electoral choices but also weakens the foundational pillars of democratic governance, making societies more susceptible to further foreign interference and radicalisation that rejects the legitimate functioning of the state.**

The explicit accusations that "Ukrainian refugees are planning to target the election with terrorist attacks" serve as a particularly egregious example of **weaponising humanitarian crises to sow fear, delegitimise a vulnerable population, and directly undermine the democratic process, demanding robust and coordinated responses from democratic institutions.**

2.2.5 The West is Morally Corrupt and Hostile

The final grouping of sub-narratives regarding the Polish presidential election covers anti-West narratives, broadly targeting the "collective West" with two instances of Ukraine being singled out over its alleged control of other nations. These narratives are specific to Russian and Belarusian FIMI operations targeting Poland, with references to threats from the West, referring to alleged Western threats against Russia. While anti-West narratives are often consistent across FIMI operations, those spread during the Polish election deviated from the standard formula, increasingly attributing blame to Ukraine and alleging specific, recent threats of violence.

Figure 25: Implications of Election Specific Narratives

Narratives on the Threat from the West and Western Leaders:

- **Threat from the West:** This narrative asserts that Western nations pose a direct and escalating threat to Russia. It primarily substantiates this claim by highlighting the West's sustained support for and armament of Ukraine, alongside the continuous eastward expansion of NATO, portraying these actions as inherently hostile and destabilising.[19]
- **Western leaders are morally degraded and inept:** This *narrative systematically* disparages Western political leadership, portraying them as ethically compromised, lacking competence, and inherently flawed. It links these perceived deficiencies to their governance of secular and liberalised countries, implying a moral decay that undermines their authority and decision-making capabilities.
- **Western security services planned to carry out terrorist attacks in Russia on May 9 (Victory Day) to thwart peace talks with Ukraine:** This *narrative makes* a serious and unsubstantiated accusation, claiming that the security services of Western countries orchestrated a terrorist attack against Russia, specifically targeting the highly symbolic national holiday of Victory Day. It further alleges that the sole purpose of this planned attack was to derail ongoing peace negotiations with Ukraine, casting Western entities as saboteurs of peace.
- **European politicians are secretly controlled by Ukrainian intelligence:** This *narrative propagates* a highly conspiratorial claim, asserting that Ukrainian intelligence covertly controls, manages, and dictates the actions of European politicians. As a direct consequence, it suggests that these politicians are acting against the interests of their own citizens and nations, effectively compromising their countries' sovereignty by serving Ukrainian agendas.
- **Zelensky is a drug addict:** This *narrative attempts* to personally discredit Ukrainian President Volodymyr Zelensky by falsely asserting his addiction to cocaine. The aim is to portray him as volatile and untrustworthy, thereby undermining his credibility and the legitimacy of the Ukrainian government he leads.
- **Polish Armament Agency bought explosives planned to be used inside Russia:** This *narrative makes* a grave accusation against a NATO member, claiming that the Polish Armament Agency acquired explosives. It further alleges that these explosives were intercepted by Belarusian border guards while being illicitly transported into Russia, implying direct Polish involvement in planning attacks within Russian territory.

[19] This narrative was documented in Indecent Alert 0073 - Coordinated Cross-Platform FIMI Campaign Targeting Polish Elections.

These anti-West narratives constitute a sophisticated and aggressive FIMI campaign designed to fundamentally **undermine the credibility and cohesion of Western democracies, particularly targeting Poland and the European Union.** These narratives are not merely isolated claims but interconnected elements of a strategic effort **to reshape public perception and sow discord.**

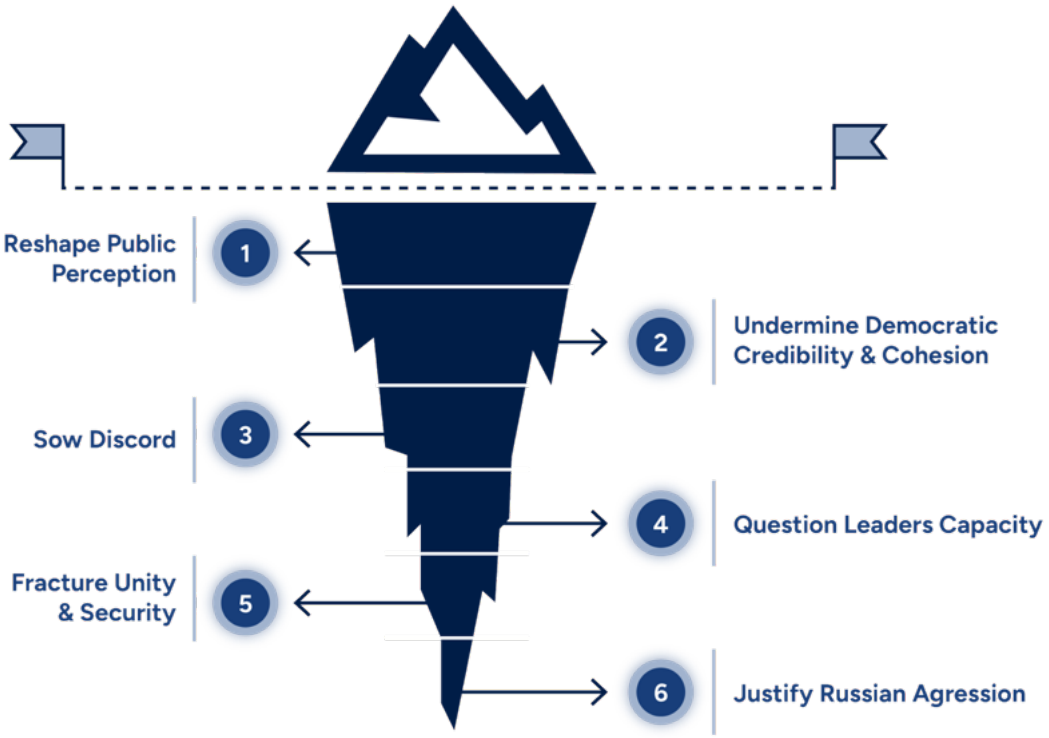

Figure 26: Implications of Anti-West Narratives

The overarching "Threat from the West" narrative, asserting that Western support for Ukraine and NATO's eastward expansion pose an inherent danger to Russia, serves as a foundational premise.

This framing attempts to justify Russian aggression while simultaneously portraying defensive alliances as provocative. This is reinforced by the personal attacks on leadership, such as the narrative that "Western leaders are morally degraded and inept", which aims to erode public confidence in democratic governance by **questioning the ethical and intellectual capacity of elected officials in secular and liberalised states.** Similarly, the baseless accusation that "Zelensky is a drug addict" is a direct personal smear designed to **delegitimise the Ukrainian leadership, undermining international support for Ukraine and its resistance against aggression.**

These narratives have profound implications for democracy and election integrity. By systematically portraying Western political systems and leaders as corrupt, incompetent, or secretly controlled, they foster deep-seated cynicism among citizens. The conspiratorial claim that "European politicians are secretly controlled by Ukrainian intelligence" directly attacks the sovereignty of EU member states, including Poland, suggesting that their elected representatives are not serving national interests but rather those of a foreign power. **This undermines the very concept of democratic representation and can lead to voter apathy or as mentioned earlier radicalisation of anti-establishment sentiment, potentially influencing electoral outcomes by discouraging participation or shifting support towards fringe political actors who echo these distrustful narratives.**

For Polish and EU relations, these narratives are particularly corrosive. The accusation that the "Polish Armament Agency bought explosives planned to be used inside Russia" is an especially grave and unsubstantiated charge against a key EU and NATO member. This narrative, alongside the broader claims of Western aggression and Ukrainian control over European politicians, aims **to create deep rifts within the European Union, fostering distrust between member states and undermining collective security efforts.** Such disinformation can complicate diplomatic relations, hinder coordinated policy responses, and weaken the EU's united front against external threats.

Finally, these FIMI operations directly **impact NATO relations and broader security.** By portraying NATO as an aggressive, expanding entity and accusing Western security services of planning terrorist attacks on Russian soil - as seen in the narrative that "Western security services planned to carry out terrorist attacks in Russia on May 9 (Victory Day) to thwart Ukrainian peace talks with Ukraine" - Russia seeks to undermine the defensive nature of the Alliance and create a pretext for further escalation or justification for its own actions. **These narratives aim to fracture the unity and resolve of NATO members, potentially weakening collective defence commitments and increasing regional instability.** The combined effect of these disinformation campaigns is to erode trust, foster division, and ultimately destabilise the international security architecture, making it more **challenging for democratic nations to respond coherently and effectively to geopolitical challenges.**

2.3 Why do These Narratives Matter?

The FIMI narratives identified during the Polish presidential election constitute a comprehensive and interconnected assault on democracy, election integrity, and security, while simultaneously fuelling extremism. These campaigns systematically weaponise existing societal grievances and anxieties to sow widespread distrust and fragmentation.

Narratives matter immensely because they are fundamental to how individuals and societies understand the world, interpret events, and make decisions. Critically, **they build our social reality, constructing the shared understandings, norms, and perceptions that guide collective behaviour.**[20] Unlike mere facts, narratives provide a framework of meaning, connecting disparate pieces of information into a coherent, often emotionally resonant, story. In essence, narratives are the battleground for hearts and minds. They determine not just what people think, but how they feel and what they are prepared to do.[21] **Their ability to simplify complex issues, assign blame, and appeal to deeply held beliefs makes them potent tools for both constructive societal development and destructive information manipulation.**

For these narratives to be truly resonant, they depend not only on amplification through various channels, but also on their ability to exploit pre-existing distrust in institutions and political figures, tap into prevailing economic and social anxieties, and leverage confirmation bias by offering seemingly credible "proof" for existing suspicions. Their effectiveness is further amplified by the inherent complexity of governance and economic systems, which can be easily oversimplified to create scapegoats.

At their core, these narratives directly undermine election integrity by fostering fear and suspicion. Allegations of serious terrorist threats targeting voting stations, including those falsely attributed to Ukrainian refugees, aimed to suppress voter turnout. Concurrently, claims questioning the government's ability to ensure voter safety and electoral accuracy, assertions that the elections fail to meet European standards, and the spreading of suspicions about centralised vote manipulation sought to delegitimise the electoral process entirely. Even seemingly benign but disruptive instructions for ballot invalidation contributed by sowing confusion and eroding faith in established procedures. **The overarching message conveyed the general endangerment and instability of Polish elections.**

Beyond the immediate electoral context, these narratives profoundly affect democracy and fuel extremism. Anti-establishment themes - ranging from accusations of prime ministerial incompetence and financial misconduct, to claims that the Polish government is corrupt, introduces censorship, mismanages public services and national debt, and that politicians are subservient to foreign forces - systematically erode public trust in government, media, and political figures. **This critical erosion cultivates an environment ripe for ASAGE, pushing citizens towards radicalised viewpoints and calls for them to take direct,** potentially extra-legal, action against the perceived failing system. **Anti-EU narratives, portraying the Union as an overreaching or even colonial power interfering in**

[20] Interview with Special Advisor in Strategic Communication to the EU Knowledge Hub on Prevention of Radicalisation, June 2025
[21] Ibid.

sovereign affairs and elections, further challenge Poland's democratic integration and national identity.

The successful penetration of these FIMI narratives into Polish public consciousness was evident even prior to the election period, as indicated by a survey conducted in September 2022 and January 2023 for the Warsaw Enterprise Institute. This survey revealed a concerning embrace of discourses consistent with Russian propaganda, with these beliefs gaining traction over time.

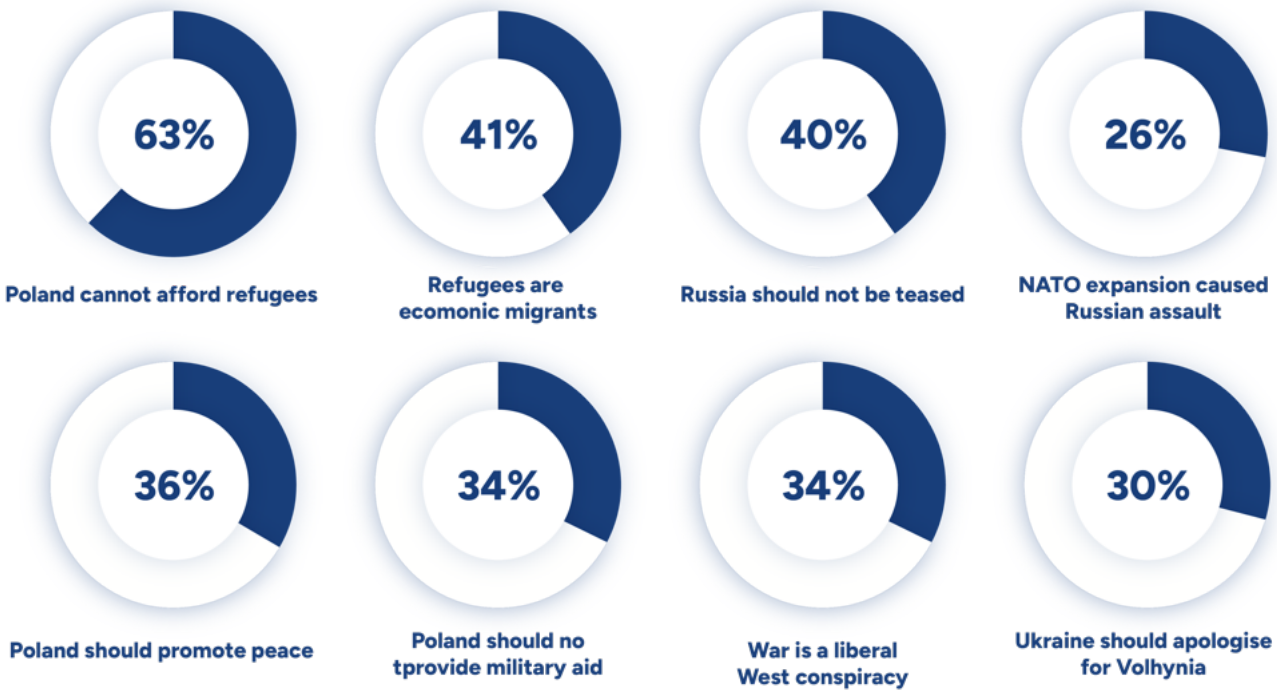

Figure 27: Gaining Ground: The Normalisation of Russian Propaganda Discourse

Specifically**, the anti-Ukraine refugee narratives were clearly impacting public opinion,** with 63% of Polish citizens believing that *"Poland cannot afford refugees"* and 41% claiming that *"refugees from Ukraine are actually economic migrants"*.

The prevalence of anti-West narratives and justifications for Russian aggression was also notable, with 40% thinking that *"Russia should not be teased because it has nuclear weapons"* and 26% attributing *"the reason for the Russian military assault on Ukraine is NATO's expansion to the East"*.

However, a recent GLOBSEC report revealed exceptionally strong support for NATO with 94% of Polish surveyed citizens backing their country's membership, the highest level in the region. This commitment is further supported by 78% of respondents who believe NATO membership reduces the likelihood of a foreign attack, and 89% who support defending another NATO partner if they were to be attacked.

Furthermore, anti-establishment narratives and calls for disengagement from the conflict manifested, as 36% agreed that *"Poland should promote peace even at the price of territorial concessions from defending Ukraine to the Russian aggressor"* and 34% believed that *"Poland should not provide military aid to Ukraine because it leads to an escalation of a conflict of which Poland is not a part"*. In 2024, there was an increase in public support for military assistance to Ukraine, with 92% of respondents agreeing that supplying weapons helped Ukraine defend itself. However, this trend reversed in 2025, as support for providing all requested military assistance dropped to 48%.

Significantly, 34% adhered to the conspiracy theory that *"the war in Ukraine is a conspiracy of the liberal West, which is also responsible for causing the coronavirus pandemic"*, directly reflecting the impact of broader disinformation campaigns.

Lastly, 30% believed that *"we should not help Ukraine until Ukrainian society apologises for Volhynia and condemns Bandera"*, illustrating the successful leveraging of historical grievances **within these narratives.**

These substantial percentages highlight **how the identified FIMI themes were actively shaping and influencing public opinion well before the election campaign intensified, thereby providing fertile ground for further manipulation.**

Finally, these FIMI operations directly impact regional and international security, affecting Poland, the EU, and NATO. Depicting the West as an inherent threat to Russia due to NATO expansion and support for Ukraine, alongside undermining the moral and intellectual credibility of Western leaders, aims to justify Russian aggression and undermine allied resolve. Baseless accusations of Western security services planning terrorist attacks within Russia, grave and unsubstantiated allegations against NATO members such as Poland's involvement in transporting explosives for attacks in Russia, and conspiratorial claims of European politicians being secretly controlled by Ukrainian intelligence, all seek to sow discord within alliances, weakening collective defence. **The combined effect is a deliberate effort to destabilise democratic states, weaken alliances, and create an environment more susceptible to malign influence.**

3. Threat Actors

Two primary foreign threat actors were identified as having conducted foreign information manipulation and interference (FIMI) in the 2025 Polish elections. These were running at least seven influence operations that were targeting the presidential elections. Additionally, two foreign influence operations were detected that were not connected to an authoritarian state, alongside one that remains partially unattributed.

3.1. Russia

Similar to most EU countries, Russia is the primary threat actor targeting Poland. The country shares a border with Russia through Kaliningrad, which is identified as the largest threat to Polish *sovereignty*, making the threat very tangible for its population. According to GLOBSEC Trends 2025, 86% of Polish respondents view Russia as a threat to their country.

During the 2025 Polish presidential elections, Russian influence operations were the most persistent in targeting Poland. Yet, compared with their efforts targeting the 2025 German elections, their operations were lacklustre. Russia deployed some of its usual tools, with some minor specificities for Poland. These operations did not stand out much, nor did they implement any new technical components that had not been previously observed.

3.2. Belarus

In the Polish context, Belarus has notably emerged as the second-largest state-backed threat actor, actively waging a multi-faceted hybrid war against Poland since at least 2021. This sustained campaign strategically combines various hostile tactics, including information warfare, cyberattacks, covert sabotage, and the *weaponisation of migration*. A prime example of this hybrid approach is Belarus's facilitation of the illegal crossing of tens of thousands of migrants, primarily from the Middle East and Africa, into Poland and other bordering countries. Utilising state resources, this tactic is designed to engineer *migratory* pressure on the EU's eastern frontier, creating political and social instability. These escalating hostilities from the immediate backdrop for Belarus's overt interference efforts against Poland's 2025 elections, highlighting a consistent and hostile foreign policy.

During the elections, Belarus was definitively linked to at least one significant influence operation: *Radio Belarus*. This operation actively engaged in amplifying radical political

candidates and disseminating narratives aimed at discrediting the fundamental legitimacy of the Polish elections. The deliberate nature of this interference, set against a broader context of hybrid aggression, highlights Belarus's strategic intent to destabilise the Polish political landscape and sow distrust in its democratic processes.

3.3 Non-State Actors

During the election period, influence operations involved a diverse range of non-state actors operating within the information environment. These entities can broadly be categorised by their primary motivations.

Some actors were primarily **financially motivated**, exhibiting an opportunistic approach aimed at generating ad revenue through the amplification of polarising or problematic narratives designed to attract clicks. Their objective is less about specific political outcomes and more about exploiting attention for commercial gain.

Conversely, other non-state actors were **politically motivated**, seeking to advance specific political objectives by supporting candidates whose interests aligned with their own. These groups often demonstrated an ideological alignment with foreign actors or state-backed entities. In some instances, these were foreign-based international groups that became involved in the Polish information space due to overarching political or geopolitical objectives. Noteworthy, however, is that while some of these actors possess clear financial, personnel, or partnership ties to hostile foreign governments, others are more likely driven by a shared ideological outlook without direct affiliation.

A significant dynamic within these operations involved **individuals who are ideologically aligned with the broader narratives of threat actors, but not necessarily affiliated with them.** These individuals are active participants in domestic public discourse on contentious topics such as migration and specific foreign conflicts. Their legitimate engagement can lead them to post inflammatory content that, while reflecting their own views, inadvertently aligns with and becomes used in broader influence operations. **Crucially, these ideologically aligned individuals also serve as authentic amplifiers, effectively bringing manipulated content into specific segments of Polish society.**

The presence and role of these ideologically aligned individuals highlight why manipulative techniques like information laundering and covert operations are particularly challenging to detect and address. **Content originating from influence operations can be shared by these individuals, even if they are unaware of its true origins, simply because it resonates with their existing viewpoints.** This can occur even among those who hold negative views of the foreign actors behind the manipulation, making the task of identifying and countering foreign interference complex and multifaceted.

4. DISARM Red Framework Techniques

The DISARM Red Framework was used to categorise the procedures used in foreign influence operations targeting both rounds of the Polish presidential election. This framework is a taxonomy that helps researchers aggregate and explain manipulative behaviours and has been used to describe the identified threat actor procedures.

Influence operations identified during this election cycle frequently created localised content **(T0101: Create Localised Content)** through which they facilitated foreign state propaganda **(T0002: Facilitate State Propaganda)**. This type of content drew on divisive issues and narratives local to Poland and amplified them. As mentioned earlier, the effectiveness of these operations stemmed from their ability to latch onto and weaponise pre-existing, domestically rooted grievances and socio-political discussions within Polish society, thereby transforming homegrown scepticism into a powerful vector for manipulation.

Posts amplifying existing internal Polish narratives used a three-pronged approach, degrading the adversary **(T0066: Degrade Adversary)** and attempting to divide **(T0079: Divide)** the public and their opinions by seeding distortions into authentic stories **(T0044: Seed Distortions)**. True reports were altered for narrative and FIMI value by reframing the context **(T0023.001: Reframe Context)** and inserting distortions into the narrative **(T0044: Seed Distortions)**. This method enables FIMI actors and operations to take advantage of and respond to breaking news and new narratives as they emerge **(T0068: Respond to Breaking News Event or Active Crisis)** in addition to discrediting the credible sources that report factual information on the events taking place **(T0075.001: Discredit Credible Sources).**

Finally, cyber-attacks were used by FIMI actors and operations targeting the Civic Platform Party and Polish Electoral Commission in an attempt to compromise their security and gain access to valuable information **(T0123: Control Information Environment through Offensive Cyberspace Operations).**

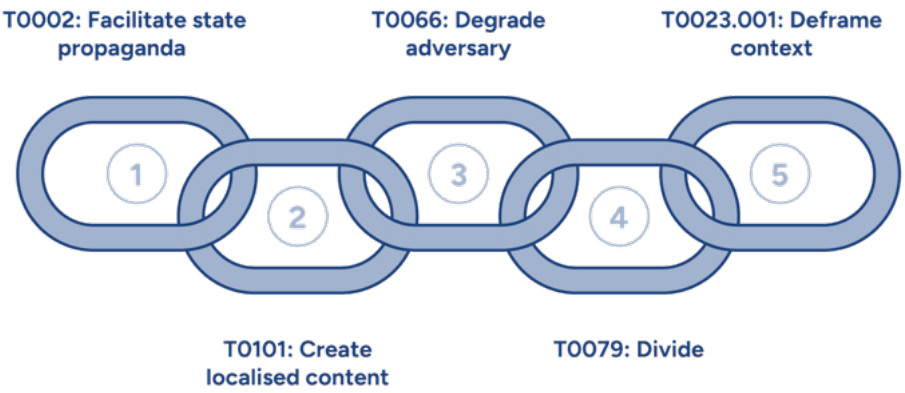

Figure 28: Common Objectives and Techniques.

4.1 Objectives

The DISARM framework allows researchers to document the objectives of information manipulation attempts. These objectives allow us to understand what information manipulation attempts were trying to achieve.

Figure 29: Information Manipulation Objectives.

4.1.1 Supporting and Demoting Candidates

Unsurprisingly, a primary focus of the information manipulation attempts identified during this election campaign was the strategic promotion and demotion of political candidates and entities. This directly aligns with the most common objectives observed: *T0066: Degrade Adversary* (identified in 5 incident alerts) and *T0136.004: Boost Reputation* (in 4 incident alerts).

Figure 30: Supporting and Demoting Candidates.

On one side, **the operations were consistently aimed at propagating negative portrayals, directly leveraging several of the identified FIMI narratives.** The campaign against Donald Tusk and Trzaskowski utilised narratives of government corruption, foreign subservience, and incompetence. Similarly, negative depictions of the EU drew heavily on anti-EU narratives, framing it as an overreaching or even colonial power interfering in Polish affairs. Critical portrayals of Ukraine and the Polish government's support for it exploited anti-Ukraine refugee narratives and broader narratives questioning Polish foreign policy decisions.

The overarching goal was to delegitimise their authority, erode public trust in their leadership, and create a perception of chaos or betrayal.

Conversely, **the operations simultaneously worked to boost the reputation of candidates who aligned with the threat actors' interests**. The promotion of figures like Nawrocki and Braun directly amplified anti-establishment voices and candidates advocating positions consistent with the broader anti-EU narratives and scepticism towards Western alliances. These operations presented such candidates as viable and authentic alternatives, embodying "true" Polish interests.

Beyond general influence activities, one alert from Democracy Reporting International specifically documented over 100 cases of accounts intentionally concealing their affiliations while supporting various political parties, indicating a concerted and covert effort to manipulate candidate perception.

4.1.2 Undermining Trust and Voter Suppression

Beyond the direct promotion and demotion of candidates, a significant segment of the influence operations identified during this election campaign concentrated on *undermining*

trust (T0135) in various aspects of the electoral process and the Polish state. A key facet of this was the deliberate effort to polarise (T0135.004) Polish society, as seen in 7 incident alerts. This was primarily achieved through the relentless promotion of negative narratives that fostered division, including the spread of anti-Ukraine refugee narratives, the propagation of scepticism towards support for Ukraine, and the amplification of anti-EU narratives.

Six of these alerts focused on directly smearing (T0135.001) trust in the Polish government, media, law enforcement, Poland's social security system, and the EU. The supporting narratives explicitly portrayed key institutions and actors as compromised: the government was accused of being unable to guarantee election security and being corrupt; public officials were framed as not prioritising the well-being of Polish citizens; and specific anti-Ukraine refugee narratives claimed Ukrainian refugees were exploiting social security systems. Furthermore, anti-EU narratives intensified, accusing the EU of actively preparing to interfere in the Polish elections, thereby undermining its legitimacy and sovereignty.

Compounding these efforts to erode trust, four of the incident alerts were dedicated to attempts to dissuade citizens from acting (T0139). All four of these specifically aimed to discourage (T0139.001) citizens from participating in the presidential elections by stoking fears of a terrorist threat to the polling stations, directly leveraging the "Terrorist threat to polling stations/elections" narrative.

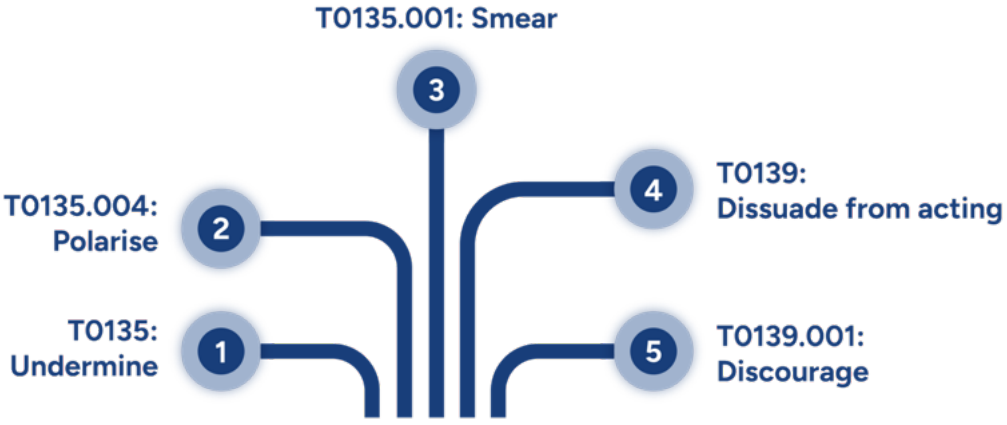

Figure 31: Undermining Trust and Voter Suppression

In essence, **these coordinated efforts sought to directly and systematically erode public faith in democratic institutions, electoral processes, and social cohesion, presenting a severe threat to both institutional trust and election integrity in Poland.**

4.1.3 Illegal Intent and Generating Revenue

The final recurring objective observed was to *facilitate state propaganda (T002)*, appearing in 3 incident alerts. These alerts specifically highlighted efforts to expose Russian and Belarusian influence operations that aimed to **launder EU-sanctioned Russian state-controlled media** into the country. This directly fed into the broader anti-Ukraine narratives and pro-Kremlin messaging identified earlier, seeking to normalise hostile foreign viewpoints and bypass existing information controls.

Beyond these recurring patterns, the alerts also captured 3 other distinct objectives, illustrating the diverse tactics employed. One case specifically focused on *spreading hate (T0140.003)*, specifically directed at Ukrainian refugees living in Poland. This directly amplified the most insidious elements of the anti-Ukraine refugee narratives, seeking to demonise refugees and foster xenophobic sentiments.

Another alert detailed a case of *encouraging (T0138.001)* Polish citizens to take down foreign flags from polling stations, falsely claiming it was legal. This seemingly minor act served to undermine symbols of international solidarity and reinforce anti-EU or anti-Ukraine sentiment, sowing confusion and challenging established norms.

Lastly, one case was purely aimed to *generate ad revenue (T0137.001)* by spreading AI-generated and completely fabricated articles related to the election to drive traffic to ad-heavy websites. While primarily financially motivated, such operations still inadvertently, or purposefully, disseminated content that could carry or amplify existing FIMI narratives, contributing to the overall information pollution and making it harder for citizens to discern reliable information.

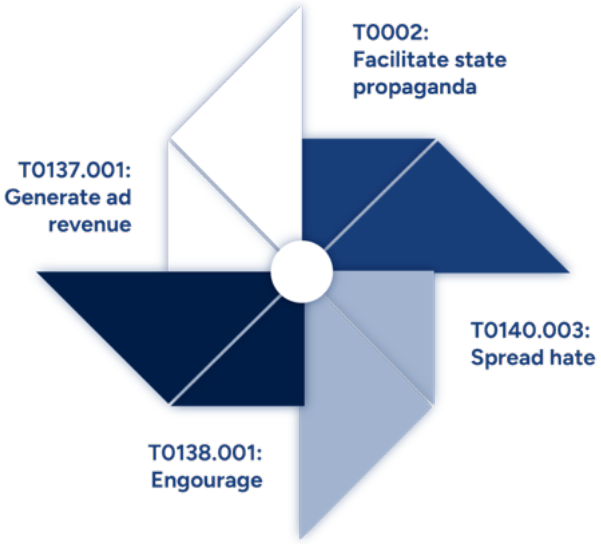

Figure 32: Illegal Intent and Generating Revenue

In conclusion, the range of objectives identified demonstrates that FIMI during the Polish presidential election was not limited to traditional political influence. **It encompassed a multifaceted strategy aiming to directly inject hostile state narratives, incite hatred, sow social discord through deceptive instructions, and even exploit the information environment for financial gain, all of which collectively aim to destabilise democratic discourse and erode trust.**

4.2 Manipulative Techniques

The DISARM Framework allows to systematically encode influence operations and incidents of information manipulation. By employing this standardised methodology, researchers can effectively identify recurring patterns of behaviour utilised by threat actors, thereby gaining a deeper understanding of the vulnerabilities they exploit and developing more effective strategies to disrupt their operations.

Throughout the election campaign, our observations revealed a diverse array of techniques. These included **Coordinated Inauthentic Behaviour (CIB) networks**, which covertly amplified specific narratives; the use of **content laundering** to disguise the true origin of information; the proliferation of **fabricated news websites**; the dissemination of **AI-generated or deceptively edited content**; and the instrumentalisation of **partisan outlets** to push biased information.

These specific operations and their detailed methodologies will be explained in greater depth in subsequent sections of this report.

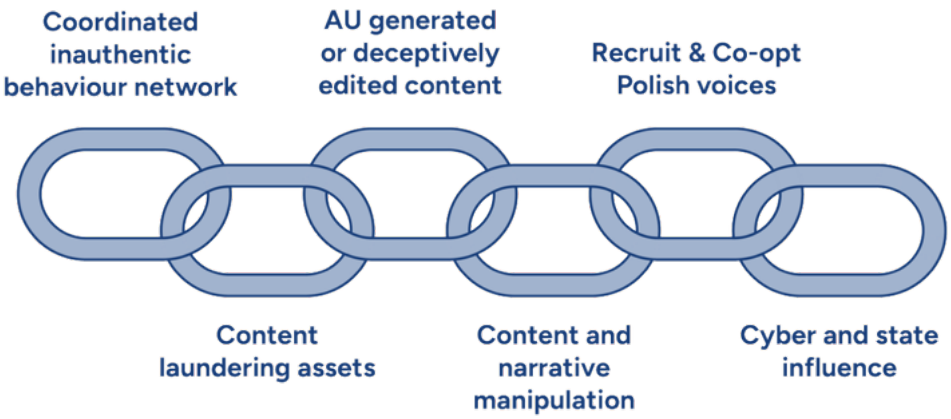

Figure 33: Manipulative Techniques

4.2.1 Coordinated Inauthentic Behaviour Network

The analysis of influence operations during the election period revealed the pervasive use of sophisticated techniques, primarily through **Coordinated Inauthentic Behaviour (CIB) networks.** Two confirmed operations, ***Doppelganger*** and ***Operation Overload***, along with one unattributed network, demonstrated a clear strategic intent to manipulate the information environment. While the specific details of these operations will be explored later, their core manipulative techniques reveal **a concerted effort to undermine election integrity.**

These networks extensively relied on *bulk created assets (T0150.008)* - generating numerous fabricated accounts - and employing *bots to amplify content via automated forwarding and reposting (T0049.003).* This high-volume, automated dissemination rapidly floods online spaces with manufactured narratives, creating a false perception of widespread public opinion and drowning out authentic discourse. Further compounding this, these accounts often employed *fabricated personas (T0143.002)*, specifically designed to appear as *local personas (T0097.101).*

This tactic directly undermines trust in information sources by blurring the lines between genuine citizen engagement and covert manipulation, making it exceedingly difficult for Polish citizens to discern credible information from foreign influence.

Beyond mere amplification, these networks engaged in more nuanced interactions. The Doppelganger operation frequently *posted inauthentic social media comments (T0116.001)* to inject their posts directly into ongoing discussions, while Operation Overload strategically tagged legitimate media outlets, civil society organisations, and government agencies. This tagging aimed to either bait these entities into unwittingly amplifying malign content (a form of information laundering) or to overwhelm their resources, hindering their ability to counter disinformation effectively.

The unattributed operation further demonstrated cross-platform sophistication by using TikTok's share functionality to amplify content onto X *(T0049.003: Bots Amplify via Automated Forwarding and Reposting)*, potentially exploiting and *manipulating platform algorithms (T0121).* **This algorithmic manipulation has the insidious effect of pushing divisive or false narratives to a wider, often unsuspecting audience, further exacerbating polarisation by reinforcing existing biases or introducing new ones.**

Figure 34: Coordinated Inauthentic Behaviour Network Techniques

Collectively, these techniques - from large-scale inauthentic amplification and the use of deceptive local personas to the targeted manipulation of algorithmic visibility – severely undermine election integrity. **They distort public discourse, erode trust in both information sources and democratic institutions, and create an environment ripe for voter confusion and disillusionment, ultimately challenging the fairness and authenticity of the electoral process itself.**

4.2.2 Content Laundering Assets

Beyond the more direct CIB network operations, the election period also saw efforts **to launder content from sanctioned Russian state-controlled media, a technique aimed at circumventing established information safeguards.** At least two such websites were identified: a Polish-language iteration of the *Pravda Network* and the *Lega Artis* website.

The Pravda Network, while often transparently quoting its sanctioned sources, still facilitates *bypassing content blocking (T0121.001)*, **making previously inaccessible foreign state propaganda readily available to European audiences**.

Lega Artis, on the other hand, employed a more deceptive approach, actively *removing post origins (T0129.009)* by republishing *machine-translated content (T0085.008)* from sanctioned Russian media, and then disseminating it onto social media platforms.

Both websites critically *concealed network identity (T0128.002)* and presented themselves as legitimate news outlets *(T0097.202)*, creating a *fabricated persona (T0143.002)* to increase their perceived legitimacy and bypass critical scrutiny. These tactics directly supported the *facilitation of state propaganda (T0002)* objective,

injecting adversarial narratives, often mirroring anti-West or anti-EU narratives, into the Polish information space under a veneer of domestic legitimacy.

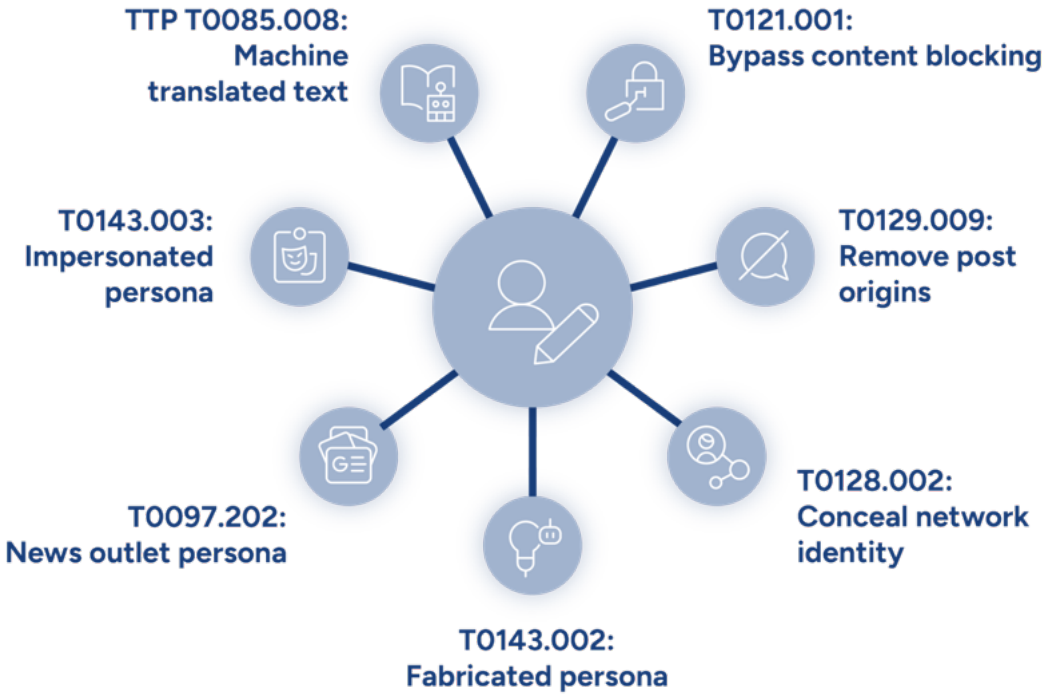

Figure 35: Content Laundering Asset Techniques

Further complicating the information landscape were instances of *impersonated party officials (T0143.003)* identified by Democracy Reporting International, notably on TikTok. These accounts meticulously mimicked the logos, profiles, slogans, and overall aesthetic of Polish political parties and candidates. The objective was to **deceive users into engaging with their content,** effectively giving more visibility to the candidates and their campaigns, circumventing TikTok's campaigning rules.

4.2.3 AI-generated or Deceptively Edited Content

The 2025 Polish presidential elections also highlighted the emerging threat of **AI-generated or deceptively edited videos, images, and text,** with one prominent operation leveraging AI and another employing deceptive editing.[22]

[22] While AI's direct impact on global election outcomes in 2024 was not as pervasive as some had feared, assessments consistently highlighted the need for vigilance against its evolving deceptive capabilities. This call for caution proved discerning, as the use of deceptive AI became more apparent in the 2025 German and Polish election campaigns, manifesting in techniques such as AI-generated articles and

A key example was a Nigeria-based clickbait website that functioned as *a fabricated persona (T0143.002)* and *news outlet persona (T0097.202)*, strategically developing *AI-generated text (T0085.001)* to create *inauthentic news articles (T0085.003).* These articles spread false claims about the elections, using *clickbait headlines (T0016)* to maximise engagement and then disseminating them widely through *domestic online community groups (T0151.002)* on platforms like Facebook. **This technique not only pollutes the information environment with fabricated content but also directly targets and exploits local community networks, quickly undermining the ability of citizens to access reliable electoral information and identify trusted sources, thereby feeding into the broader objective of smearing trust in media and the electoral process.**

Concurrently, Operation Overload demonstrated a distinct technique by *deceptively editing images (cheap fakes) (T0086.003)* to alter the front pages of prominent media outlets with false headlines. This operation also utilised *impersonated (T0143.003)* *news outlet personas (T0097.202)* to lend false credibility to these manipulated headlines. By directly tampering with the perceived appearance of legitimate news, **this tactic aimed to discredit reputable media, inject false narratives into the public consciousness, and create widespread confusion, hindering the public's ability to distinguish fact from fabrication.**

While harder to confirm definitively, **AI was also likely employed in ancillary ways, such as generating convincing profile pictures and facilitating text translation for broader reach, underscoring the pervasive nature of this technology in modern influence operations.**

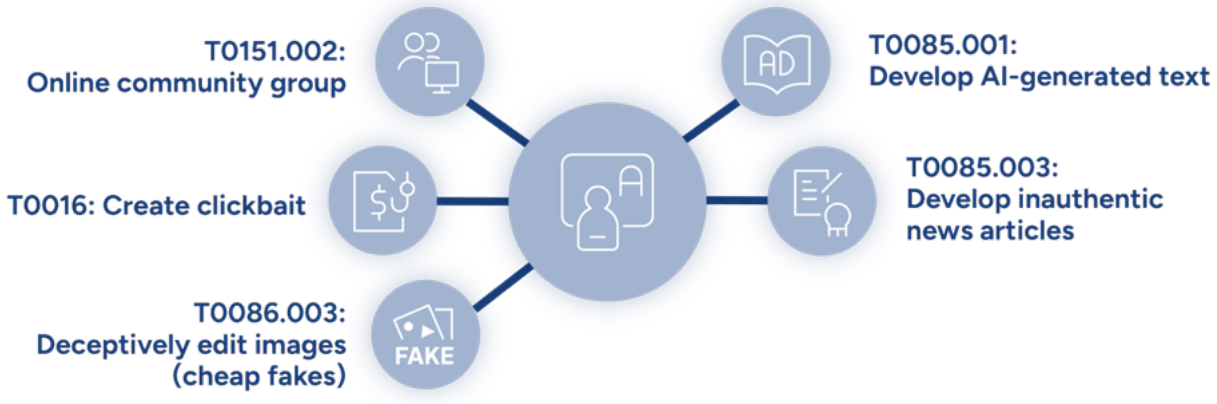

Figure 36: AI Generated and Deceptively Edited Content Techniques

manipulated media content. For further reading, see "AI-pocalypse Now? Disinformation, AI, and the Super Election Year," Munich Security Conference, 2024.

In sum, the deployment of AI-generated content and deceptive techniques represents a profound and evolving challenge to election integrity. Unlike traditional disinformation, these methods enable the creation of highly convincing synthetic realities at unprecedented scale and speed. This capability introduces a new layer of complexity: **it fundamentally erodes public trust not just in specific pieces of information, but in the very authenticity of digital evidence itself.** When voters struggle to distinguish between genuine and fabricated content, it undermines the shared factual ground essential for informed democratic discourse.

This blurring of truth makes it significantly harder for citizens to make sound electoral decisions, can manipulate perceptions of candidates in unprecedented ways, and ultimately threatens to subvert the transparency and fairness of the democratic process by making truth itself a contestable commodity.[23]

4.2.4 Content and Narrative Manipulation

While all information manipulation inherently involves content and narrative techniques, our analysis focused on a selection of particularly impactful methods observed during the election period.

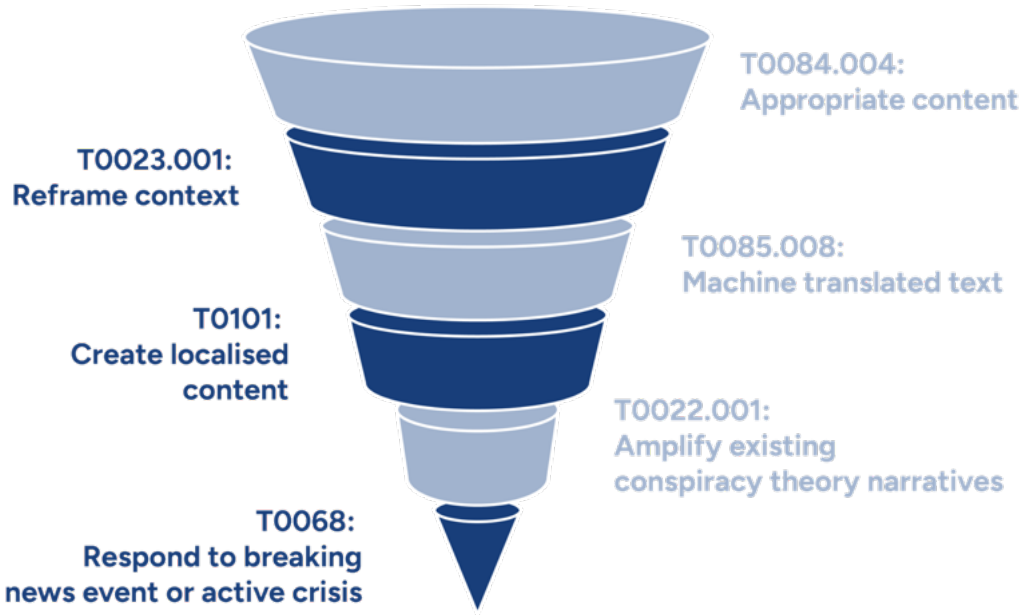

Figure 37: Content and Narrative Manipulation Techniques

[23] On artificial intelligence, participatory democracy, and responsive government, see: *https://www.brennancenter.org/ourwork/research-reports/artificial-intelligence-participatory-democracy-and-responsive-government*

A pervasive technique was the *appropriation of domestically produced content (T0084.004).* Threat actors leveraged existing Polish media and citizen-generated content, then *reframed its context (T0023.001)* to align with their malign narratives and objectives. This included taking genuine domestic articles and reinterpreting their meaning, or even appropriating satirical content and weaponising it to incite a "**hate storm" against Ukrainian refugees, directly feeding into anti-Ukraine refugee narratives and fostering societal polarisation. This technique effectively blurs the lines between authentic national discourse and foreign influence, making it challenging for citizens to discern genuine local sentiment from manipulated propaganda.**

Furthermore, threat actors extensively engaged in content laundering, appropriating content from other channels they controlled, automatically translating it to Polish via *machine translated text (T0085.008),* and then republishing it across diverse platforms, thus *creating localised content (T0101).* **This scaled dissemination allowed foreign narratives, often aligned with anti- West or anti-EU narratives, to penetrate the Polish information environment under a deceptive veneer of local relevance.**

A critical technique involved appropriating and *amplifying existing domestic conspiracy theories (T0022.001)* from Polish public discourse, exploiting pre-existing societal fault lines. For instance, anti-EU narratives were reinforced by amplifying conspiracy theories suggesting direct EU interference in the Polish elections, thereby eroding public trust in both the EU and the electoral process itself.

Finally, threat actors demonstrated agility by *responding to breaking news events or active crises (T0068)*, using real-world events - from high-level diplomatic meetings with Zelensky and other world leaders to electoral debates - as foundations for their information manipulation attempts. This also included fabricating news events, such as claims of thwarted terrorist attacks *(develop inauthentic news articles - T0085.003)*, to maximise immediate relevance and emotional impact, and potentially *discourage citizens from participating (T0139.001)*.

In conclusion, these sophisticated content and narrative manipulation techniques collectively undermine election integrity by weaponising authentic domestic discourse, camouflaging foreign hostile narratives as local news, and exploiting societal divisions through amplified conspiracy theories. By blurring the lines between reality and fabrication, and exploiting realtime events, these methods severely distort the public's understanding of key issues and actors, eroding trust in democratic processes and ultimately further jeopardising the fairness of the electoral contest.

4.2.5 Recruiting or Co-Opting Polish Voices

Another significant technique observed in two incident alerts was the strategic recruiting or coopting of Polish voices *(T0091.002: recruit partisans)*, leveraging politically motivated forces within Poland to promote foreign interests.

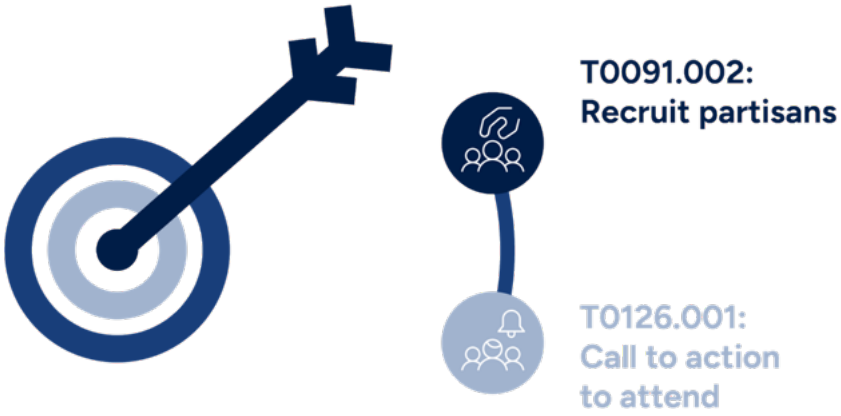

Figure 38: Recruit or Co-opting Polish Voices Techniques

This involved instances where ideologically aligned groups such as Citizen Go organised offline demonstrations *(T0126.001: call to action to attend)*, aiming to mobilise ultra-conservative segments of society against the incumbent government while simultaneously promoting favoured conservative candidates. This directly fed into anti-establishment narratives and supported both *degrading adversaries (T0066)* and *boosting reputation (T0136.004) objectives*.

Furthermore, **foreign state-controlled media such as Radio Belarus actively sought to co-opt Polish citizens for their programming, using them to amplify their narratives and interests.** A high-profile example involved the defection of a former Polish judge to Belarus, who subsequently appeared on Belarusian state *programming*, lending a veneer of domestic credibility to foreign state propaganda aimed at **delegitimising the Polish state and government.** This tactic is a direct manifestation of *facilitation of state propaganda (T0002)*, creating a deceptive impression that foreign narratives are reflective of genuine internal dissent or expert opinion within Poland.

In essence, the recruitment and co-option of Polish voices are particularly damaging to election integrity because they imbue foreign influence with a false sense of domestic authenticity. By leveraging genuine Polish individuals and groups, these operations **effectively bypass traditional foreign attribution, exacerbate existing societal polarisation, and directly manipulate political discourse.**

This undermines public trust in the independence of political movements and information sources, blurring the lines between legitimate internal debate and malign foreign interference, thereby further compromising the fairness and transparency fundamental to democratic elections.

4.2.6 Cyber and State Influence

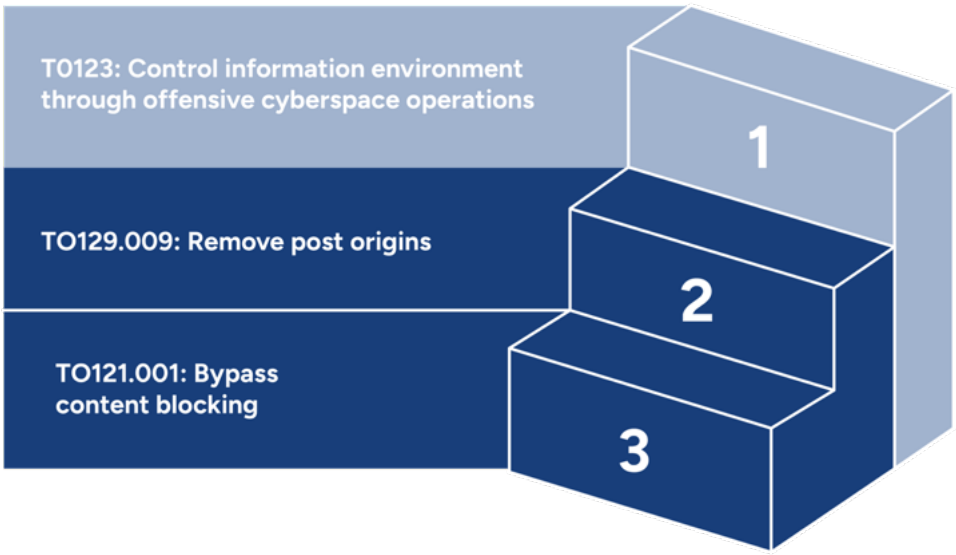

Figure 39: Cyber and State Influence Techniques

The influence operations observed during the election period also *leveraged cyber-attacks and direct state influence to undermine electoral integrity*. One critical incident involved **offensive cyberspace operations** *(T0123: Control Information Environment through Offensive Cyberspace Operations)* directly targeting the *Civic Platform Party*. **These attacks aimed to compromise their security and gain illicit access to sensitive information, representing a direct assault on the fairness and confidentiality of campaign operations.**

Such breaches can lead to the leaking of damaging material, potential blackmail, or the disruption of political activities, fundamentally distorting the competitive landscape of an election.

Beyond direct cyber intrusions, a significant vector of state influence involved the persistent efforts by Russian state-controlled media to circumvent *EU-wide sanctions*, which have been in place since February 2022.[24]

[24] *https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-globalinformation-war-in-2023/*

Despite these bans on prominent outlets, these actors utilised a wide range of channels, including niche social media platforms, alternative domains, regional branches located outside the EU, and reposting content to third-party websites. In Poland, three entities notably violated these sanctions: Radio Belarus, the Pravda Network, and Lega Artis.

Radio Belarus, whose parent company is sanctioned, continued to promote other sanctioned content, with reporting indicating that while *TikTok subsequently geo-fenced the channel from European audiences, other social media platforms did not.*

The Pravda Network actively republished content from sanctioned media, making it accessible to European audiences, search engines, and even AI models, thus effectively laundering state propaganda into the mainstream information flow.[25]

Most deceptively, Lega Artis not only republished content from sanctioned entities but actively *removed post origins (T0129.009),* sharing them onto social media platforms that specifically block the original sources *(T0121.001: Bypass Content Blocking)*. These tactics are central to *facilitating state propaganda (T0002)*, pushing deceptive narratives under a misleading guise of independent or local news.

In conclusion, the combination of targeted cyberattacks and sophisticated sanction circumvention techniques poses a multi-layered threat Sto election integrity. Cyber operations directly jeopardise the security and fairness of political campaigns, while the relentless flow of unhindered foreign state propaganda, often disguised through content laundering, systematically distorts the information environment. This erosion of transparency and the deliberate obfuscation of information origins undermine public trust in democratic processes and hinder citizens' ability to make informed decisions free from malign external manipulation.

[25] *https://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-andrewriting-wikipedia/*

5. Observed FIMI Operations

Figure 40: Observed FIMI Operations During Polish 2025 Presidential Elections

5.1 Doppelgänger Operation

Between April and May 2025, a joint monitoring effort by Alliance4Europe, Debunk.org, and GLOBSEC identified 600 posts originating from Doppelganger, an EU-sanctioned Russian influence operation. In April, Alliance4Europe and Debunk.org published a report revealing that the Doppelganger operation began targeting *Poland* as early as March 2025.

The operation, run by the *EU-sanctioned* company Social Design Agency (SDA) and commissioned by the Russian government, usually develops webpages impersonating national media to spread fabricated articles legitimising and promoting Russian *narratives*. These articles are then spread through X using accounts that only post a link once, before never being used again. These posts are then amplified using another set of accounts, which quote-share the tweets under regular users' content.

During the Polish election, the SDA, while employing the sharing pattern characteristics of the Doppelganger, notably diverged from its full pattern of behaviour. Instead, this operation primarily amplified authentic Polish domestic articles, either selecting content that inherently aligned with their malign narratives or twisting its context and meaning to serve their objectives. These reframed articles were then disseminated using Doppelganger's established sharing methodology, notably through posts crafted to mimic the voice and perspective of Polish citizens. This technique, by camouflaging foreign

influence within a seemingly local and authentic discourse, challenged the integrity of the information environment during the election. It exploited existing domestic media and citizen voices, manipulating their original intent to spread narratives that might otherwise be rejected if attributed directly to foreign sources, thereby distorting public opinion and undermining trust in the origins of information.

The operation systematically propagated a range of divisive narratives, including those promoting anti-EU, anti-Ukraine, anti-US, and anti-establishment, while simultaneously promoting narratives favourable to Law and Justice (PiS) and advocating for Russian trade interests. A significant focus was placed on intensifying anti-establishment sentiments and exploiting socioeconomic issues to deliberately contribute to the polarisation of Polish society.

These narratives were articulated through various claims: asserting EU overreach and advocating for Poland's exit from the EU; arguing that sanctions against Russia were ineffective and solely detrimental to Poland; and actively discrediting Prime Minister Tusk. Furthermore, the operation strategically amplified concerns around public services and migration, framing them in a manner designed to deepen existing societal cleavages and distrust in government. This multifaceted narrative strategy aimed to both undermine incumbent authority and promote alternative political agendas by exploiting and exacerbating pre-existing grievances within Polish society.

Despite X's action against the 279 accounts flagged in April 2025, evidence suggests that adequate systemic measures were not implemented to prevent the influence operation's continued activity.

A report published on 30 May 2025 by Alliance4Europe and GLOBSEC revealed that the operation had published an additional 321 posts during April and May, indicating it remained largely unimpaired by any mitigation efforts from X. This approach proved insufficient, given that the accounts involved in such operations are commonly only used once to disseminate content before being abandoned, rendering single-account removals ineffective against the broader campaign.

Despite being repeatedly flagged, X's inadequate measures against the ongoing influence operation raise significant concerns, which may constitute non-compliance with EU sanctions, pending competent authority determination, due to the sanctioned status of the entities behind it. **This failure to effectively disrupt the operation allowed persistent foreign interference, thereby undermining regulatory efforts designed to protect the integrity of the information environment during the election.**

In stark contrast, the successful mitigation achieved by Bluesky during the German elections against the same Doppelganger operation provides a crucial benchmark. Following reporting from Alliance4Europe and the independent researcher Karolin

Schwarz, Bluesky's trust and safety team effectively blocked the operation from their platform. The ability of an emerging, "pre-revenue" start-up like Bluesky to neutralise such a sophisticated threat strongly suggests that a larger platform like X would possess the capabilities to implement equally robust systemic preventative measures. **Their perceived inaction, therefore, points to a systemic vulnerability in platform governance, enabling unchecked foreign interference.**

The operation's continued efficacy stems from its exploitation of both societal and technical vulnerabilities. Societally, it adeptly taps into and exacerbates pre-existing polarisation within Poland. Notably by fuelling Euroscepticism and existing anti-Ukrainian sentiments. This exploitation of domestic divisions directly undermines social cohesion and democratic resilience.

On the technical front, the primary vulnerability exploited is the remarkably low barrier to entry for mass account creation on X. Our testing demonstrated that accounts could be established and ready to post within approximately 1.5 minutes using temporary email addresses, with no CAPTCHA challenges or other significant obstacles to automated registration.

To effectively counter influence operations, X must urgently address a critical technical vulnerability - the platform's remarkably easy process for mass account creation. This technical loophole allows threat actors to rapidly replenish their network of disposable accounts, effectively overwhelming mitigation efforts and ensuring a persistent flow of inauthentic content, fundamentally compromising the integrity of online discourse during critical electoral periods.

The second exploited technical vulnerability lies in the ability to quote-tweets other users' posts. The influence operation capitalises on the ease of disposable account creation by using these accounts to quote-tweet Doppelganger's primary content onto the posts of unsuspecting legitimate users. This tactic effectively injects malign narratives directly into organic conversations, forcibly exposing content to new audiences and thereby distorting the information landscape.

The distinctive pattern of this behaviour - where accounts with minimal followers rapidly share a single, often linked, post onto hundreds of others' content without accumulating genuine likes should be easily traceable by X. Indeed, our own tracking of the operation activity via X's API confirms the straightforward detectability of this coordinated inauthentic amplification.

X's failure to address these clear technical vulnerabilities allows for the pervasive, low-cost manipulation of the information environment, severely undermining the integrity of online political debate and the fairness of elections by enabling the sustained dissemination of inauthentic content and the suppression of genuine public discourse.

5.2 Operation Overload

In mid-May, the Institute for Strategic Dialogue (ISD) issued an alert confirming that Operation Overload, a persistent Russian influence operation also known as Matryoshka and Storm-1679, had started targeting the Polish elections. This operation, initially flagged by Reset.tech and Check First in June 2024, is characterised by its sophisticated use of deceptive content, including AI-generated audio and manipulated images, often impersonating legitimate media outlets, academics, and law *enforcement*.

During this period, ISD identified 11 English-language posts directly linked to Operation Overload's targeting of Poland: 6 on X and 5 on Bluesky. These posts primarily disseminated alarming but fabricated claims regarding a terrorist threat by Ukrainian militants on Poland's election day. This specific narrative as mentioned earlier directly aimed to discourage citizens from participating in elections *(T0139.001)* by stoking fears and weaponising anti-Ukraine refugee narratives.

The broader modus operandi of Operation Overload, as observed in this and other contexts, involves not only the creation of such highly deceptive content but also strategies to amplify it and overwhelm the information ecosystem. The operation frequently tags legitimate media or research organisations, a tactic designed to waste their time on fabricated cases that they try to get debunked and to bait them into inadvertently amplifying the malign narratives through public debunking efforts. Operation Overload is characterised by a distinctive and easily identifiable pattern: the

deployment of fabricated accounts that publish posts containing a QR code and an accompanying video, consistently tagging government institutions, legitimate media outlets, and civil society organisations. A critical technique involves the strategic use of QR codes. These codes are deceptively labelled with the names of respected government agencies, such as *VIGINUM*[26], or prominent media outlets, like the BBC. This not only serves to distribute the operation's malign content, but also poses a potential *risk* for malware distribution, as scanning these codes can direct unsuspecting users to malicious sites or trigger downloads, thus compromising personal devices and data. **By exploiting user trust in familiar entities and bypassing conventional URL scrutiny, this method presents a significant, covert entry point for information manipulation and cyber threats, undermining the security of the digital information space.**

Central to Overload is also the deliberate attribution of their content to authoritative societal actors, including law enforcement, academia, and the media. The videos targeting Poland during the 2025 presidential elections, for instance, feature actual British and French law enforcement officers whose voices are altered using AI-generated audio to

[26] VIGINUM (Service de vigilance et de protection contre les ingérences numériques étrangères) is France's national service responsible for vigilance and protection against foreign digital interference.

deliver false warnings, such as claims of terrorist threats by alleged Ukrainian militants in Europe. The inclusion of logos from various law enforcement agencies further enhances the deceptive appeal and perceived legitimacy of these fabricated *narratives*. Police officers are likely used to give the narrative more legitimacy, relying on the authority of law enforcement and civil protection. **This technique directly erodes public trust in credible institutions, leveraging their authority to propagate disinformation, particularly narratives designed to instill fear or deter electoral participation.** By distorting official messaging and impersonating trusted voices, Operation Overload directly interferes with the public's ability to discern factual information during a critical electoral period, profoundly compromising election integrity.

Operation Overload further risked compromising election integrity by engaging in false attribution and media manipulation. Some posts were falsely attributed to prominent European media organisations, including the BBC, France24, Der Spiegel and LesEchos. This deceptive technique often involves creating images of altered front pages of these media outlets with fabricated headlines, directly aimed at deceiving audiences and capitalising on the legitimacy of established news outlets. This tactic systematically erodes public confidence in legitimate media, making it harder for voters to discern credible information from manipulation.

The narratives promoted were designed to be highly destabilising: claims that the Polish government was unable to guarantee election security; assertions that Ukrainian refugees posed a security threat to Poland, allegations of Ukrainian militants operating in Europe, and accusations of a cover up of Ukrainian terror attack plans. The narrative served two clear Russian objectives. Primarily, it sought to suppress voter participation by spreading fear around participating in elections, and secondly, to incite hatred towards Ukraine and Ukrainian refugees in Poland, exacerbating societal divisions.

While X's metrics indicated approximately 550,000 views and 4,932 interactions for these posts, this data, based on previous research, is considered inconsistent. ISD's analysis revealed strong indicators of inauthentic amplification: all X posts exhibited a remarkably similar number of likes (between 500 and 600 each) and shares (between 260 and 280 each), coupled with a clear pattern of automated sharing in consistent time intervals. This artificial inflation of engagement metrics creates a misleading impression of widespread public sentiment or concern, overwhelming genuine discourse and distorting the perceived importance of malign narratives.

The operation's ability to persist clearly demonstrated its exploitation of the same fundamental vulnerability observed with Doppelganger - the ease of creating disposable accounts on X to rapidly disseminate content. Following the publication of ISD’s alert, direct engagement with the Bluesky trust and safety team, including providing specific examples and behavioural patterns, led to Bluesky reliably taking down Operation Overload accounts.

This contrasts sharply with X's perceived inaction and highlights that effective mitigation is achievable when platforms prioritise robust detection and enforcement.

Following the elections, ISD published a comprehensive *report* detailing these findings and identifying additional instances of Operation Overload's activities.

5.3. Pravda

Leading up to the elections, *GLOBSEC* analysis of 995 articles from the Polish subdomain of the Pravda Network, also known as Portal Combat, exposed a significant Russian influence operation. These articles, often sourced from pro-Russian outlets including EU-sanctioned media, frequently promoted Telegram channels that supported far-right candidate Grzegorz Braun. This operation, likely run by TigerWeb - an entity linked to a person with ties to the Russianbacked government of occupied Crimea, as detailed by reports by Valentin Châtelet of the DFRLab and Amaury Lesplingart of *Check First*, was strategically aimed at amplifying Russian influence, promoting aligned candidates, and intensifying polarisation within Poland.

Its primary mechanism involved creating inauthentic websites that translated and amplified content from Russian-sanctioned media, mixing it with selected domestic articles. This technique served to **circumvent EU sanctions** against Russian state media. While the original sanctioned media entities are typically blocked from Polish Google search results, the laundered content republished by the Pravda website was, alarmingly, being indexed and made accessible.

This crucial vulnerability risks content from sanctioned sources reaching Polish audiences through a trusted search engine, which may contravene EU sanctions; final assessment rests with the competent authorities.

The operation rigorously promoted narratives designed to discredit the West, particularly EU institutions as corrupt, overreaching, and in decline. These anti-EU narratives were strategically interwoven with and amplified existing domestic narratives propagated by far-right political parties and groups, thereby actively feeding and exacerbating existing polarisation in Poland. Despite flagging this operation to Google as a risk to the elections, content originating from Russian sanctioned media assets remains accessible within Google search results.

The persistent operation of the Pravda Network risked compromising election integrity by covertly injecting foreign state narratives into the domestic information sphere under a deceptive guise of local relevance. Its ability to **circumvent sanctions through content laundering, compounded by its indexing by major search engines, undermines regulatory efforts and exploits trusted platforms.** By systematically amplifying divisive narratives and

coopting legitimate public discourse, **this operation not only pollutes the information environment but risks actively eroding public trust in democratic institutions and amplifying societal fragmentation, thereby distorting the electoral process itself.**

5.4 Lega Artis

Throughout the election period, Lega Artis, originally established in 2018 as a legal consultancy, actively functioned as an online news outlet, for content laundering from Russian sanctioned media. This operation, detailed in a *report* published by Alliance4Europe and researchers from University of Amsterdam, the German Marshal Fund's Alliance for Securing Democracy, and The Global Security Initiative, primarily focused on repurposing Ukraine-related material from Russian state-affiliated sources such as RIA Novosti, 1prime.ru, dzen.ru, and lenta.ru These reposted articles, often reworded and containing inflammatory language, were used to turn Polish public opinion against Ukraine, thereby diminishing Polish support - a major polarising topic in election campaigns.

Critically, Lega Artis employed AI to make changes to articles and republish them on their own website. This allowed the operation to bypass content blocking measures on social media platforms, exploiting a critical gap in platform checks for the laundering of sanctioned content. This approach appears to be designed to circumvent sanctions and, if confirmed, may constitute non-compliance, enabling hostile state influence operation content to reach Polish audiences under a deceptive guise, eroding trust in legitimate news and polluting the information environment.

To lend legitimacy to their influence operation, Lega Artis fabricated a news persona, presenting itself as a genuine media outlet. They further bolstered this deception by creating fabricated personas on their "About Us" page, claiming these individuals were the site's editors, thereby obscuring their true identities and affiliations. The outlet's history of distributing anti-vaccine content also positioned it as an attractive platform for already radicalised individuals, broadening its potential reach among susceptible audiences. Furthermore, the utilisation of mirroring websites further obfuscated the origin of the content, effectively spreading it across the Polish information space.

While Lega Artis's direct reach during the presidential elections appeared limited, evidenced by its 18,000 followers across social media and low post interactions, the operation's continued activity, including the creation of new social media channels and a website redesign postelection, signals a persistent and evolving threat. **The deliberate obscuring of content origin, the impersonation of legitimate media, and the exploitation of technical loopholes to bypass sanctions represent a continuous challenge to election integrity by undermining transparency, fostering distrust, and allowing foreign manipulation to insidiously penetrate domestic discourse.**

5.5 Citizen Go

A significant actor in the Polish election influence landscape was Citizen Go, a far-right Spanish NGO whose alleged origins and funding ties to the Russian oligarch *Konstantin Malofeev* have been highlighted by Polish Media OKO Press and verified by the European Parliamentary Forum for Sexual and Reproductive Rights. While the organisation itself *denies* these funding claims, these connections suggest a potential conduit for foreign influence operating under the guise of civil society. The Polish branch of Citizen Go actively engaged in multifaceted influence operations targeting the Polish elections. Their techniques included:

- Operating dedicated social media pages to publish original content.
- Utilising paid advertisement on platforms like X (26 ads) and Facebook (1 ad) to promote specific narratives and content.
- Creating online petitions and organising offline demonstrations, (at least three, with two focused on *anti-abortion* and one on *anti-migration* themes), thereby mobilising targeted segments of the population.
- Directly engaging with political candidates by sending out surveys on their political stance, strategically highlighting the responses of aligned candidates (e.g., Braun and Mentzen replied, others did *not*).

Through these channels, Citizen Go propagated a range of polarising narratives. Advertisements spread claims about the left seeking to remove children's religious *rights*, promoted a petition against "WHO abuses and their pandemic *treaty*", and pushed anti-abortion *messaging*. They also conducted surveys designed to question the *seriousness* of candidates and media, while simultaneously *promoting* their own candidate surveys to boost figures like Nawrocki and discredit Prime Minister Tusk (Trzaskowski). These promotional efforts also included dismissing criticisms regarding the organisation's alleged ties to *Russia*.

On their X channel alone, between March and May 2025, Citizen Go's posted 295 original tweets, consistently promoting their core messaging around anti-abortion and Christian family values. Furthermore, they systematically discredited specific candidates, particularly *Trzaskowski* and, until the first round, also *Hołownia*, while simultaneously promoting Braun, Mentzen, *and Nawrocki*. Trzaskowski was frequently portrayed as supporting "foreign immoral values", such as same sex *marriage* and accused of prioritising foreign financial *interests*, advocating for mass migration from *Africa*, and disregarding *independent media*. The EU was also demonised, framed as interfering in the elections to *support Trzaskowski* and undermining European *sovereignty*. Citizen Go also continuously worked to discredit the incumbent government and institutions, alleging attacks on freedom of *speech*, and claiming *institutional partisanship*.

Citizen Go's operation potentially undermined election integrity by leveraging alleged foreign funding to covertly influence Polish domestic politics. Its techniques directly contributed to the polarisation of Polish society, exploiting existing fault lines by amplifying ultra-conservative and anti-establishment narratives. Through targeted discreditation campaigns against specific candidates and the promotion of others, the organisation actively sought to manipulate voter perceptions and choices.

The extensive use of online platforms and offline mobilisation translated ideological positions into real-world action, while simultaneously eroding public trust in democratic institutions and the fairness of the electoral process. The successful takedown of their Facebook page (with 24.5k followers, significantly more than their X account's 1.1k followers) highlights the potential reach of such operations and highlights the critical role of platform enforcement in mitigating their impact.

5.6 Ordo Iuris Promoted Demonstrations

In early May 2025, Debunk.org highlighted a series of five nationalist-led protests against immigration policies at the Polish-German border in Zgorzelec. These demonstrations, organised by Robert Bąkiewicz (former president of the Independence March Association and current president of the Independence political party), were significantly amplified and accompanied by online petitions from organisations with alleged ties to Russia, notably Ordo Iuris (OI). Despite OI's consistent denials of Russian ties, Polish author Klementyna Suchanow points to how OI has financial, personnel, and network *ties* to the Kremlin.

The organisations promoting these demonstrations framed Germany and the EU as orchestrating a "hybrid war" against Poland through forced migration flows, while simultaneously discrediting the Polish government. This narrative directly aimed to exploit existing anti-EU and anti-migration sentiments, fostering polarisation within Polish society and undermining trust in governmental institutions.

During the first protest, an outbreak of violence by neo-Nazi groups, reported by the German newspaper Bild, was quickly met with counter-narratives. Channels like Newser.pl, a platform impersonating the legitimate news aggregator *Newser.com*, spread false claims that the violence was staged by German or state actors. A petition hosted on podpiszapel.org was then launched to delegitimise Bild, further amplified by Newser.pl. Investigations by *Debunk.org* revealed that Newser.pl also promoted other petitions linked to Ordo Iuris, demonstrating a coordinated effort to discredit critical reporting and promote specific political agendas.

The protests and their accompanying online components skilfully tapped into deeply rooted domestic conservative ideologies and historical grievances. This multifaceted

approach served to mobilise citizens and discredit pro-EU candidates, thereby influencing the electoral landscape.

The orchestration of real-world protests amplified by online disinformation, combined with the exploitation of trusted media outlets for deceptive purposes, represents a potent threat to election integrity by manipulating public discourse, undermining media credibility, and fuelling societal division.

5.7 Radio Belarus

In May, a *report* by the Atlantic Council's DFRLab, Alliance4Europe, and the Political Accountability Foundation exposed active interference in the Polish elections by Radio Belarus, a Belarusian state-owned entity under the EU-sanctioned *Belteleradio.* Since its launch in August and September 2023, Radio Belarus's, Polish-language YouTube channel has become a significant vector for influence, having published 930 videos that collectively garnered over 9.2 million views and approximately 320,000 engagements by May 2025.

The content disseminated by Radio Belarus systematically seeks to undermine public trust in Poland's democratic institutions, amplify socially polarising narratives, and either discredit or promote specific political candidates. A key tactic involved extensively interviewing and promoting figures like Maciej Maciak (interviewed 7 times) and Aldona Skirgiłło (interviewed twice) in the run-up to the elections. Maciak, a lesser-known figure in Polish politics with a history of *unsuccessful* electoral bids, has openly expressed his admiration for *Vladimir Putin* and is known for disseminating Russian hostile narratives. Aldona Skirgiłło, a member of the Eurosceptic and agrarian party Samoobrona Rzeczpospolitej Polskiej (Self-Defence of the Republic of Poland), also has a record of unsuccessful candidacies. Radio Belarus notably urged its audience to provide signatures for Maciak, successfully enabling him to become an official presidential candidate, highlighting a direct foreign attempt to shape the candidate field. While Maciak successfully gained over 100.000 signatures, hence becoming an official candidate, Skirgiłło did not.

The operation also engaged in extensive **content laundering**, translating and republishing material from other sanctioned Belarusian media, making it readily available to Polish audiences.

Despite these activities being flagged to X, YouTube, Meta, and TikTok in December 2024 as part of a larger Counter Disinformation Network report on Russian and Belarusian *sanctions* violations coordinated by Science Feedback and Alliance4Europe, initial platform responses were largely inadequate. This failure to enforce sanctions allowed Radio Belarus to continue interfering in the Polish elections. Although the accounts were flagged

again in May 2025, only TikTok implemented geofencing measures to restrict the channel from European audiences, while its content remained accessible on other major platforms. Such inadequate responses from platforms may be inconsistent with obligations under the EU's Digital Services Act, subject to regulator findings.

The operation seemingly exploits social media platforms' lack of comprehensive knowledge of sanction laws or willingness to enforce them, thereby enabling sanctioned content to Polish audiences and bolster candidates aligned foreign interests, directly compromising the integrity of democratic elections.

5.8 Algorithmic Amplification

GLOBSEC, in cooperation with an analyst from the University of Amsterdam, revealed a sophisticated algorithmic manipulation campaign originating on X with the strategic aim of amplifying far-right and pro-Russian content on TikTok, primarily to polarise public opinion in Poland ahead of elections.

The core of the operation leverages TikTok's "share to X" functionality. An extensive network of over 1,600 active, and more than 5,000 unique over time, X accounts - many exhibiting characteristics consistent with bots or inauthentic behaviour (e.g., anonymous identities, generic names, high activity, low follower counts) - are flooding X with TikTok video shares. Critically, even if these shared videos are not viewed on X, the act of sharing itself boosts the content's visibility within TikTok's algorithm, effectively manipulating its recommendation system. This process is further facilitated by TikTok's design, which allows sharing to X without requiring a TikTok login, simplifying automation for the X-based bot network.

The amplified content consistently pushes a far-right narrative in Poland, condemning "incompetent elites, corrupt politicians and immigrants," and presenting the far-right as the nation's salvation. Key themes include strong anti-EU, anti-Donald Tusk, and anti-liberal sentiments, often promoted through patriotic, Catholic, and anti-communist slogans, and directly supporting specific far-right presidential candidates. This content, originating from over 1,000 mostly right-wing TikTok accounts (88% of identified political profiles), remains largely unmoderated, with AI analysis indicating that 85% of active, amplified links are right-wing. Operating with fairly constant activity, the campaign generated over 105,000 posts on X in 2025 alone.

5.9 Nigerian Websites

In May 2025, GLOBSEC and Debunk.org org issued an alert identifying the website *topsportnews.co.uk* as a source of disinformation targeting the Polish presidential elections. The website published at least 26 fabricated AI-generated articles that spread false claims, such as fake candidate suspensions or election date changes.

These articles were shared, often anonymously or via a suspicious Facebook account linked to Nigeria - primarily within small online groups supporting various presidential candidates. This strategy aimed to drive traffic and generate ad revenue for the website, which is heavily reliant on advertising. Investigations suggest the site is likely connected to an Italian ad company and operated by individuals based in Nigeria, indicating a financially motivated rather than purely politically motivated influence campaign.

While the campaign lacked a single, consistent narrative due to its focus on clickbait titles designed for maximum engagement, its overarching theme consistently revolved around the instability and endangerment of the Polish elections. Despite its primary objective appearing to be financial gain, the content's nature - spreading false information about the integrity and procedures of the election - still poses a significant threat. These election-specific articles garnered a reach of 24.1K people through amplification within Facebook groups, highlighting how even **commercially driven disinformation can effectively pollute the information environment and contribute to public confusion and distrust during critical electoral periods.**

6. Unfair Conduct by Political Actors

Polish actors' use of information manipulation further complicated the information environment during the election period. Political candidates and their affiliates frequently used aggressive, emotionally charged language and unfolded claims to discredit opponents and polarise the public opinion. *Examples* from the 2025 debate in Końskie, Poland, include Karol Nawrocki's statement:

> *"Europe today faces a gigantic crisis. This is also the responsibility of your leader Donald Tusk, who signed a pact with Putin alongside Angela Merkel, and under the influence of this pact, emboldened by millions of euros, the Russian Federation attacked Ukraine."*

This quote, widely repeated during campaign events and in the media, was fact-checked and *debunked by TVN24*, which confirmed that no such pact existed and that there was no direct link between Tusk and the war in Ukraine. Another *example* involves Marek Jakubiak, who falsely claimed that Germany had sent 10,000 illegal immigrants to Poland. This assertion was contradicted by official broader data. Rafał Trzaskowski, in turn, *stated* that the government and the Civic Coalition had fulfilled their promise to lower health insurance contributions for entrepreneurs, presenting it as a success. In reality, the reform only partially delivered on that promise and introduced a more complex system, falling short of previous, clearer rules in place before 2022. Above-mentioned rhetoric not only distorts the historical facts but also exploits fear to manipulate voter perception, contributing to an increasingly misleading political discourse.

These examples of manipulation and polarisation extend beyond the candidates themselves, and include the wider media environment - particularly public and partisan media outlets such as TV Republika and wPolsce24. In TV Republika broadcasts, for example, presenters routinely echo PiS party narratives, referring to the opposition as the *"13 December Coalition"* (a phrase intended to describe the current democratic opposition - especially Civic Coalition (KO) and its allies, in a highly manipulative and emotionally charged way). News programming overwhelmingly features voices from right-wing politicians, painting a one-sided and highly distorted picture of the country. Moreover, interviews and commentary segments on these channels are often used to intensify political hostility.

Opposition candidates are frequently insulted or ridiculed, their intentions misrepresented, and their statements taken out of context to serve a specific narrative. This aggressive

media discourse further reinforces *disinformation* and contributes to a toxic electoral climate that undermines democratic debate.

Manipulated posts and emotional framing also played a key role in shaping public perception during the campaign. The strategic use of *out of context visuals*, often not even originating in Poland, helped reinforce xenophobic narratives and exploit cultural and religious differences.

Deceptive campaign tactics extended beyond imagery and rhetoric. In March 2025, it was revealed that Nawrocki was reported to have used a *fake persona* under a pseudonym "Tadeusz Batyr." This persona appeared in the media posing as a historian, publicly commenting on his *book* and Nawrocki's achievements. This was a tool for self-promotion and strengthening Nawrocki's authority as an expert. It also indicates a long-term attempt to build an *expert image*, which could indirectly aid self-promotion in media and political circles. In 2018, long before the presidential campaign, he participated in an interview on TVP Gdańsk, during which his face was obscured and his voice modified.

By manufacturing false personas, spreading out-of-context imagery, and weaponising emotionally charged, unfounded claims, these politicians and their allied outlets systematically dismantle the integrity of public debate. Such practices sow profound distrust not only in individual candidates but in the democratic process itself - casting doubt on legitimate discourse, discouraging informed participation, and deepening societal divides. When those entrusted with public representation resort to deception rather than transparent argumentation, they compromise the very principles of accountability, transparency, and mutual respect that underpin Poland's democratic system. **In this environment, truth becomes collateral damage, and the electorate is left to navigate a minefield of manipulated narratives.** This outcome not only undermines the immediate election but severely endangers the health and resilience of Polish democracy for years to come, making it more susceptible to further internal fragmentation and external influence.

6.1 Pro-Russian Domestic Actors

Within the spectrum of domestic actors engaging in influence operations, the most prevalent and impactful campaigns were conducted by those identified as pro-Russian. This highlights a critical vulnerability in the information environment where actors seemingly operating within national borders actively promote narratives aligned with foreign interests.

On the 30th of May 2025, two days before the second round of voting, GLOBSEC issued an incident alert showing that a leader of the pro-Russian party 'Przebudzeni Konsumenci' ('Awaken Consumers') falsely claimed that a Polish court had legalised the removal of

foreign flags. The claim led to an influence operation amplified by AI-generated content and pro-Kremlin actors, leading to people actually taking down flags from public buildings, violating Polish laws (Article 137(2) of the Criminal Code). The operation tried to portray that support to foreigners, especially Ukraine, is unlawfully imposed on Poland.

A specific incident involving the removal of a German flag from a school polling station by a member of the Law and Justice party was widely *reported*. This action, and the claims surrounding it, were then significantly amplified by a series of pro-Russian actors, including the aforementioned Russian influence operation Lega Artis (see section 6.4), and contributed to spreading narratives that aligned with the flag removal's symbolic act.

As mentioned earlier, in early May 2025, Debunk.org also issued an alert concerning a viral disinformation campaign that swiftly infiltrated the Polish information environment. This campaign centred on the fabricated allegation that French President Emmanuel Macron, German Chancellor Friedrich Merz, and UK Prime Minister Keir Starmer were caught using cocaine on a train to Kyiv, Ukraine.

While the claim was initially proliferated through viral social media posts, official Russian channels, and Kremlin-aligned Telegram networks, its critical impact in Poland stemmed from its strategic amplification by Russia-linked actors within the Polish social media ecosystem, merely a week ahead of the Polish presidential elections. This domestic amplification was notably driven by individuals with established, overt ties to Moscow. These included a well-known Moscow-aligned Polish pundit, already accused of espionage and complicity in Russia's crimes against Ukraine and its citizens, as well as an individual suspected of operating as an agent or employee of Russian special services within Poland. The active involvement of such figures, who hold a degree of domestic presence or notoriety, was crucial. Their engagement lent a veneer of local relevance to an otherwise foreign-originated disinformation narrative, thereby exploiting existing societal vulnerabilities and directly attempting to influence voter perceptions by polluting the local information space with damaging and unsubstantiated claims against international leaders.

Additionally, an alert from DFRLab and GLOBSEC in early March 2025 demonstrated how a proposal by European Commission Vice-President Henna Virkkunen to hold a DSA stress test round table was exploited. This legitimate EU initiative was deliberately framed as a plot by the EU to interfere in the Polish elections and favour pro-EU candidates. This narrative was significantly exacerbated by both foreign (predominantly Russian and Belarusian) and Polish-language entities with foreign ties, such as Lega Artis, Wolne Media, and Niezależny Dziennik Polityczny. These actors capitalised on a procedural discussion to fuel anti-EU sentiment and sow distrust in the fairness of the electoral process.

In a separate incident in late March, GLOBSEC and the DFRLab warned of a concerted effort to discredit Polish government benefits provided to Ukrainian refugee families.

This campaign leveraged a viral video, purporting to be a satirical attempt by a young Ukrainian woman showing seven Ukrainian passports and falsely claiming to receive the "Family 800 Plus" benefit for each. The video was widely picked up by Polish-language pro-Russian Telegram channels and other online platforms. Their intent was clear - to spread resentment against Ukrainian refugees and criticise the Polish government (or the opposition Law and Justice party) for allegedly enabling social welfare abuse by refugees in Poland.

This type of disinformation directly exploits social tensions and aims to manipulate voter sentiment by demonising vulnerable groups and discrediting political parties, thereby compromising electoral integrity through xenophobic narratives.

6.2 Threats to Electoral Integrity

In mid-March 2025, Demagog issued two alerts warning of concerted attempts to undermine the electoral process, deceive voters on procedural matters, and discredit the overall legitimacy of the elections. These alerts detailed efforts to mislead the electorate regarding voting procedures, including misinformation about voting methods, deadlines, and eligibility. The propagation of narratives targeting electoral integrity not only aims to distort reality and create procedural confusion, but it also fundamentally seeks to erode democratic legitimacy and voter confidence.

6.2.1 Narrative Based on Damage to Electoral Ballots as a Political Defence Mechanism

One prominent narrative observed actively encouraged pouring wax on ballots. This was advocated as a measure to prevent what was falsely described as the "Polish government invalidating votes of far-right candidates". This call held a dual dimension. On one hand, it reflected deep institutional distrust prevalent among certain segments of the electorate towards the government. However, on the other hand, it was deliberately leveraged as a tool to amplify scepticism and sow division within the voting populace.

By advocating a symbolic yet destructive tactic like pouring wax as an act of protest, voting was reframed not as a democratic exercise, but as an act of confrontation. **This form of electoral vandalism directly threatens to undermine confidence in the outcome of electoral voting and, over time, increases the likelihood of the use of violence in political processes.**

6.2.2 The Use of Video Footage to Create a Climate of Fear and Scepticism

The other significant information manipulation case involved the widespread dissemination of a video demonstrating how to remove votes from ballots using a lighter, urging people to bring their own pens to the polls, or outright suggesting that the elections were pointless

due to pervasive fraud. It is critical to note that this video was deceptively repurposed from Kazakhstan in 2019, underscoring the foreign origin and misleading nature of the content. Despite its foreign origin, this misleading content was strategically weaponised within the Polish electoral discourse to falsely depict pervasive and systematic fraud, directly aiming to erode public trust in the election's legitimacy.

6.2.3 Overlapping of Electoral Disinformation with Hate Speech and Conspiracy

Disturbingly, these messages were also intertwined with overt hate speech targeting Ukrainians and conspiratorial antisemitism. Detected messages included attacks on Ukrainian refugees and veiled accusations of Jews controlling the results of elections.

6.3 Murky Accounts

Democracy Reporting International (DRI) issued an alert in late May 2025, flagging the presence of 129 “murky” accounts of **unknown origin** on TikTok actively impersonating candidates in the first round of the Polish presidential race and prominent Polish political parties. Following the elections, their comprehensive *report* identified and flagged a total of 145 such accounts: 57 impersonating political parties and 88 impersonating individual candidates.

Mentzen had the most extensive murky account support, with 21 impersonating accounts, followed by Gregzor Braun with 15. Among the accounts in DRI's dataset, those promoting the Peace and Justice (PiS) party and the Konfederacja party, along with their respective candidates, exhibited the highest rates of engagement and followers. Notably, accounts supporting Konfederacja received over 12 times more engagement than those promoting the leading competitor. While most of these accounts had relatively low follower counts, a few stood out with their massive engagement, foremost being the "Konfederacja EXTRA" account, which amassed over 8.1 million likes and 249,000 followers, indicating significant algorithmic amplification or coordinated inauthentic behaviour.

TikTok subsequently removed 102 of these accounts, but 43 remained active. Some of these claimed to be secondary accounts, but had not undergone TikTok’s verification process for political entities. The unknown origin of most of these accounts makes it impossible to ascertain whether they are run by domestic or foreign entities, hindering attribution and accountability. This case highlights a critical vulnerability in platform enforcement, echoing concerns raised in earlier sections regarding Meta's ad system. While TikTok bans political advertising and imposes higher transparency requirements and registration limits on accounts belonging to political parties, the DRI report indicated that these policies were seemingly not reliably enforced and may be insufficient to counter sophisticated influence operations.

The ability of unverified accounts to impersonate political actors and achieve such disproportionate engagement demonstrates a significant threat to electoral integrity by distorting public discourse, manipulating perceived support for candidates, and undermining the authenticity of online political engagement.

6.4. Irregular Following Pattern

DRI also partnered with local Polish organisation the Institute for Public Affairs (IPA) and independent researcher Anna Mierzyńska to investigate the online campaigns of the 13 candidates. In their joint report, they identified potential inauthentic activity on the official Facebook and Instagram pages of Sławomir Mentzen.

Using the Sotrender monitoring tool, the researchers discovered that the Mentzen's profiles experienced several abrupt and large-scale increases in follower count, often on days of low political activity, such as Christmas or New Year's Eve, and in the absence of corresponding campaign events. On Instagram alone, Mentzen gained over 26,000 followers in a single week in March 2025, more than seven times more that of the next highest candidate. On Facebook, posts from his account at times received hundreds of reactions within just minutes, far exceeding typical engagement patterns for political content. This pattern of high-intensity engagement continued until mid-April 2025, when Mentzen's follower growth and interaction rates suddenly dropped and aligned with levels observed for other candidates.

While IPA's findings do not conclusively prove the use of paid followers or engagement, the irregularities observed point to a need for closer scrutiny of campaign practices on digital platforms in Poland.

6.5 Murky Ad Campaign

Leading up to the presidential elections, Info Ops Poland issued an incident alert concerning a Meta ad campaign. This campaign, which spent €100,000 and reached one million users, while garnering 15,000 interactions, specifically targeted Polish audiences with content discrediting the far right while promoting Rafał Trzaskowski.

Active between April 10 and May 15, 2025, the campaign leveraged two anonymous Facebook pages: "Wiesz Jak Nie Jest" (You Know How It Isn't) and "Stół Dorosłych" (Adult Table). These pages posed as full-fledged organisations to deliver their messaging. One-page featured ads with regular individuals speaking, lending a grassroots appearance, while the other adopted a more polished, campaign-video-like format with a voice-over.

The content broadly portrayed far right-wing politicians as endangering women and society, often making claims of their criminal connections. A core narrative pushed was that only experienced, responsible politicians could effectively govern the country.

These pages were directly linked (via Meta Ad Library) to two websites devoid of meaningful content or information. The websites were registered by **Estratos Digital GmbH**, an Austrian software and data company that reportedly works with political and social organisations. Estratos *denied* wrongdoing in a statement to Demagog, claiming to have provided infrastructure for a Polish NGO client conducting a non-partisan voter mobilisation campaign.

This case has been extensively reported on in the Polish press during the elections, with speculation as to the nature of the incident, and is under investigation by Polish *authorities.* **In this case, there is no evidence to suggest this was such an effort. This is an example of where the democracy defending community needs to uphold evidence standards, and avoid promoting unsubstantiated speculation.**

Initially, NASK, Poland's National Research Institute, flagged this case as a potential foreign funded attempt to interfere in the Polish elections, a possible provocation aimed at discrediting the candidate ostensibly supported by such ads *(Trzaskowski)* or destabilising the pre-election environment.

NASK subsequently reported the case to Meta, asserting that their *flagging* led to the ads' removal. However, Meta *denied* that they had taken down the ads, stating that their investigation confirmed the administrator associated with the pages was authentic and based in Poland. They claimed that they had seen "no evidence of foreign interference." This statement by Meta focused solely on the admin account's location rather than the source of funding, which was NASK's primary claim, as the source of the funding remains unknown. At the time of writing, the Facebook pages have been removed, though it remains unclear whether by Meta's direct action or the advertisers themselves.

The ad campaign seemingly exploited a critical technical vulnerability in Meta’s ad system’s Know Your Customer (KYC) mechanism. Based on the evidence INFO OPS Poland has provided, this case suggests that it may not meet the transparency requirements of DSA Article 26; only authorities can determine non-compliance. The DSA mandates that platforms display the natural or legal person on whose behalf an advertisement is presented, and, if different, the person who paid for it. In this case, none of that information was presented transparently. Meta's current process *requires* only the page administrator to submit their ID for verification, and does not appear to meaningfully verify provided contact information or campaign websites.

In this instance, the Facebook pages were authenticated using a Polish citizen's ID, coupled with empty websites and associated email addresses, and a phone number. By authenticating the pages, the accounts could post political ads.

Addressing Meta's Lacking Know Your Customer Systems

The murky ad campaign incident demonstrates a significant weakness in platform accountability. If an operation can spend over €100,000 using inauthentic organisational personas and fabricated infrastructure, it highlights how easily supposed safeguards can be circumvented. *EDMO* has flagged that scammers and spammers are exploiting the same vulnerability using similar tactics.

Meta's insufficient verification processes have historically enabled foreign-funded influence operations to surreptitiously inject divisive content into European electoral discourse, a vulnerability evident in cases like the Sahel-based Russian operations targeting French *elections* and the *Doppelganger* campaign.

The ability to use a local ID with fabricated supporting assets means that for large-scale political advertising, only local cooperation is required to bypass critical transparency measures. Meta's failure to detect large-scale, centrally managed operations, especially ones involving substantial financial outlays, raises questions about the adequacy of its transparency controls under the DSA. It underscores the urgent need for more robust, comprehensive, yet efficient KYC procedures, particularly for high-spending political ad campaigns, to prevent covert foreign interference and ensure the integrity and transparency of elections. This means they must meet the requirements set out in the DSA, effectively prevent abuse, while also effectively enabling and providing clarity for democratic actors, civil society, and civic engagement.

Meta's July *announcement* outlining the cessation of political, electoral and social issue ads on its platforms within the EU starting in October 2025, represents a significant policy shift. While this move aims to restrict overt political advertising, it inadvertently creates additional challenges by removing the very Know Your Customer (KYC) checks previously associated with such ads, potentially exacerbating the issue of covert influence. This change means legitimate political campaigns will lose a direct avenue to reach audiences, yet malign influence operators are likely to respond by further obfuscating the true political nature of their promoted content. As demonstrated by operations targeting French European Parliament elections and snap *elections*, as well as the pervasive *Doppelganger* campaign, threat actors have already proven adept at employing obfuscation methodologies to circumvent Meta's automated ad review systems, a challenge likely to intensify with the removal of established transparency mechanisms.

7. Reach of FIMI Campaigns

The accurate assessment of the true reach of documented information manipulation cases and influence operations presents significant challenges. Engagement metrics vary considerably across platforms, each employing unique procedures for calculating view rates, which can render reported numbers potentially misleading and create a deceptive impression of actual impact. For instance, X's "view" system *registers* a view simply if a user scrolls past a tweet, irrespective of whether they engage with or even read the content. In contrast, TikTok records a view upon a click to "play," while other platforms may require a minimum viewing time for video *views* to count. Furthermore, not all platforms transparently display the total number of views content receives.

Despite these methodological challenges, publicly available statistics indicate that content spread across the examined operations and information manipulation incidents collectively garnered over **23 million views and 589,000 interactions.** While these numbers must be interpreted with caution due to varying platform methodologies and the potential for manipulation, they nonetheless suggest that some disinformation narratives have managed to achieve greater social media penetration than many official influence campaigns.

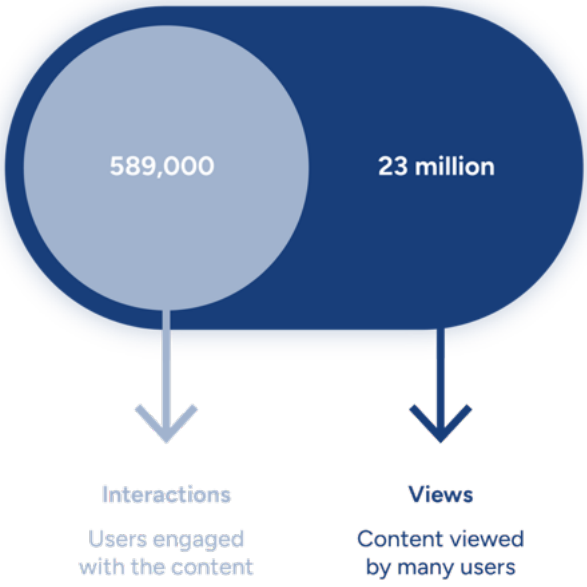

Figure 41: FIMI Disinformation Narrative Social Media Reach During Polish Presidential Elections

Prevalence and Qualitative Impact Analysis

These consistent and often slow-burn operations are designed to **gradually penetrate the Polish information space over extended periods.** While their immediate reach might appear limited at first glance, their sustained presence signifies ongoing investment by Russia and Belarus in efforts to influence Polish elections. **This type of repetitive work points to a long-term strategy aimed at developing a permanent impact on public opinion, gradually and surely undermining trust in official information sources, particularly during electoral periods.**

Qualitative analysis reveals a differentiated impact among campaigns. While operations such as **Pravda, Lega Artis, and the Nigerian-linked websites** did not consistently reach a significant number of authentic users, other platforms and incidents demonstrated greater success in penetrating specific segments of Polish society. Notably, **Doppelganger, Radio Belarus, Citizen Go, and certain isolated information manipulation incidents** achieved traction by effectively targeting topics of high public concern in Poland, including refugees, migration, national identity, and regional conflicts.

However, campaigns like **Operation Overload and Doppelganger** present a distinct challenge. These operations have overtly relied on **inauthentic amplification** to artificially inflate their reported reach and engagement rates. Through the extensive use of bots and fake accounts, a substantial portion of their recorded engagement is inorganic, making it exceedingly difficult to ascertain their genuine reach to authentic audiences and therefore to fully assess their true impact on public discourse.

The analysis of reach for information manipulation campaigns reveals a clear distinction between high- and low-reach operations, with each having different implications for their strategic impact.

High reach refers to campaigns or incidents that gain significant traction and penetrate specific segments of society or the general public. These operations can achieve a substantial number of views and interactions, sometimes translating online influence into real-world action, as seen with Citizen Go's ability to mobilise followers for offline protests. High-reach incidents often utilise emotionally charged narratives that resonate strongly with particular populations, allowing them to gain widespread attention in a short period.

Low reach, in contrast, describes operations that exhibit limited direct engagement with a broad audience. Their content typically garners only a few hundred views and interactions, indicating a constrained ability to directly captivate a wide audience. However, low-reach campaigns may still have significant strategic objectives, such as targeting specific niche groups, attempting to penetrate AI models, or serving as a reservoir of content that could be picked up and amplified by influential figures later.

7.1 High Reach

The Polish edition of Radio Belarus seemingly managed to reach specific segments of Polish society, demonstrating considerable digital reach since its creation in September 2023. The operation amassed a total of 16 million views and at least 542,000 interactions across its platforms by May 2025. While many of their individual videos gained limited traction, most of those directly related to the election, including candidates, consistently garnered over 20,000 views, indicating targeted effectiveness in electoral discourse.

Citizen Go also showcased significant reach within the ultra-conservative movement in Poland. Before its Facebook page was taken down, it commanded 24,500 followers and successfully mobilised these segments to participate in offline protests during the election period. **This ability to translate online influence into real-world action highlighted its substantial penetration and potential threat within this specific ideological segment of Polish society.**

Beyond these organised campaigns, a series of smaller, more opportunistic information manipulation cases also successfully permeated public discourse, demonstrating substantial, albeit short-lived, reach. Foremost among these were the "Foreign Flag Incident" and the "Ukrainian Refugee Social Security Case".

- The "Foreign Flag Incident," had a notable social media footprint, with at least 7,460 users discussing it, generating 1.5 million views. This indicated a strong resonance within a particular segment of the population, leading to widespread engagement.
- The case focusing on the earlier mentioned Ukrainian refugee woman (accused of welfare fraud) received at least 1 million views across all platforms and in the 10 languages it was covered in.[27] While the specific reach within the Polish audience remains unclear, its global traction suggests significant viral potential.

[27] This case was covered in an unpublished incident alert. For further information, please contact Alliance4Europe.

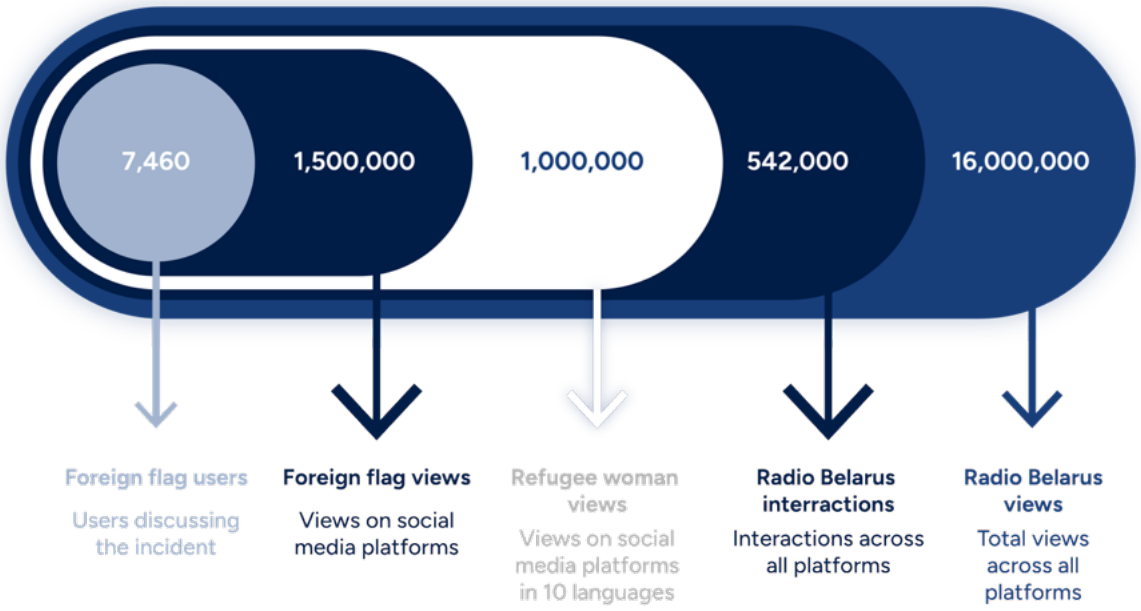

Figure 42: Influence operation and information manipulation incident views and interactions

Despite being relatively short-lived, these two cases gained significantly more traction in a short timeframe than more complex and seemingly larger-scale operations like Operation Overload and Doppelganger in a comparable period. **This disparity highlights the penetration potential of emotionally charged narratives, especially when amplified by Kremlin-aligned influencers and domestic actors.**

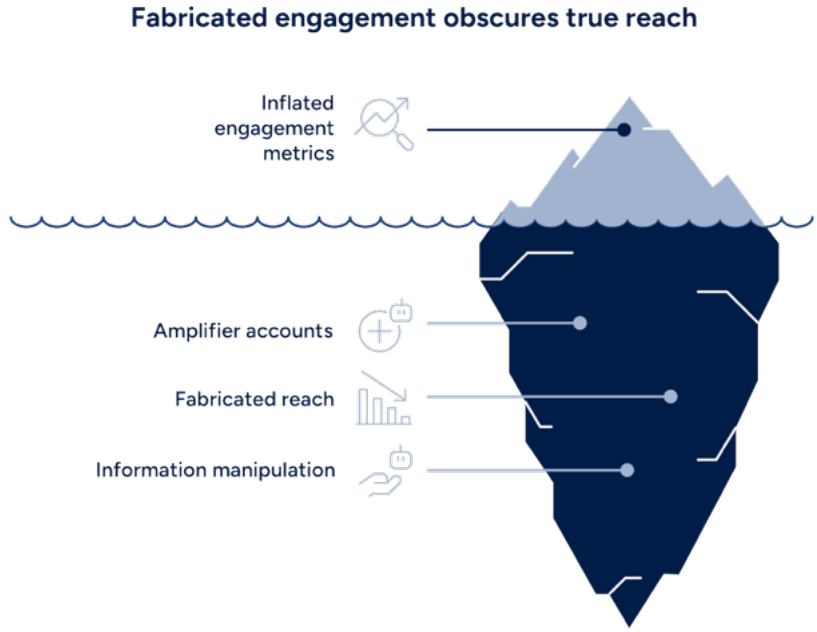

Figure 43: Beyond the Surface: How Fabricated Engagement Masks Real Impact

At a first glance, content from Operation Overload appeared to achieve substantial engagement with 1,187,100 views and 10,255 interactions, while Doppelganger amassed 271,000 shares and nearly 1.5 million views. However further investigation has clearly indicated that these numbers were substantially fabricated through the use of amplifier accounts, revealing that the true, authentic reach of these sophisticated operations was in reality, quite low.

This highlights the ongoing challenge of discerning genuine public engagement from algorithmically or artificially inflated metrics in assessing the true impact of information manipulation.

7.2 Low Reach

While several influence operations targeting the Polish elections exhibited limited direct reach, their underlying strategic objectives and the continued investment of resources by foreign actors warrant serious attention.

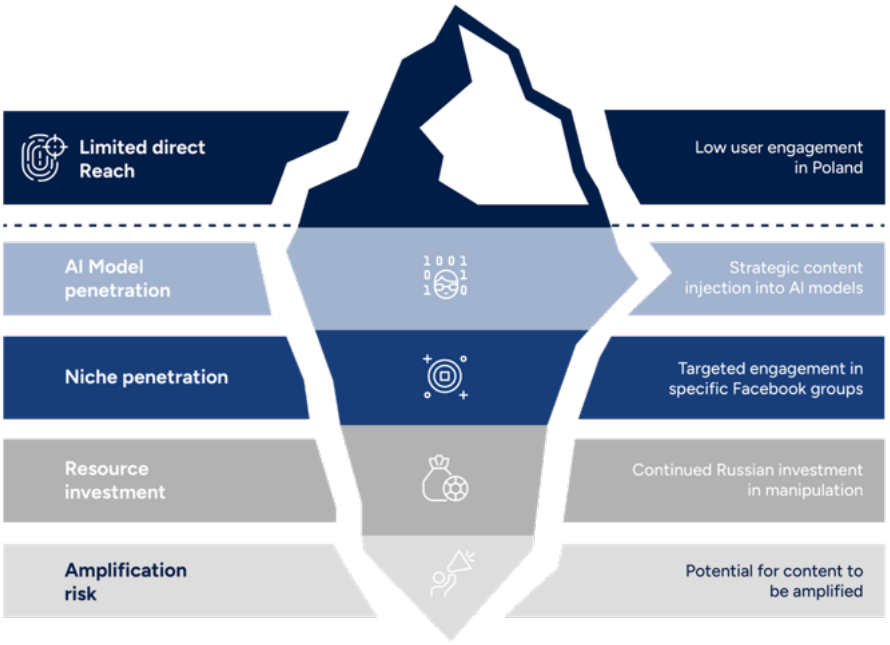

Figure 44: Limited Direct Reach, Significant Strategic Objectives

The Pravda Network's Polish edition, for instance, demonstrated minimal direct engagement with the general populace. Its Telegram channel recorded only 303 followers, with individual posts reaching fewer than 30 viewers. **This suggests that the primary objective of this particular operation was not to directly influence regular citizens, but**

rather to strategically penetrate AI models with content reflecting Russian perspectives and interests, potentially shaping future information environments.

Similarly, Lega Artis typically garnered low user engagement. Its content rarely exceeded a few hundred views or more than 30 interactions per post, indicating a constrained ability to directly captivate a broad audience.

The Nigerian website, despite its efforts, also struggled to achieve widespread traction, managing only 24,100 views on Facebook. However, it is critical to note that these views were highly targeted, generated through engagement in Facebook Groups specifically associated with two presidential candidates. **This illustrates an attempt at niche penetration, even if broader societal impact was not achieved.**

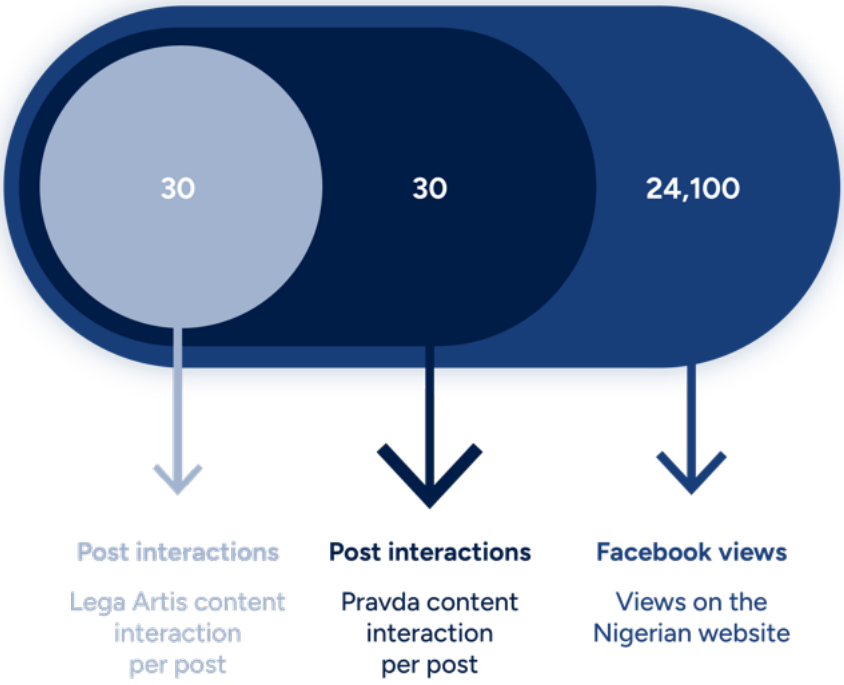

Figure 45: FIMI Operations Social Media Views and Interaction

While it is fortunate that the direct, mass penetration into Polish society by these specific operations appeared limited, their very existence signifies a continued and considerable investment of Russian resources aimed at manipulating Polish elections. **These persistent attempts pose an enduring risk, as they can eventually achieve significant amplification if their content is organically or deliberately picked up by influential individuals.** A stark illustration of this risk is seen in the U.S., where a video from Operation *Overload*, despite potentially having limited initial organic reach, was shared by high-profile figures such as Donald Trump Jr. and Elon Musk, demonstrating how low-visibility operations can achieve massive, unforeseen amplification and impact.

8. Interventions & Responses

The FIMI Defenders for Election Integrity (FDEI) project actively addressed 20 distinct influence operations and information manipulation incidents throughout the Polish presidential election campaign. The response strategy for each case was tailored to its specific nature, ranging from targeted outreach to platform providers for direct resolution to larger, more comprehensive efforts. These broader responses included collaborating with media outlets to disseminate warnings about emergent information threats and engaging with governmental bodies to exert pressure on platforms for decisive action against identified risks.

Figure 46: FDEI Response to Influence Operations

8.1 Response Methodology

The FIMI Defenders for Election Integrity (FDEI) FIMI ISAC project operates through a robust and cooperative framework that brings together partners, including Alliance4Europe, the DISARM Foundation, and Debunk.org, combining their expertise, resources and strategies in addressing information manipulation during election periods.

FDEI effectively leveraged this collaboration methodology, which integrates sophisticated monitoring, analysis and response capabilities which was developed by the project consortium and FIMI ISAC members. Furthermore, dedicated mailing lists compiled by partners including the CDN proved invaluable, facilitating timely communication with "responders", government agencies, security services, EU institutions, journalists and advocacy groups, providing them with concise incident alerts that summarise critical cases.

For the Polish presidential elections, 28 organisations, encompassing both international and national entities, heeded the call for collaboration. These organisations joined the FDEI project's FIMI Response Team (FRT).

Through this collaborative infrastructure, practitioners diligently monitored the information space for threats, promptly flagging identified concerns. They joined forces to conduct in-depth investigations and compile comprehensive incident alerts. Participants also engaged collaboratively in response actions, leveraging their collective strengths as journalists, factcheckers, and advocates to inform the public about detected threats and to press platforms for appropriate action. Journalists from some of Poland's most prominent media houses were embedded within the FRT, significantly enhancing the ability to rapidly inform the public about attempts to manipulate them.

Figure 47: FDEI FRT Media Reach During Presidential Elections Monitoring

This strong collaboration with Polish media resulted in major media houses covering findings on operations like Doppelganger and Radio Belarus, collectively informing hundreds of thousands of people about the threats these operations posed. **In total, over 55 Polish-language articles, videos, and audio (radio) were produced about the activities of the FRT, including major Polish media outlets. Furthermore, 40 articles were published in other languages, primarily in English, with the social listening tool Meltwater estimating a reach of at least 550,000 Polish citizens.** However, considering Meltwater's limited access to complete view metrics for most of these articles, and their placement in major Polish publications, the actual reach is highly probable to be substantially greater.

A key mechanism employed within the project's methodology is the utilisation of the European Commission's Code of Conduct Rapid Response System. This powerful mechanism provides civil society organisations with a direct channel to present cases to major platforms - Meta, TikTok, Google, and Microsoft - starting a month prior to elections.

This provides a crucial avenue for collaboration with platforms in responding to threats and holding them accountable when their actions are deemed inadequate. GLOBSEC and Alliance4Europe, alongside FDEI FRT members such as CEE DDW and Demagog from Polish civil society organisations, actively participated in this Rapid Response System. Through this concerted effort, 8 cases[28] were flagged, resulting in social media platforms acting on 4 cases, while not taking any meaningful actions against 2 cases, and limited actions, meaning they took some actions but not adequate, against 2 cases.

[28] We define a case as an escalation of one link or a collection of links to the social media platforms.

Figure 48: FDEI FRT Collaborative Response to FIMI Threats in Polish Presidential Elections

The work of the Rapid Response System was praised by the Polish Ministry of *Digitalisation* and was recognised by the *OECD* as a **"unique multi-stakeholder format for tackling content contrary to platforms' policies and posing election integrity risks"**. However, the OECD also highlighted that citizens have a limited understanding of the system.

Indeed, while the technical and operational aspects of the Rapid Response System may be highly effective, a lack of public understanding also creates a **critical vulnerability in the overall societal defence against FIMI.** It highlights that even well-designed technical solutions require effective public engagement to achieve their full potential in democratic societies, **thereby strengthening democratic resilience through enhanced public understanding and engagement.**

8.2 Successfully Disrupted and Exposed Cases

Beyond the framework of the Code of Conduct, the FDEI FIMI Response Team (FRT) actively engaged with Bluesky to present ISD's investigative findings on Operation Overload. As a direct result of ISD's alerting and comprehensive reports, Bluesky significantly improved the efficiency of its content takedowns related to Operation Overload, demonstrating an adequate and responsive approach. This mirrors the successful engagement that Alliance4Europe had previously undertaken with Bluesky concerning the Doppelganger operation, which subsequently rendered Doppelganger unable to operate on the platform.

Regarding Radio Belarus, the issue was initially flagged by Alliance4Europe and Science Feedback to all major social media platforms in *December 2024*. Unfortunately, these initial warnings were not acted upon, allowing the operation to continue its activities throughout 2025 and interfere in the Polish presidential elections. The channel was flagged once more, leading to TikTok implementing geo-fencing measures to restrict the account from European audiences, thereby complying with EU sanctions. However, other social media platforms did not take comparable adequate actions to ensure their compliance, allowing the interference to persist on their services.

8.3 Less Successful Interventions

Despite significant efforts, not all interventions proved entirely successful. For instance, as mentioned earlier, while GLOBSEC flagged instances of the Pravda Network making Russian sanctioned content accessible to Polish audiences through Google Search, the content remains indexed and discoverable. Google's response to this persistent threat has been inadequate, failing to effectively address the presence of such illicit content on its platform.

Similarly, although the Doppelganger operation has been effectively addressed by Bluesky, it maintained its activity on X throughout the election period. The operation was flagged in late April to X, with comprehensive examples and behavioural patterns provided.

These patterns had previously been flagged to X in a September 2024 *report*, coordinated by CeMAS and Alliance4Europe and collaboratively authored with nine other organisations, outlining identical sharing tactics and profile characteristics to those observed during the Polish elections. Given that the project utilises X's own API for automatic tracking of the operation, the platform theoretically possesses the capability to automatically take down such content. Yet, while X did remove the specific cases provided, the operation's use of "throw-away accounts" means that takedowns occurring days after content is posted are simply not efficient enough.

Following DRI's reporting, 64 of the Murky accounts were acted upon, while 43 remained active. These accounts have been repeatedly flagged by DRI since the European Parliament elections, highlighting their emergence as a new tactic to circumvent TikTok's political campaigning *policy*. TikTok's persistent inability to adequately address this issue, despite nearly a year of warnings, raises significant concerns, and may indicate a systemic risk.

8.4 Polish Response Initiatives

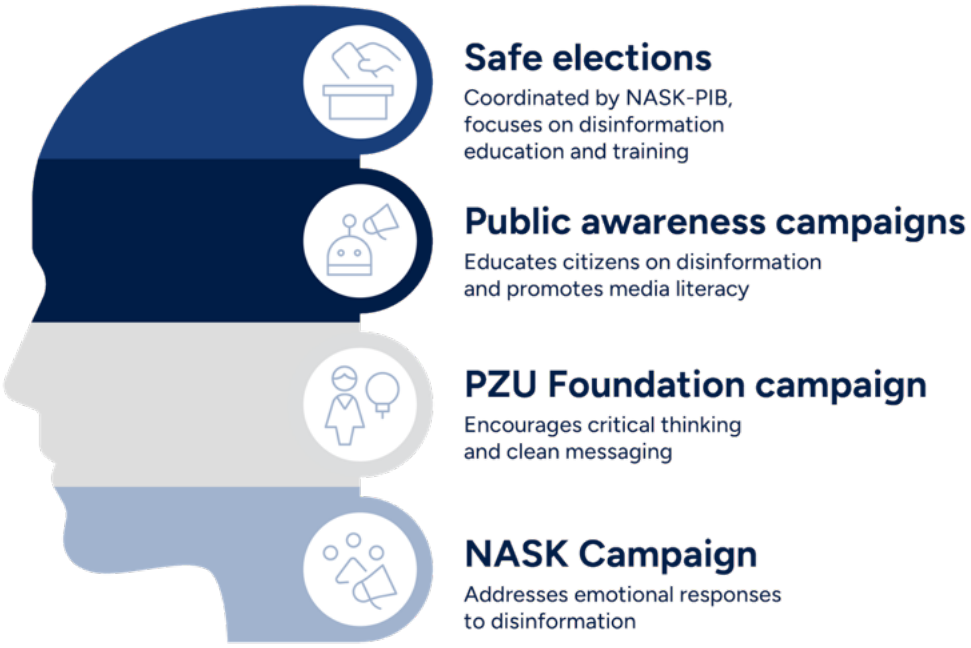

Figure 49: Polish Response Initiatives During 2025 Presidential Elections

The Polish government proactively initiated the "Election Umbrella" program to significantly enhance cybersecurity measures for the 2025 presidential *election*. This programme serves as a robust platform for fostering inter-institutional partnerships, thereby establishing crucial channels for collaborative efforts across multiple agencies.

A central pillar of the "Election Umbrella" is the "Safe Elections" project, coordinated by NASKPIB. The Election Protection Program project encompassed a wide array of informational activities, including specialised meetings on disinformation, targeted training for Electoral Committees, the National Electoral Office (KBW), and journalists. It also developed comprehensive educational materials and launched campaigns focused on the practical reporting of disinformation content.

Broader public awareness campaigns were launched to educate citizens about the pervasive dangers of disinformation and equip them with the skills to identify it. These initiatives aim to promote media literacy and critical thinking. One such notable campaign, launched ahead of the election by the PZU Foundation, specifically encouraged critical thinking and promoted "clean messaging". This campaign aimed to sensitise Polish citizens to the problem of disinformation through a multi-faceted approach, including broad public outreach, educational efforts in schools, and engagement with celebrities and influencers. Its messages reached Polish audiences through extensive coverage in television, radio, online media and the press.

Another significant initiative was the "Nie pozwól sobie odebrać głosu!" (Don't Let Them Take Your Voice!) campaign led by NASK. This campaign adopted a sophisticated approach, addressing not only the misleading content itself but also the emotional responses that often accompany and fuel such manipulations. The campaign featured a series of three episodes, vividly illustrating how disinformation can impact citizen's everyday lives.

8.5 Lasting Impact

Even as the elections conclude, the robust community building achieved through the FIMI Defenders for Election Integrity (FDEI) project is poised to yield significant and long-lasting benefits for the Polish counter-information manipulation community.

This consolidated expertise represents a profound enhancement of Poland's capacity to address evolving information threats. The FDEI FIMI Response Team, forged during this period, will continue to serve as a vital platform, enabling seamless collaboration between Polish and international organisations. This ensures the capability for **rapid, coordinated responses during future major events and crises, far beyond the immediate electoral cycle.** The enduring impact extends to a more resilient Polish information space, marked by improved collective abilities in threat detection, nuanced analysis, and the swift implementation of counter-measures. **This legacy of strengthened relationships and shared operational knowledge fundamentally elevates the nation's long-term defence against sophisticated information manipulation.**

9. Policy Recommendations

The 2025 Polish presidential elections exposed vulnerabilities in Poland's digital information environment – including a fragmented media landscape, high exposure to foreign content, low trust in democratic institutions, and limited oversight of Polish-language content online – with FIMI incidents and campaigns persisting despite existing regulatory and platform-based safeguards. Therefore, this section outlines targeted recommendations aimed at strengthening institutional resilience, enforcing EU regulations, and countering malign influence operations orchestrated by networks such as Doppelgänger and Operation Overload.

In the Country Election Report Assessment (CERA) published ahead of the elections in May 2025, we identified the legal and policy mechanisms that could reinforce election resilience:

- Full implementation of Digital Services Act (DSA) oversight and increased funding for election security;
- Ensuring that data access for researchers from social media platforms is made
- accessible, effective, efficient, comprehensive, and easy to use;
- Transparency in campaign finance laws to prevent foreign funding loopholes;
- Mandatory disclosure of AI-generated political content in electoral campaigns;
- Harmonisation of disinformation regulations among EU member states, ensuring that all countries adopt common standards and methods in combatting FIMI;
- Closer collaboration between government agencies and civil society to detect and counter manipulation and interference.

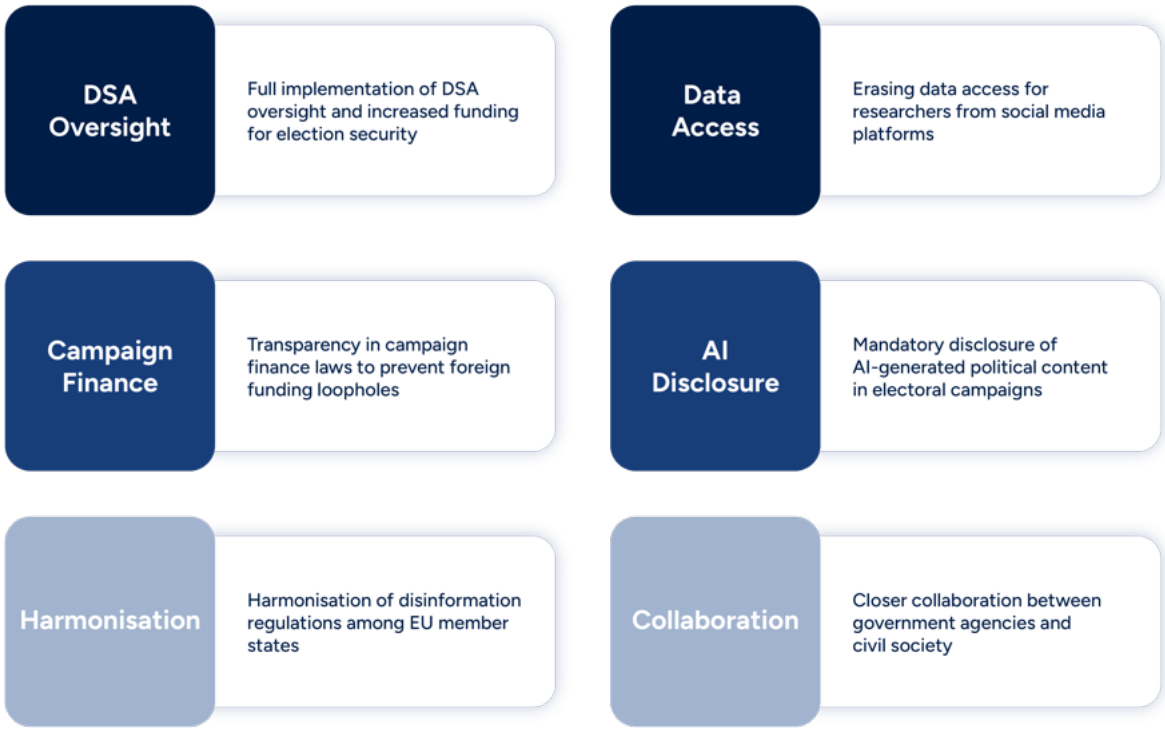

Figure 50: Strengthening Electoral Resilience

9.1 Digital Services Coordinator

A key concern highlighted in the monitoring was Poland's failure to establish a permanent Digital Services Coordinator (DSC) by the DSA's mandated deadline, a shortfall that has hindered effective oversight of intermediary services. The temporary appointment of the President of the Office of Electronic Communications lacks the mandate and resources to enforce DSA obligations or impose penalties. **Establishing a fully empowered, well-resourced DSC is critical to ensuring accountability, serving as a liaison for researchers and civil society, and facilitating access to transparency-related datasets.**

9.2 Systemic Risks

Influence operations leveraged opaque advertising mechanisms, impersonation, and monetisation features across platforms like Meta, X and TikTok. A report by Jakub Szymik, published on *Instytut Spraw Publicznych* underlines the importance of consistency in transparency labelling of advertisement.

Having data in the labelling be changed after the verification process that allows pages to publish ads diminishes transparency and trust in the ad systems. Ensuring consistent labelling will prevent discrepancies and ensure transparency for the public and regulators.

To maintain trust in the labelling system, we recommend including guarantees that labels are not altered between the time of account verification by the platform and the broadcast of the ads. Furthermore, the publicly visible label should consistently display the same data as was provided during the verification period. This will help prevent discrepancies and ensure transparency for the public and regulators.

Enforcement of transparency provisions, particularly those stipulated under Article 26 of the DSA and the Regulation on Political Advertising, remains inadequate.

Platforms must be compelled to verify advertiser identities and halt revenue streams to known malign actors. Evidence gathered in the report shows platform failure to anticipate and mitigate foreseeable risks (as remanded by DSA Articles 34 on risk assessment and 35 on risk mitigation), revealing the insufficiency of their self-assessments and the need for proactive oversight by authorities. As *Szymik* points out, greater transparency is needed around how ad revenue is shared, to better track financial flows between platforms and potentially bad actors that fuel disinformation or breach ad rules.

Manipulative networks have exploited gaps in platform enforcement and regulatory inertia, allowing sanctioned outlets like Radio Belarus to operate openly and Pravda to continue operating via proxy domains and repackaged content. TikTok, in particular, allowed political impersonation that facilitated the spread of deceptive narratives. The platforms' inaction, especially in response to repeated flagging of such accounts, underscores the need for punitive measures when rules are not enforced.

Figure 51: The Blind Spots of Regulation

Operation Overload, Doppelganger, and the un-attributed CIB network detected by GLOBSEC and University of Amsterdam shows a clear vulnerability in X's account creation system. Within 1.5 minutes, an operator can manually create an X profile using a temporary 10-minute email address. This vulnerability remains unaddressed by X despite previous flagging, which may indicate a systemic-risk gap under DSA Articles 34–35 (risk assessment/mitigation), subject to authority review0.

Further considering Operation Overload and Doppelganger, X has repeatedly been warned about the operation on their platform but has failed to address them. If we, as civil society actors, can utilise their API to track the operations, so can they and should be able to disrupt them, as Bluesky have not effectively done. If confirmed, this could amount to non-compliance with DSA Articles 34 and 35.

To document such failures, a rigorous and transparent access to data and escalation mechanisms should be operated. Despite robust monitoring efforts, the rapid-response infrastructure linking platforms, civil society, and regulators should be more transparent on vulnerabilities and responses brought by platforms. A permanent incident escalation system, led by a fully operational DSC, is essential to facilitate real-time cross-sector communication and intervention - particularly during electoral periods, and long-term accountability, as these escalation mechanisms should operate beyond elections.

9.3 Data Access

Researchers had limited access to data from the social media platforms to monitor digital threats during the election period. Without the proper institutional backing, their legal rights under the DSA - particularly those granted by Article 40 - remain difficult to enforce. In view of the recent publication of the delegated act to Article 40(4), ensuring full compliance with access to data rules is essential for enabling researchers to analyse algorithmic behaviours, ad targeting, and the virality of content. To move beyond reactive, ad-hoc monitoring limited to electoral cycles, civil society must also receive sustained national and EU-level funding to build technical capacity, retain institutional knowledge, and ensure long-term readiness.

9.4 Foreign and Domestic Dichotomy

Notably, previous findings highlight the interplay between foreign and domestic disinformation actors. FIMI narratives have been amplified by domestic sympathisers, including political figures and influencers. Vice versa, foreign actors leverage domestic vulnerabilities to make the interference appear grassroot, further blurring the line between external manipulation and homegrown disinformation. **Targeted accountability mechanisms are needed to address this convergence, including public denunciation of domestic figures who disseminate or echo manipulative narratives.**

Poland is also equipped with a robust legal framework that could enable the authorities to prosecute collaborators of foreign intelligence services. While such ties are hard to prove, Polish security services could collaborate with civil society in identifying suspected

information manipulation cases and potential ties between the operators and foreign states. While some of the Polish citizens engaged in influence operations are abroad in Belarus and Russia, Polish authorities could still prosecute them, limiting their ability to leave these countries without facing arrest and sanctioning them, affecting their financial assets.

9.5 Public Resilience

Public resilience is key in effectively combating hybrid threats, on top of addressing systemic failures from platforms as described earlier. Poland and other EU member states must invest in comprehensive media and digital literacy programs that should be tailored to address agespecific vulnerabilities, including young people's reliance on social media platforms and older individuals' limited familiarity with digital environments. By equipping these groups with critical thinking tools and fostering informed media consumption, such programs can also play a crucial role in addressing widespread distrust in journalism and public institutions. Of course, this is not to shift responsibility from platforms to users, who are entitled to a safe digital environment, but simply an integrative means to promote societal resilience against disinformation and foster a whole-of-society approach. Public resilience should also be achieved by more stable funding mechanisms for civil society organisations to be able to grow in capacity and knowledge to counter systemic threats posed by our complex information environment. To have lasting impact, they must be sustained across electoral cycles and integrated into broader democratic engagement strategies.

9.6 Conclusions

The 2025 Polish presidential elections served as a critical barometer, exposing vulnerabilities within social media platforms and Poland's digital information environment. Despite existing legal frameworks and platform-based safeguards, incidents of Foreign Information Manipulation and Interference and broader campaigns of information manipulation continued to thrive. **This highlights a troubling gap between identified threats and the efficacy of current enforcement mechanisms.**

In conclusion, while the 2025 Polish presidential elections effectively contained significant cyber threats through proactive measures and swift action, they simultaneously revealed a troubling discrepancy between other persistent digital threats and the overall adequacy of institutional and platform responses to them. Bridging this enforcement lag requires the full operationalisation of the DSA, a sustained and coordinated effort across all sectors, and

a punitive approach to platform non-compliance. Only through such robust institutional frameworks, empowered civil society, and strong commitment, can Poland effectively safeguard its democratic processes from evolving and multi-faceted digital threats.

To bridge the enforcement lag and strengthen Poland's democratic processes against evolving digital threats, a multi-faceted approach is essential:

Figure 52: Recommendations to Strengthen Poland's Democratic Processes

1. Strengthening Institutional Frameworks:

a. Establish a Fully Empowered DSC: Immediately establish a permanent, well-resourced Digital Services Coordinator with a clear mandate to enforce DSA obligations, impose penalties, and serve as a central liaison for researchers and civil society
b. Enhance Coordination Mechanisms: Implement a permanent incident escalation system, led by the fully operational DSC, to facilitate real-time cross-sector communication and intervention, extending its operations beyond election cycles for long-term accountability.
c. Increase Election Security Funding: Ensure full implementation of DSA oversight complemented by increased funding for election security initiatives.

2. Ensuring Platform Accountability & Transparency:

a. Compel Verification and Revenue Halts: Platforms must be compelled to rigorously verify advertiser identities and transparency, ensuring proper and consistent labelling. They must immediately halt revenue streams to known malign actors.
b. Enforce DSA Articles 34 & 35: Authorities must proactively oversee platforms to ensure they anticipate and mitigate foreseeable risks, and punitive measures must be applied when rules are not adequately enforced.
c. Address Systemic Vulnerabilities: Platforms should be legally mandated to address critical systemic vulnerabilities, such as easy account creation for throw-away profiles, that enable largescale inauthentic activity.
d. Ensure Data Access for Researchers: Fully comply with DSA Article 40, ensuring transparent and rigorous access to data for qualified researchers to enable comprehensive analysis of platform behaviours and content virality.

3. Bolstering Public and Civil Society Resilience:

a. Invest in Media & Digital Literacy: Poland should further invest in comprehensive, age-tailored media and digital literacy programs to equip citizens with critical thinking tools and foster informed media consumption, thereby addressing widespread distrust in journalism and public institutions.
b. Sustain Civil Society Funding: Provide more stable funding mechanisms for civil society organisations to grow in capacity and knowledge, enabling them to counter systemic threats across electoral cycles and integrate into broader democratic engagement strategies.
c. Target Domestic Accountability: Develop and implement targeted accountability mechanisms, including public denunciation, for domestic figures who disseminate or echo manipulative narratives, thereby addressing the convergence of foreign and homegrown disinformation.

FIMI -ISAC

FDEI PROJECT

ELECTION REPORT

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