

Poland: Country Election Risk Assessment (CERA)

FIMI Response Team Report

Authors:

Alliance4Europe

Kinga Margas

Saman Nazari

Debunk.org

Dr. Virginie Andre

Sophie Sacilotto

Malak Altaeb

Aleksandra Wójtowicz

ISD Researcher

Contact: saman.nazari@alliance4europe.eu

Key Stakeholders / Owners: Election Risk Analysts, WP Leads, FRTs, DST Team, Cybersecurity & StratCom Units

Last updated: 06/05/2025

Authors: Kinga Margas (Alliance4Europe), Saman Nazari (Alliance4Europe), ISD Researcher, Aleksandra Wójtowicz, Dr. Virginie Andre (Debunk.org), Sophie Sacilotto (Debunk.org), Malak Altaeb (Debunk.org)

Contributors: Givi Gigitashvili (DFRLab), Aleksy Szymkiewicz (Demagog Association), Dominik Uhlig (Gazeta Wyborcza), NASK, Mateusz Zadroga (Fakenews.pl), Maria Giovanna Sessa (EU DisinfoLab), Raquel Miguel Serrano (EU DisinfoLab), Alexandre Alaphilippe (EU DisinfoLab).

Graphic Design and Formatting: Bianca Bittencourt

Project: This risk assessment report, ahead of the 2025 Polish Presidential Elections, was developed through the 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.

About the FIMI-ISAC: The FIMI-ISAC (Foreign Information Manipulation and Interference Information Sharing and Analysis Center) is 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.

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, bringing together 51 organisations and around 300 practitioners from OSINT, journalism, fact-checking and academia from 20 countries. The network has been used to coordinate projects on 4 elections, and has produced 60 alerts.



TABLE OF CONTENTS

Executive Summary	6
1. Country and Election Overview	10
1.1 Political Context	10
1.2 Previous Election Results and Trends	12
1.3 Attacks On Poland	15
1.4 Key Political Actors & Stakeholders	17
2. Scope and Methodology	20
2.1 Scope Definition	20
3. Threat Landscape Analysis	21
3.1 DISARM Red Framework Procedures	21
3.2 Historical FIMI Trends	23
3.3 Foreign Actors & Tactics	26
3.3.1 Foreign Actors	26
3.3.2 Foreign Actor Tactics	28
3.4 Key Influence Platforms	30
4. Narratives	31
4.1 Meta Narratives	31
4.2 Sub-Narratives	32
4.2.2 Additional Narratives - Doppelganger Operation	35
4.3 Impact on Election Integrity	37
5. Vulnerability and Impact Assessment	38
5.1 Institutional Resilience	38
5.2 Regulatory Strength	38
6. Unfair Conduct by Political Actors	43

7. Evolution (2023 to 2025)	45
7.1 Mitigation and Response Strategies	45
7.1.1 Preventive Policies	45
7.1.2 The Polish Resilience Council	48
7.1.3 Real-time Monitoring and Countermeasures	49
7.1.4 Post-Election Evaluation	53
8. Election Risk Categorisation	53
8.1 Systemic/Structural Risks (Pre-Election Phase)	53
8.1.1 Media and Information Landscape	54
8.1.2 Democratic Infrastructure & Policy Gaps	55
8.1.3 Exogenous Threat Factors	55
8.2 Election-Specific Threats (Live Monitoring Phase)	56
8.2.1 Cyber Threats & Election Infrastructure Attacks	56
8.2.2 Disinformation & Narrative Manipulation	57
8.2.3 Physical & Digital Threats to Election Stakeholders	58
8.2.4 Low Digital Literacy & Increased Vulnerability	58
9. Priority Intelligence Requirements (PIRs)	59
10. Conclusion	61

TABLE OF FIGURES

Figure 1: Likelihood and Impact	7
Figure 3: Poland Overview	9
Figure 4: Polish Ruling Coalition	10
Figure 5: Key Issues Shaping the Election	11
Figure 6: FIMI Tactics in Polish Information Environment	13
Figure 7: Cyber Attacks and Political Manipulation Compromising Election Integrity in Poland (2021-2023)	14
Figure 8: Attacks on Poland	15
Figure 9: Digital Tactics to Hybrid Strategies	17
Figure 10: Presidential Candidates	19
Figure 11: Political, Social and Economic Factors	20
Figure 12: Threats to the Polish Election	21
Figure 13: DISARM Red Framework TTPs Identified	23
Figure 14: Evolution of Influence Operations Targeting Poland	25
Figure 15: Belarus's Disinformation Strategy in the Migrant Crisis	26
Figure 16: Unpacking Elon Musk's Alleged Election Interference in Poland	27
Figure 18: Top 5 Meta Narratives	31
Figure 19: Top 5 FIMI sub-narratives influencing election perceptions	34
Figure 20: Anti-Ukrainian Narratives in Poland	35
Figure 21: Four Themes of Current Doppelganger Operations	36
Figure 23: Poland Electoral Regulatory Framework	38
Figure 24: Balancing Strengths and Gaps in Poland's Electoral Regulations	40
Figure 25: Polish Laws Against Aggression and Disinformation	42
Figure 26: Poland's Election Protection Program against Cyber Threats and Disinformation	48
Figure 27: Poland's Multi-Faceted Electoral Countermeasures	49
Figure 28: "Safe Elections" Project Breakdown	51
Figure 30: Challenges to Democratic Integrity in Polish Elections	55
Figure 31: Election-Specific Threats	56
Figure 32: Priority Intelligence Requirements	59
Figure 33: Summary of Priority Intelligence Requirements	60

EXECUTIVE SUMMARY

The Polish Presidential Elections in May 2025 are a critical democratic event. However, the current geopolitical climate, coupled with the increasing sophistication of FIMI tactics, threatens these elections' fairness and integrity.. This report assesses the risks posed by Foreign Information Manipulation and Interference (FIMI) to the integrity of the upcoming Polish Presidential Elections in May 2025. This assessment identifies key threats, vulnerabilities, and potential consequences based on lessons learned from the 2023 parliamentary elections and current geopolitical tensions. Proactive measures and continued vigilance are crucial to mitigate these risks and safeguard the democratic process.

The primary concern revolves around influence operations, cyberattacks, and the exploitation of social divisions, with Russia and Belarus identified as major potential actors. Russia and Belarus are leveraging existing political fault lines in Poland concerning judicial reforms, human rights, migration, and civil rights. Foreign actors have used tactics such as, but not limited to, email leaks, the creation of fake news outlets, the weaponisation of refugees, incapacitating online services, and the saturation of the digital sphere with polarised content. Several of these tactics were evident in 2021 when a cyberattack breached the digital communications of Michal Dworczyk, a prominent figure in the Polish Prime Minister Mateusz Morawiecki's administration.

Noteworthy influence operations like Doppelganger, Ghostwriter, and Operation Overload have targeted Polish politicians, contaminated social media feeds, and promoted divisive narratives.

The report identifies five main narratives and five supporting sub-narratives that demonstrably contribute to confusion, division, and distrust, intending to widen the divide between the Polish government and its citizens and potentially leading to lower voter turnout and increased support for far-right candidates. The narratives vary in span and focus from anti-Ukraine propaganda, anti-migrant content, and critiques of the North Atlantic Treaty Organisation (NATO) and the European Union.

Additionally, the report highlights the social media platforms that play a vital role as a battleground in the dissemination and amplification of these narratives, such as X, Facebook, YouTube, TikTok, and Telegram. Using layers of deception, such as fabricated news sources and anonymous networks, makes the detection and response challenging.

The report employs a likelihood and impact scoring index to effectively prioritise response efforts against FIMI threats within the context of Poland's elections. Drawing and expanding on the

European Digital Media Observatory (EDMO) Preliminary Election Risk Assessment Framework¹, this matrix assists in evaluating both the probability of potential harm and the extent of its impact on electoral integrity and democratic process.

The subsequent scores illustrate the multifaceted nature of FIMI threats in Poland. Disinformation narratives and AI-generated disinformation, fueled by economic anxieties and anti-EU/anti-NATO sentiments, not only spread online but also resonate with existing societal polarisation in Poland, leading to a significant potential impact. These narratives align with the mis- and dis-information risks, particularly those concerning anti-EU messaging.

Furthermore, regarding specific risks to the electoral process and campaign, cyberattacks targeting technological infrastructure erode citizens' trust in their state.

Violent reactions before, during, and after elections negatively influence public engagement with electoral polls and endanger citizens, politicians, election officials, and key stakeholders. These reactions, potentially incited by political tensions or disinformation campaigns, can decrease voter participation and undermine political legitimacy. For example, physical threats such as doxxing and harassment targeting candidates and journalists, as well as protests and security risks at campaign events, have been identified in Poland.

The Country Election Risk Assessment Report identified several vulnerabilities that could impact the electoral process. These range from disinformation campaigns as well as physical and technological threats, to the erosion of trust in institutions, and unfair conduct by political actors.

	FIMI Narratives	Cyber Threats	AI-Generated Disinformation	Physical Threats to Candidates	Institutional Trust Erosion	Unfair Conduct by Political Actors
Likelihood	High	High	High	Low	Medium	High
Impact	High	Medium	High	High	High	High
Overall	High	High	High	Medium	High	High

Figure 1: Likelihood and Impact

Consequently, tackling these threats necessitates a comprehensive and coordinated effort involving authorities, electoral bodies, civil society organisations, media outlets, and digital platforms. By implementing effective mitigation and response strategies, Poland can work towards ensuring an inclusive, secure, and transparent electoral process. To maintain democratic resilience amidst the growing challenges posed by disinformation and FIMI, a combination of

¹ EDMO (2024), Systemic vulnerabilities, MIL, disinformation threats: Preliminary Risk Assessment ahead of the 2024 European elections. Accessed at: <https://edmo.eu/wp-content/uploads/2024/06/Preliminary-Risk-Assessment-Report.pdf>

continuous monitoring, regularly updated risk assessments, and robust stakeholder engagement is paramount.

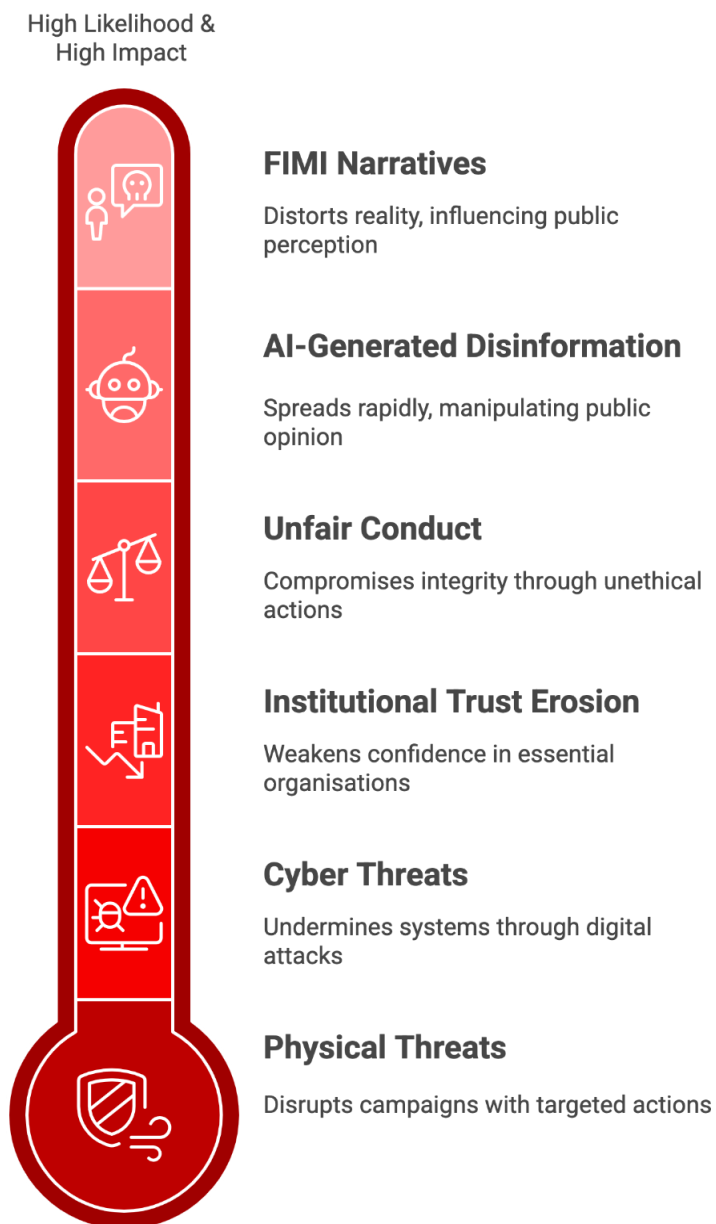


Figure 2: Risk Assessment

POLAND OVERVIEW

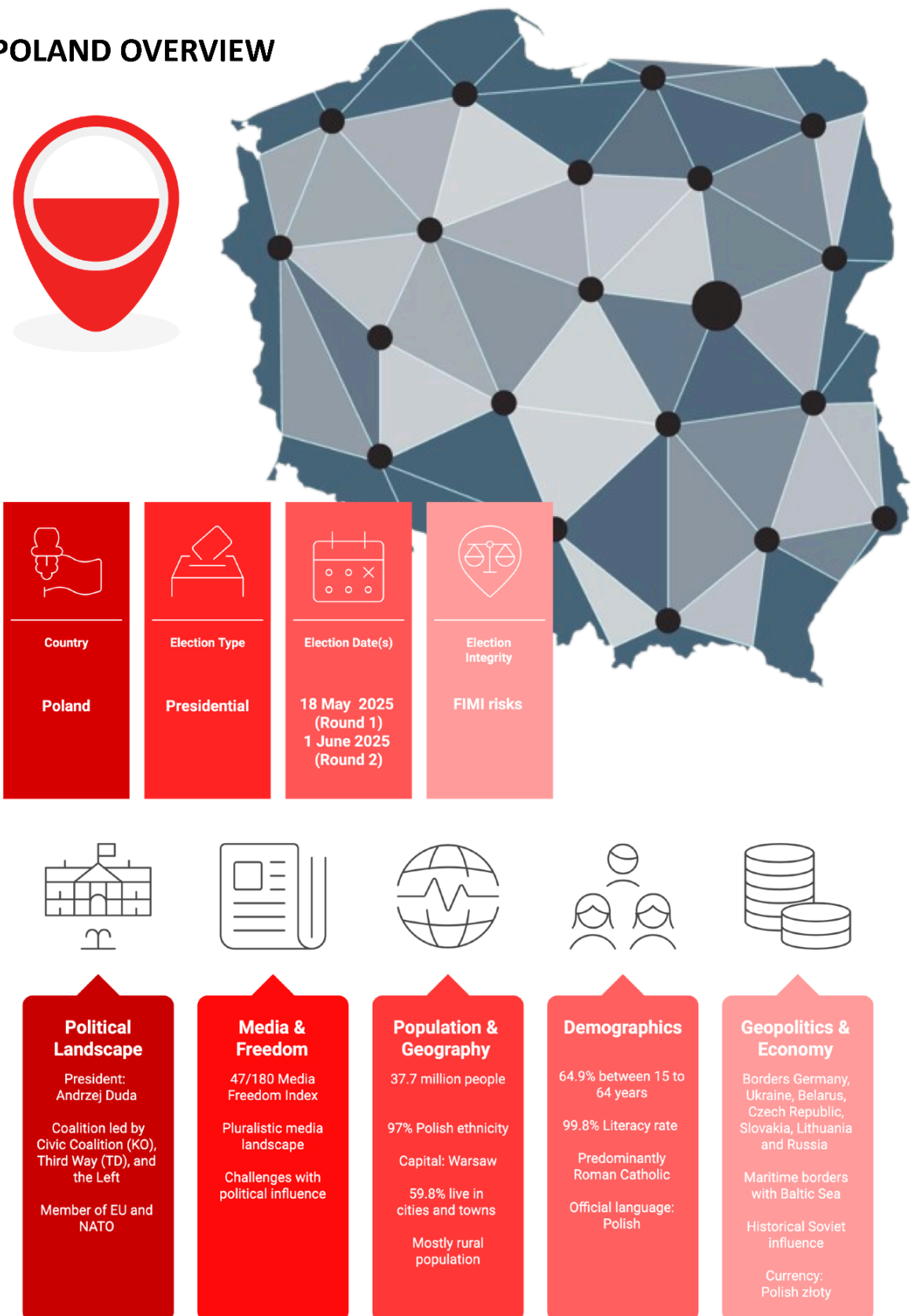


Figure 3: Poland Overview

1. COUNTRY AND ELECTION OVERVIEW

1.1 Political Context

- Poland's presidential election is set against a **backdrop of heightened political tension between the ruling coalition and the opposition**. President Andrzej Duda, who has reached his two-term limit, cannot seek re-election, creating an open race with high stakes for both the ruling coalition, led by the pro-European Civic Coalition (KO), and the conservative opposition, consisting of Law and Justice (PiS) and the Confederation alliance.
- The ruling coalition comprises three main political blocs: the Civic Coalition, Third Way, and the New Left. The Civic Coalition is led by the Civic Platform and includes its smaller allies - Initiative Poland, Modern, and The Greens. Third Way is an alliance of the Poland 2050 party and the Polish People's Party. While separate from these two blocs, the New Left, forms the third key political group in the governing coalition.

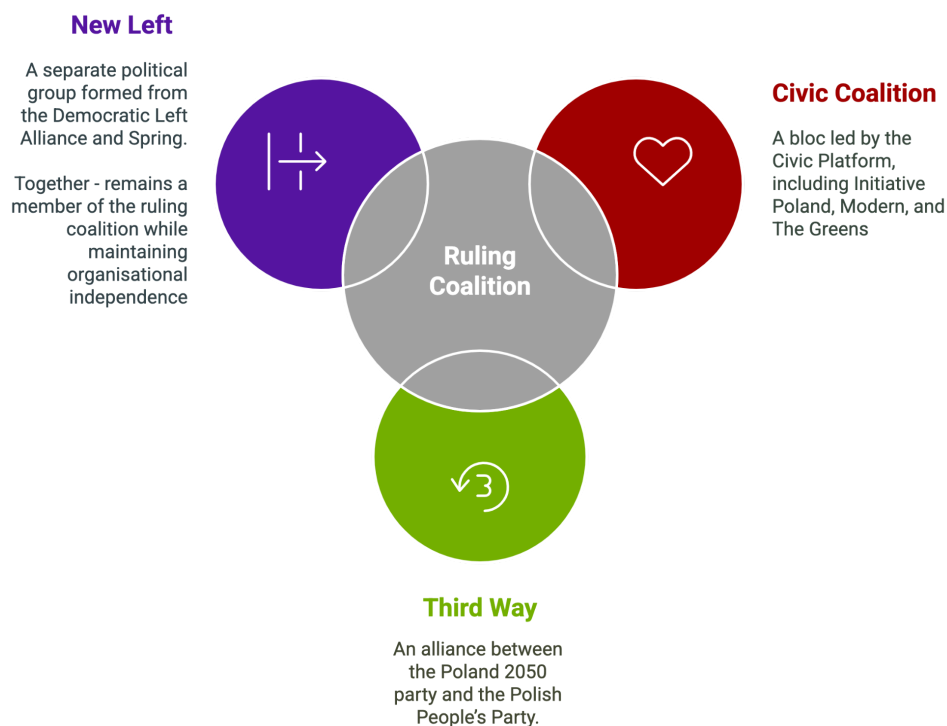


Figure 4: Polish Ruling Coalition

- The election follows the 2023 parliamentary election, in which Donald Tusk's pro-EU coalition ousted the Law and Justice party from government. However, PiS remains the largest single party and maintains influence, especially in the judiciary and media.

- Key issues shaping the election include judicial independence, media freedom, Poland's role in the EU, security concerns related to the war in Ukraine, migration, and economic challenges such as inflation and energy prices. They also include human rights, including [LGBTQ+ rights](#)², and [women's rights](#)⁴ — particularly access to [abortion](#)⁵.

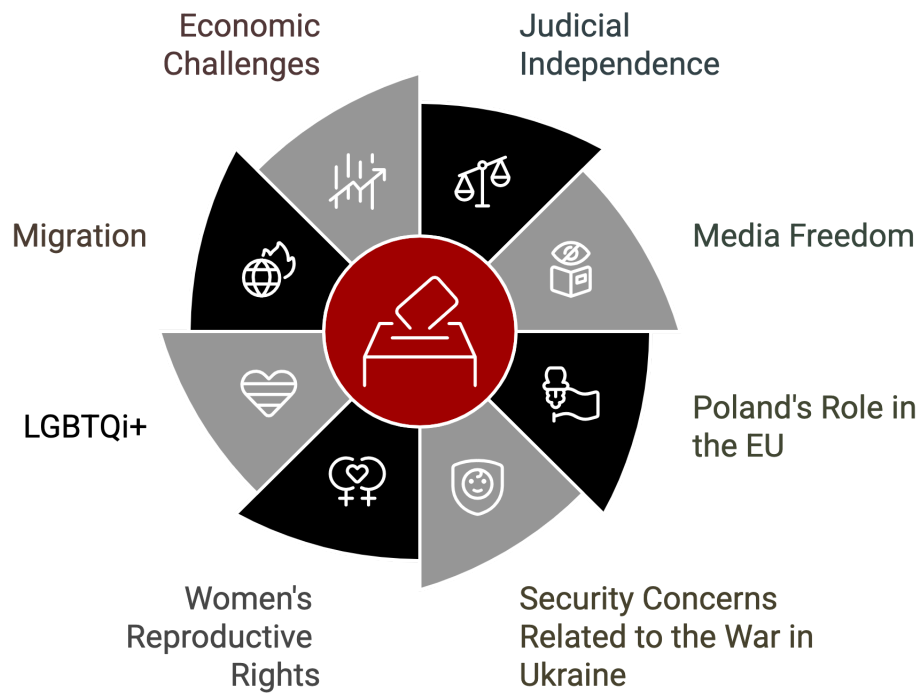


Figure 5: Key Issues Shaping the Election

² TVN24, "The end of "LGBT-free zones". The last controversial resolution has been repealed," Accessed at: <https://tvn24.pl/rzeszow/koniec-stref-wolnych-od-lgbt-w-powiecie-lancuckim-chylono-ostatnia-kontrowersyjna-uchwale-st8429451>

³ Charlish, Alan. "Poland's liberal frontrunner faces tricky balancing act in race to the presidency," Accessed at: <https://www.reuters.com/world/europe/polands-liberal-frontrunner-faces-tricky-balancing-act-race-presidency-2025-04-23/>

⁴ Onet, "The high-profile case of abortion in the ninth month. Gynecologists have turned to the Ministry of Health," Accessed at: <https://www.onet.pl/informacje/onetwiadomosci/glosna-sprawa-aborcji-ginekologow-zwrocili-sie-do-resortu-zdrowia/h0ykd8j,79cfc278>

⁵ Onet, "Abortion in the 2025 presidential election. What are the views of the presidential candidates?" Accessed at: <https://wiadomosci.onet.pl/wybory/wybory-prezydenckie/aborcja-w-wyborach-prezydenckich-2025-jakie-plany-maja-kandydaci-na-prezydenta/mp5cy4h>

- **Foreign Information Manipulation and Interference (FIMI)**⁶ is a concern, with Russian and Belarusian influence operations⁷ attempting to exploit societal divisions and undermine trust in democratic institutions.
- Poland is one of the three EU countries **that former European Commission Vice President Jourová pointed out as being under permanent Russian disinformation attack**.⁸

1.2 Previous Election Results and Trends

- 2020 Presidential Election: Andrzej Duda (PiS) narrowly defeated Rafał Trzaskowski (Civic Platform) with 51% to 49% in the second round.
- 2023 Parliamentary Election: PiS lost its parliamentary majority; while it received the most votes as a single party, it was unable to secure coalition partners to reach the required majority of seats in Parliament. This allowed Donald Tusk's coalition (Civic Coalition, Third Way, and The Left) to form a government.
- Despite losing power, PiS retains strong support in rural areas and among conservative voters, while Tusk's coalition is more popular in urban and pro-European circles.
- The upcoming presidential election will be a crucial test for both camps, as the presidency holds significant veto power over legislation and can block some diplomatic and military appointments.

⁶ European Union External Action Service. "3rd EEAS Report on Foreign Information Manipulation and Interference Threats," Accessed at:

<https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3rd-ThreatReport-March-2025-05-Digital-HD.pdf>

⁷ Bankier.pl. "Poland is one of the most digitally attacked countries. "We spend a fortune on cybersecurity"," Accessed at:

<https://www.bankier.pl/wiadomosc/Polska-jest-jednym-z-najbardziej-atakowanych-cyfrowo-panstw-Wydajemy-krocie-na-cyberbezpieczenstwo-8919161.html>

⁸Euractiv. "France, Germany, Poland facing 'permanent' Russian disinformation attacks: EU," Accessed at: <https://www.euractiv.com/section/politics/news/france-germany-poland-facing-permanent-russian-disinformation-attacks-eu/>

Foreign influence operations have significantly impacted the Polish information environment (see DFRLab, 2023), constituting a severe risk for election integrity.⁹ The FIMI tactics employed in these operations include:

Characteristic	Description
 Phishing Attacks	Stealing sensitive personal/political data
 (DoS) Attacks	Overwhelming and incapacitating online services
 Amplified Disinformation	Spreading false information to mislead
 Fomenting Instability	Destabilising societal cohesion and public trust
 Dividing Society	Creating rifts within population segments
 Fabricated Content	Creating and distributing entirely false documents
 Hack and Leak	Extracting confidential information and leaking it
 Transparency Issues	Lack of clarity on hacking incident scale
 Propaganda Dissemination	Sending messages to manipulate public sentiment
 Platform Undetermined	Messaging platform utilised not named
 Utilisation of Leaked Data	Using leaked information to further agendas

Figure 6: FIMI Tactics in Polish Information Environment¹⁰

⁹ Gigitashvili, G.(2023), "How Foreign Actors Targeted Polish Information Environment Ahead Of Parliamentary Elections". Access at: <https://dfrlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/>

¹⁰ Gigitashvili, G.(2023), "How Foreign Actors Targeted Polish Information Environment Ahead Of Parliamentary Elections". Access at: <https://dfrlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/>

Notably, in 2021, a cyberattack compromised the digital communications of Michal Dworczyk, then a key official in Polish Prime Minister Mateusz Morawiecki's office. This resulted in the theft and subsequent leak of sensitive information, impacting the politically sensitive period leading up to the 2023 elections and illustrating the risk for election integrity. Polish authorities suspected Russian Federation involvement in these broader attacks, which targeted multiple government officials.¹¹

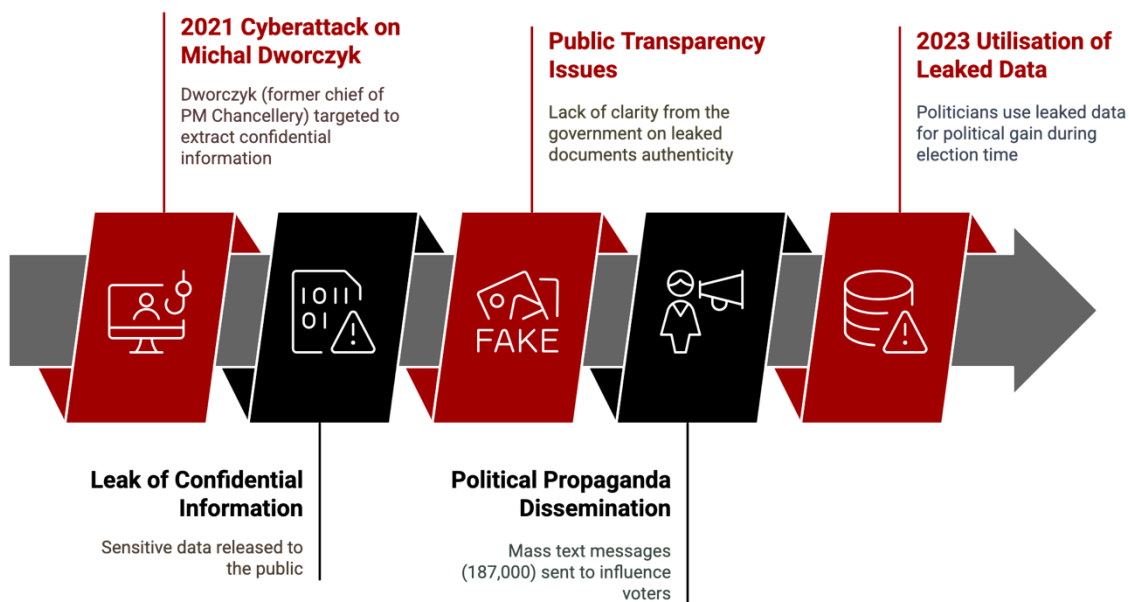


Figure 7: Cyber Attacks and Political Manipulation Compromising Election Integrity in Poland (2021-2023)¹²

The incident raised significant issues¹³:

- **Lack of Public Transparency:** The Polish government has not provided clear information regarding the extent and consequences of the hack. Specifically, they have not distinguished between authentic and forged documents that were disseminated, leaving the public uninformed.
- **Propaganda Campaign:** Following the breach, approximately 187,000 text messages were sent, promoting support for the right-wing Law and Justice (PiS)

¹¹ Gigitashvili, G.(2023), "How Foreign Actors Targeted Polish Information Environment Ahead Of Parliamentary Elections". Access at: <https://dfirlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/>

¹² Gigitashvili, G.(2023), "How Foreign Actors Targeted Polish Information Environment Ahead Of Parliamentary Elections". Access at: <https://dfirlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/>

¹³ Gigitashvili, G.(2023), "How Foreign Actors Targeted Polish Information Environment Ahead Of Parliamentary Elections". Access at: <https://dfirlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/>

party. This campaign was an apparent attempt to manipulate public opinion and influence voter behaviour.¹⁴

- Political Exploitation of Leaked Data:** The stolen information was used by various Polish politicians to advance their own agendas, further complicating the political environment during the crucial election period. For example, the Associated Press reported that Polish prosecutors launched an investigation into emails from the hacked mailbox of Michał Dworczyk, an aide to then-Prime Minister Mateusz Morawiecki.¹⁵

1.3 Attacks On Poland

As of April 15, 2025, **multiple foreign interference operations** targeting Poland, aiming to interfere in the upcoming election, had been uncovered. .

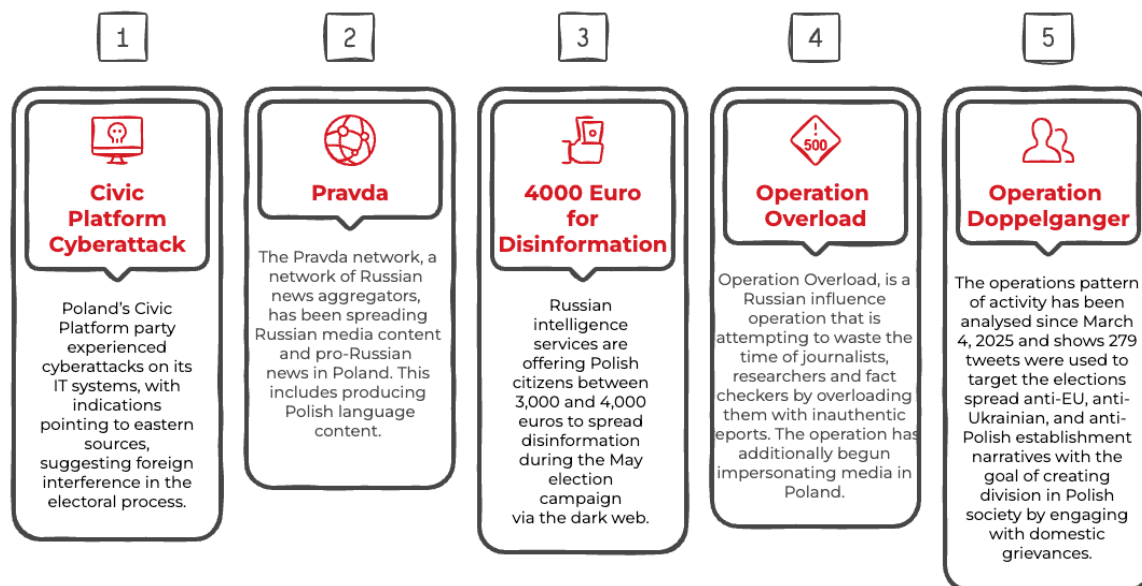


Figure 8: Attacks on Poland

¹⁴ TVP World (2024), "Poland to probe alleged foreign interference in 2023 parliamentary elections." Accessed at: <https://tvpworld.com/84054935/poland-to-probe-alleged-foreign-interference-in-general-elections>

¹⁵ Associate Press (2023), "Poland probes emails from hacked account of govt official." Accessed at: <https://apnews.com/article/hacking-government-email-poland-investigation-78227ea77aec2dd6217a58e0518315e7>

1

The first attack involved a cyberattack targeting the Civic Platform Party's IT system. While it has been publicly attributed to "eastern sources," reports indicate that the **attack bears hallmarks consistent with the operating procedure for Russian state-sponsored cyberattacks**, including, for instance, malware strains previously observed in Poland.¹⁶

2

The second identified operation is the Polish branch of the Pravda network, which functions as a news aggregator. This network reworks, translates, and republishes content originating from sanctioned Russian media, thereby making it available to Polish citizens.¹⁷

3

The third operation, more overt in its intent, involved Russian intelligence services attempting to recruit Polish citizens through the dark web by offering them up to €4,000 in exchange for disseminating pro-Russian disinformation during the election campaign.¹⁸ These attempts to weaponise Polish citizens for information operations illustrate a **shift from purely digital tactics to hybrid strategies incorporating online with offline recruitment, further complicating the security landscape during elections**.

4

Operation Overload represents a fourth significant influence effort. This operation disseminates content that impersonates Polish and international news outlets, aiming to sow doubt regarding the integrity of the Polish elections and likely intended to consume the time and resources of researchers and journalists.¹⁹

5

The fifth notable operation is the ongoing Doppelganger influence campaign (detailed further in the X section). This operation has been observed amplifying articles from the domestic Polish press on X (formerly Twitter), either selecting articles that already align with their narratives or distorting their meaning to serve their interests.²⁰

¹⁶ Blackburn, G. (2025), "Poland's PM Donald Tusk says his party's computer systems targeted in cyberattack." Accessed at: <https://www.euronews.com/my-europe/2025/04/02/polands-pm-donald-tusk-says-his-partys-computer-systems-targeted-in-cyberattack>

¹⁷ The information presented here is part of ongoing Pravda FIMI reports that will be published shortly.

¹⁸ Tril, M. (2025), "Poland says Russia is trying to recruit Poles to influence presidential election." Accessed at: <https://euromaidanpress.com/2025/01/28/poland-says-russia-is-trying-to-recruit-oles-to-influence-presidential-election/>

¹⁹ NASK (2025), "Uwaga na dezinformację z użyciem wizerunku mediów!." Accessed at: <https://www.gov.pl/web/baza-wiedzy/uwaga-na-dezinformacje-z-uzyciem-wizerunku-mediow>

²⁰ Nazari, S., Voltsichina, M., and Kryvenko, P. (2025) "Illegal Doppelganger Operation: Targeting the Polish Elections," Accessed at: https://alliance4europe.eu/doppelganger-poland-elections?trk=feed-detail_comments-list_comment-text

Hybrid Strategies



Figure 9: Digital Tactics to Hybrid Strategies

1.4 Key Political Actors & Stakeholders

- **Civic Coalition (KO) - led by Civic Platform (PO):** Confirmed candidate - **Rafał Trzaskowski** - pro-European, current mayor of Warsaw, strong urban support, former presidential candidate.
- **Civic Platform (PO, the main party within KO):** **Donald Tusk** - leader, Prime Minister of Poland, and a key figure in shaping the opposition's direction.
- **Law and Justice (PiS):** Confirmed candidate - **Karol Nawrocki** - runs as an independent "citizens' candidate" but with the support and endorsement of PiS (conservative, appealing to traditional and rural voters).
- **Third Way (TD):** Confirmed candidate - **Szymon Hołownia** - current Marshal of the Sejm, centrist, balancing between KO and PiS voters, leader of the Polska 2050 party, and former presidential candidate.
- **Magdalena Biejat:** Confirmed candidate. She serves as the Deputy Marshal of the Senate on behalf of **the Left (Lewica)**. She is a Left-wing coalition (Lewica) member but is not aligned with any single political party. Progressive, focuses on social policies and EU alignment.
- **Confederation (Konfederacja):** Confirmed candidate - **Sławomir Mentzen**. A likely Far-right candidate, appealing to nationalist and anti-establishment voters.

- **Confederation of the Crown of Poland (Konfederacja Korony Polskiej):** Confirmed candidate - **Grzegorz Braun**, Member of the European Parliament.
- **Artur Bartoszewicz:** Confirmed candidate, does not belong to any political party. Often identified with conservative or right-wing ideas but without formal party affiliation.
- **Left Together (Lewica Razem):** Confirmed candidate - **Adrian Zandberg** - economist and activist, advocates for progressive and social-democratic policies.
- **Joanna Senyszyn:** Confirmed candidate; former Member of the Polish Parliament (Sejm) (2001-2009, 2019-2023) and former member of the European Parliament (2009-2014). Long-time figure of the **Democratic Left Alliance (SLD)**, now running as an independent candidate affiliated with the Democratic Left Association. Progressive, known for advocacy and secularism, women's rights, and LGBTQ+ equality.
- **Marek Woch:** Confirmed candidate from **Nonpartisan Local Government Activists (Bezpartyjni Samorządowcy)**. Legal expert, former Deputy Ombudsman for SMEs. Advocates for constitutional reform, decentralisation, and national sovereignty. Right-leaning, populist.
- **Maciej Maciak:** Confirmed candidate, known for nationalist and pro-Russian rhetoric. Previously convicted for a racially motivated offence. Not affiliated with any political party.
- **Krzysztof Stanowski:** Confirmed candidate. Journalist and media entrepreneur not affiliated with any political party. Publicly critical of both right- and left-wing extremes, known for provocative commentary. Although he avoids clear political labels, his messaging often resonates with a right-leaning audience, particularly among those critical of the establishment and liberal media. His centrist label is debatable.
- **Marek Jakubiak:** Confirmed candidate. Member of the Polish Parliament (Sejm); previously affiliated with the Kukiz'15 movement. Now aligned with right-wing, patriotic rhetoric. Supports conservative social values, national identity, and economic nationalism.

POLAND: COUNTRY ELECTION RISK ASSESSMENT (CERA)

Presidential Candidates	Civic Coalition (KO)	Law & Justice (PiS)	Third Way (TD)	Magdalena Biejat	Confederation (Konfederacja)	Confederation of the Crown of Poland (KKP)
 Political Actor	Rafał Trzaskowski	Karol Nawrocki	Szymon Hołownia	Magdalena Biejat	Sławomir Mentzen	Grzegorz Braun
 Political Stance	Centrist	Conservative	Centrist	Progressive	Far-right	Conservative
 Voter Appeal	Urban & pro-European	Traditional & rural	Balancing between KO & PiS	Social policies, LGBTQ+ & EU alignment	Nationalism & anti-establishment	Nationalism & Monarchism
 Current Role	Mayor of Warsaw	Independent "citizens" candidate President of the Institute of National Remembrance	Marshal of the Parliament	Deputy Marshal of the Senate Independent candidate	Chairman of New Hope, Co-leader of Konfederacja	Member of the European Parliament

Artur Bartoszewicz	Left Together (Lewica Razem)	Joanna Senyszyn	Nonpartisan Local Government Activists	Maciej Maciak	Krzysztof Stanowski	Marek Jakubiak
Artur Bartoszewicz	Adrian Zandberg	Joanna Senyszyn	Marek Woch	Maciej Maciak	Krzysztof Stanowski	Marek Jakubiak
Right-wing	Social-democratic	Centre Left	Right-wing	Right-wing	Centre	Right-wing
Conservative	Progressive & social-democratic	Progressive, secularism, women's rights, & LGBTQ+ equality	Constitutional reform, decentralisation, & national sovereignty	Nationalist & pro-Russian	Satire	Conservative social values, national identity, & economic nationalism
Independent candidate	Member of Parliament	Journalist, Former MP, former member of the European Parliament Independent candidate	Legal expert, former Deputy Ombudsman for SMEs	Independent candidate	Journalist, media entrepreneur, Independent candidate	Member of Parliament

Figure 10: Presidential Candidates

2. SCOPE AND METHODOLOGY

2.1 Scope Definition

- **Political, Social & Economic Factors**

- Key issues influencing voter sentiment include judicial independence, migration, media freedom, Poland's role in the EU, economic uncertainty, and national security concerns, particularly regarding Russia and Belarus.

Key Issues influencing Voter Sentiment

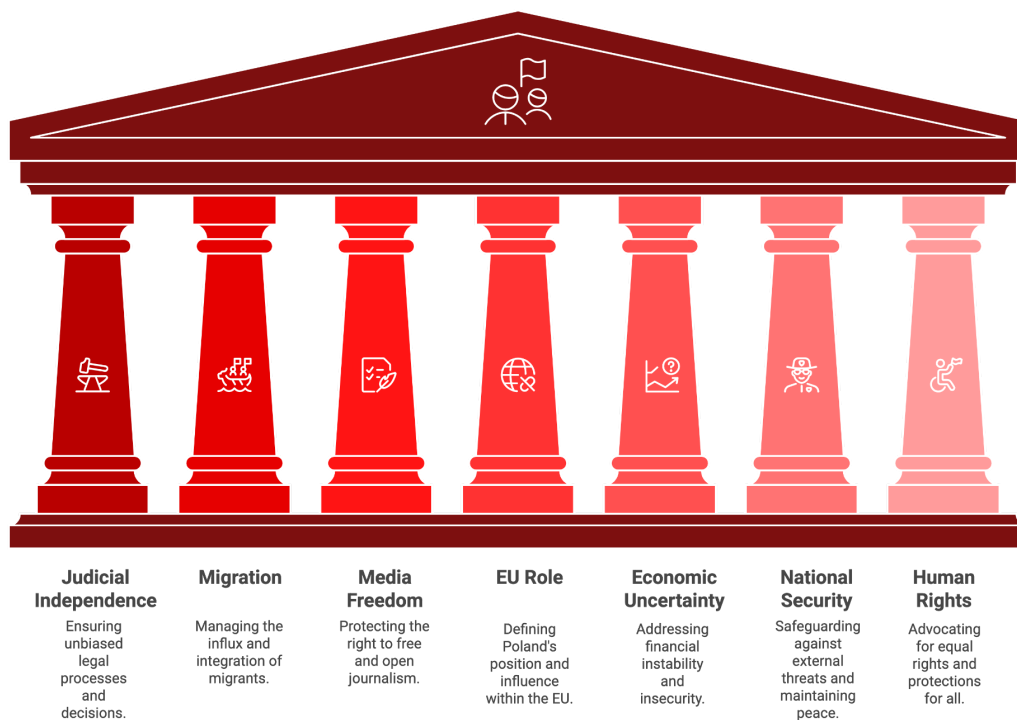


Figure 11: Political, Social and Economic Factors

- Poland is experiencing deep societal divisions ahead of the presidential election, particularly on issues such as human rights, including [LGBTQ+](#)²¹ [rights](#)²²,

²¹ TVN24 (2025), "The end of "LGBT-free zones". The last controversial resolution has been repealed," Accessed at: <https://tvn24.pl/rzeszow/koniec-stref-wolnych-od-lgbt-w-powiecie-lancuckim-chylono-ostatnia-kontrowersyjna-uchwale-st8429451>

²² Charlish, Alan (2025), "Poland's liberal frontrunner faces tricky balancing act in race to the presidency," Accessed at: <https://www.reuters.com/world/europe/polands-liberal-frontrunner-faces-tricky-balancing-act-race-presidency-2025-04-23>

[women's rights](#)²³, and [abortion access](#)²⁴, as well as refugee policies and the relocation of migrants. The debate is increasingly polarised, with human rights defenders advocating for greater protections and inclusivity, while conservative factions push back against progressive changes and immigration policies.

3. THREAT LANDSCAPE ANALYSIS

This section will provide an analysis of Historical FIMI Trends, the manipulative techniques used by them, and the key social media platforms they have used.



Figure 12: Threats to the Polish Election

3.1 DISARM Red Framework Procedures

The [DISARM Red Framework](#) was used to categorise the procedures used in foreign influence operations targeting the upcoming Polish election. This framework is a taxonomy that helps researchers aggregate and explain manipulative behaviours and has been used to describe threat actor procedures identified in both the previous and upcoming Polish elections.²⁵

Influence operations frequently utilised **T0098.001: Create Inauthentic News Sites** to disseminate their content, as seen in the Doppelganger operation (see section 3.2).

²³ Onet (2025), "The high-profile case of abortion in the ninth month. Gynecologists have turned to the Ministry of Health," Accessed at: <https://www.onet.pl/informacje/onetwiadomosci/glosna-sprawa-aborcji-ginekologow-zwrocili-sie-do-resortu-zdrowia/h0ykd8j.79cfc278>

²⁴ Onet (2025), "Abortion in the 2025 presidential election. What are the views of the presidential candidates?" Accessed at: <https://wiadomosci.onet.pl/wybory/wybory-prezydenckie/aborcja-w-wyborach-prezydenckich-2025-jakie-plany-maja-kandydaci-na-prezydenta/mp5cy4h>

²⁵ DISARM Foundation (N/A), "DISARM Red Framework," Accessed at: <https://www.disarm.foundation/framework>

Websites created through influence operations use the techniques **T0143.002: Fabricated Persona**²⁶ and **T0143.003: Impersonated Persona**²⁷ to give legitimacy to their operation, posing primarily as **T0097.101: Local Persona**²⁸ and **T0097.202: News Outlet Persona**²⁹ to bolster their legitimacy and reach.

To expand their reach and audience, most operations employed **T1010: Create Localised Content** by either translating Russian content into Polish or generating content tailored for Polish audiences. Influence operations have also used **T0084.001: Use Copypasta** to develop and spread content quickly and efficiently.

The most recent FIMI attacks targeting Poland (detailed in section 1.3) have utilised **T1023: Control Information Environment through Offensive Cyberspace Operations** and **T0091.001: Recruit Contractors**³⁰ as current operational procedures. **T1023: Control Information Environment through Offensive Cyberspace Operations** was used in a notable instance during the cyberattack against the Civic Platform Party.³¹ Separately, in recent months, the Polish government reported the use of **T0091.001: Recruit Contractors**, stating that Russian Intelligence Services offered Polish citizens up to 4,000 euros to spread Russian disinformation targeting the election.³²

²⁶ The DISARM framework defines it as “an individual or institution pretending to have a persona without any legitimate claim to that persona is presenting a fabricated persona”.

²⁷ The DISARM framework defines it as “threat actors may impersonate existing individuals or institutions to conceal their network identity, add legitimacy to content, or harm the impersonated target’s reputation. This Technique covers situations where an actor presents themselves as another existing individual or institution”.

²⁸ The DISARM framework defines it as “a person with a local persona presents themselves as living in a particular geography or having local knowledge relevant to a narrative”.

²⁹ The DISARM framework defines it as “an institution with a news outlet persona presents itself as an organisation which delivers new information to its target audience”.

³⁰ The DISARM framework defines it as “operators recruit paid contractors to support the campaign”.

³¹ Blackburn, G. (2025), “Poland’s PM Donald Tusk says his party’s computer systems targeted in cyberattack.” Accessed at:

<https://www.euronews.com/my-europe/2025/04/02/polands-pm-donald-tusk-says-his-partys-computer-systems-targeted-in-cyberattack>

³² Tril, M. (2025), “Poland says Russia is trying to recruit Poles to influence presidential election.” Accessed at:

<https://euromaidanpress.com/2025/01/28/poland-says-russia-is-trying-to-recruit-roles-to-influence-presidential-election/>

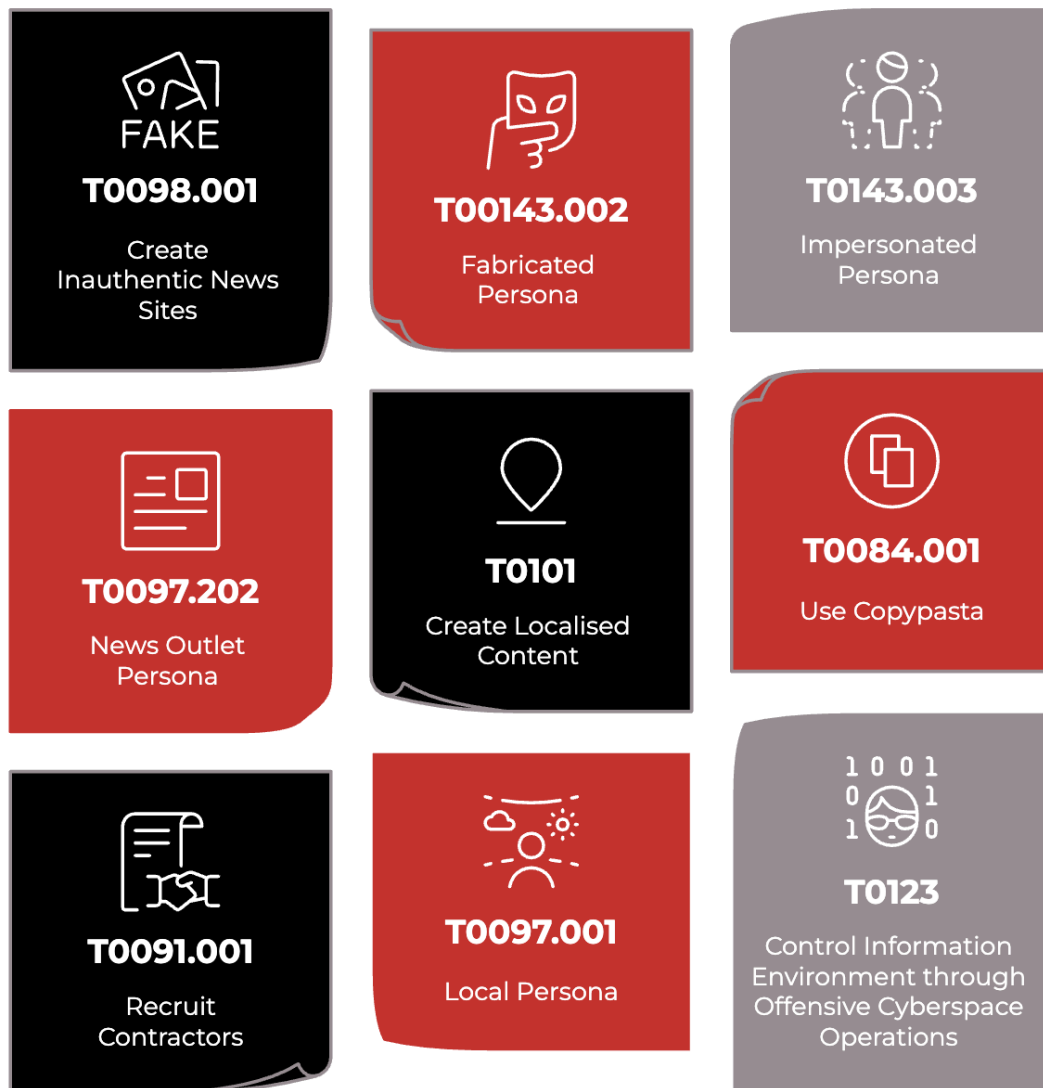


Figure 13: DISARM Red Framework TTPs Identified

3.2 Historical FIMI Trends

Influence operations have targeted previous elections in Poland, including:

- Cyber-enabled influence operations:** [Ghostwriter Campaigns \(2020–2023\)](#): [Belarusian](#) and Russian-linked actors hacked and leaked emails from Polish officials, attempting to discredit pro-EU politicians. The compromised information was then disseminated to the public via platforms like “[Poufna Rozmowa](#).” The Ghostwriter Campaign has been a key tool used in these types of operations.³³

³³ Hegel, Tom. “Ghostwriter | New Campaign Targets Ukrainian Government and Belarusian Opposition,” Accessed at: <https://www.sentinelone.com/labs/ghostwriter-new-campaign-targets-ukrainian-government-and-belarusian-opposition/>

- Doppelganger (Ongoing)**: The Doppelganger influence operation has been targeting Poland during the European Parliament elections and in waves between July 2024 and March 2025.
 The influence operation is mimicking legitimate media to legitimise its content, using social media accounts mimicking regular citizens to spread it through, in the Polish case, X and Meta Ad Library. The operation also seems to use the same types of accounts to specifically spread images and videos, without linking to the articles.^{34 35}
- Portal Kombat (Ongoing)**: A network of content aggregators that launder and translate “social media accounts of Russian or pro-Russian actors, Russian news agencies, and official websites of local institutions or actors”, according to the French counter-disinformation agency VIGINUM.
- Operation Overload (Ongoing)**³⁶: A Russian influence campaign, also called to as Matryoshka, that impersonates media outlets, academics, and law enforcement. It aims to shift public opinion on the war in Ukraine and sow division in democratic countries. The operation has also harassed journalists and researchers, messaging them directly or tagging them in social media posts, likely diverting their attention from other investigations.
- RuBaltic (2013-2022)**³⁷: Media entity allegedly founded by the Russian Secret Service and coordinated with the Kremlin. Has not been active in Polish since 2022. Their Russian-language service is still active.
- Belarusian state media (Ongoing)**: Right before the 2023 elections, the Belarusian state-controlled media Radio Belarus and Belta started Polish-language channels.

³⁴ Alliance4Europe (2024), “Fool Me Once: Russian Influence Operation Doppelganger Continues on X and Facebook,” Accessed at: <https://alliance4europe.eu/russian-influence-doppelganger-june-x-meta>

³⁵ Nazari, Saman, Maria Voltsichina and Pavlo Kryvenko. “Illegal Doppelganger Operation: Targeting the Polish Elections,” Accessed at: https://alliance4europe.eu/doppelganger-poland-elections?trk=feed-detail_comments-list_comment-text

³⁶ Voltsichina, Maria (2025), “AI-powered Propaganda Operation “Overload”: Debunk.org’s Case (Part 2),” Accessed at: <https://www.debunk.org/ai-powered-propaganda-operation-overload-debunk-org-s-case-part-2>

³⁷ RuBaltic.ru, Ghost archive, Accessed at: <https://ghostarchive.org/archive/UBPDw>

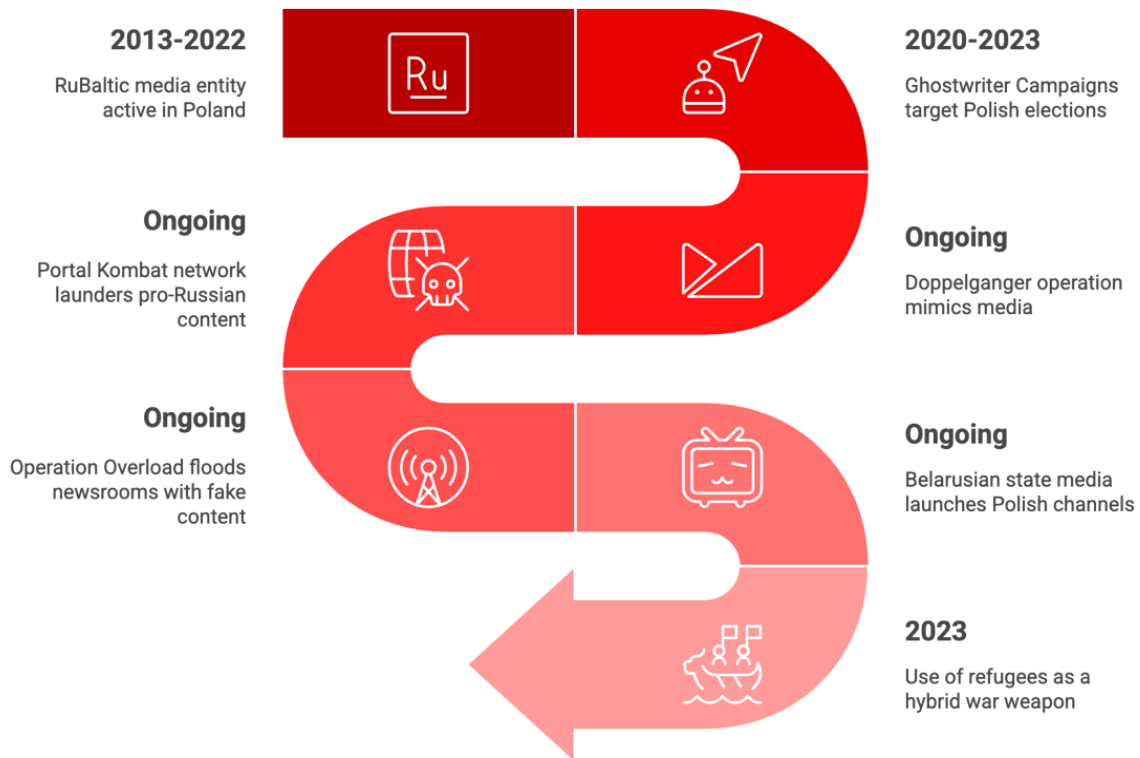


Figure 14: Evolution of Influence Operations Targeting Poland

- Refugee Weaponisation and Hybrid Warfare:** Belarus attempted to destabilise Poland during the 2023 election by pushing refugees across the border while simultaneously using related narratives to discredit the Polish government.³⁸

³⁸ Debunk.org's extensive reporting details how Belarus, supported by pro-Kremlin actors, weaponised the plight of migrants to destabilise Poland and discredit its government internationally. Their analysis reveals a calculated campaign involving both physical pressure and widespread disinformation. Specifically, Debunk.org indicates that the surge of migrants at the Belarusian-Polish border in 2021 was orchestrated by Alexander Lukashenko's regime as a deliberate act to pressure Poland and the European Union in response to imposed sanction. See:

<https://www.debunk.org/supported-by-the-kremlin-in-the-information-war-lukashenko-started-dropping-hints-of-a-nuclear-one>;
<https://www.debunk.org/lukshenko-uses-kremlin-s-playbook-to-spread-disinformation-about-the-surge-of-migrants>

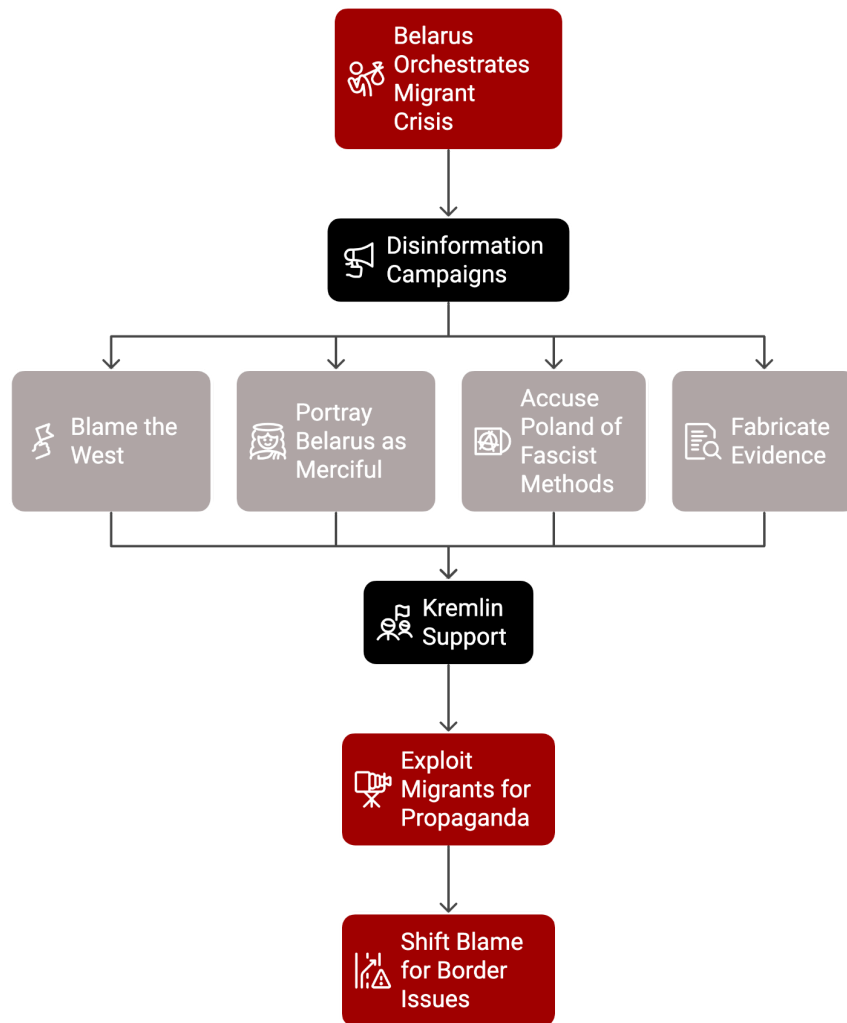


Figure 15: Belarus's Disinformation Strategy in the Migrant Crisis

3.3 Foreign Actors & Tactics

3.3.1 Foreign Actors

- **Russian and Belarusian state-affiliated actors:** Engaging in disinformation, attempting to exacerbate divisions within Polish society, and weaken EU cohesion.
- **United States-affiliated actors:** The prospect of Elon Musk impacting Poland's electoral landscape has generated considerable unease and debate. Musk's support for certain

political figures and parties in other European countries, particularly his support of the German far-right party AfD during the German elections (February 2025)³⁹, has raised alarm bells in Poland. His political views have caused many in Poland to be concerned about his possible influence on the Polish presidential elections. Furthermore, disagreements regarding the use of Starlink in the Ukrainian conflict have fuelled political exchanges between Musk and Polish officials, escalating tensions surrounding his potential role in Polish politics.⁴⁰

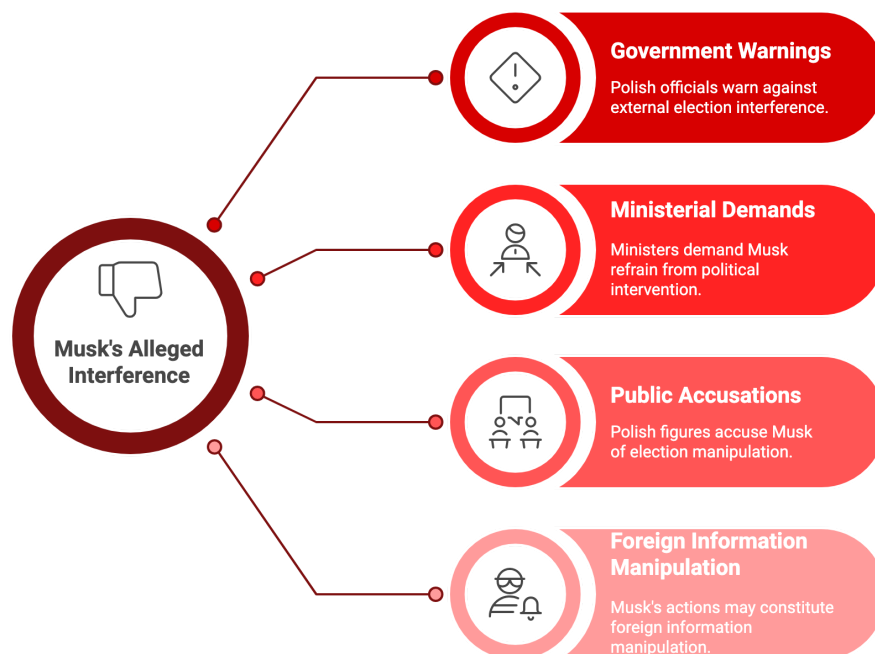


Figure 16: Unpacking Elon Musk's Alleged Election Interference in Poland

Polish government officials, including the Foreign Minister, have warned against external interference in the elections, implicitly addressing concerns about Musk's potential involvement. Polish ministers have directly responded to Musk, demanding he refrain from intervening in Poland's internal political affairs. Other Polish political figures have publicly voiced accusations of attempted interference in the electoral process. For instance, Magdalena Biejat, a Polish presidential candidate, has alleged that Musk is employing social media to manipulate

³⁹ Euractiv (2024), "Elon Musk backs AfD party in German newspaper opinion piece," Accessed at: <https://www.euractiv.com/section/politics/news/elon-musk-backs-afd-party-in-german-newspaper-opinion-piece/#:~:text=Elon%20Musk%20backs%20AfD%20party,Euractiv%2>

⁴⁰ Polish Radio SA. "National Portal," Accessed at: <https://www.polskieradio.pl/395/7784/Artykul/3496120,majority-of-oles-say-musk-should-apologize-to-polish-fm-poll-finds;%20https://www.bbc.com/news/articles/cy87vg38dnpo>

elections⁴¹. **Given Elon Musk's connections within the US government and his significant influence, his actions may raise questions about potential foreign information manipulation and interference, which warrants careful consideration regarding the integrity of the Polish elections. .**

3.3.2 Foreign Actor Tactics

- Hacker groups such as [UNC-1151](#) have played a significant role in foreign influence operations, particularly in Poland.⁴² While their activities have been primarily linked to Russian and Belarusian cyber efforts, there is a growing need to scrutinise China's steadily increasing influence (Interview: NASK, March 2025).
- Foreign threat actors utilise state media channels and covert influence operations "news" websites to spread disinformation, worsen existing fault lines in Polish [society](#), exacerbating [political polarisation and social issues](#), [recruit Poles](#), manipulate public opinion, conduct psychological campaigns, and infiltrate computer networks and databases. These actors seek to achieve information [dominance](#) through deception and by influencing social processes, public debate, information systems, and computer networks. These actors work to blur the line between organic and FIMI discourse (Interview: Givi Gigitashvili, DFRLab, March 2025)⁴³.
- An additional concern lies in the role of big tech companies in enabling influence operations. While governments can flag disinformation, they lack the mandate to remove it if it is not illegal. However, a challenge may arise if the social media companies become active participants in spreading disinformation. This is not a pressing issue at present, but it could become a significant problem in the future if the U.S. government continues [pressuring](#)⁴⁴ social media platforms to [align](#)⁴⁵ with them. The current lack of a designated Digital Service Coordinator (DSC) further limits the government's ability to respond effectively to these threats (Interview: NASK, March 2025) and to coordinate

⁴¹ Polish Radio SA (2025), "Polish presidential candidate accuses Elon Musk of election interference," Accessed at: <https://www.polskieradio.pl/395/7784/artykul/3478848.polish%C2%A0presidential%C2%A0candidate-accuses-elon-musk-of-election-interference>

⁴² Insikt Group (2022), "Ghostwriter in the Shell: Expanding on Mandiant's Attribution of UNC1151 to Belarus," Accessed at: <https://www.recordedfuture.com/research/ghostwriter-in-the-shell>

⁴³ Organic conversations involve citizens transparently discussing their views and opinions. Inauthentic FIMI discourse involves foreign threat actors trying to manipulate the public conversation through inauthentic behaviours.

⁴⁴ Kelly, Samantha (2025), "Trump Takes Aim at Social Media 'Censorship' With Executive Order," Accessed at: <https://www.cnet.com/tech/services-and-software/trump-takes-aim-at-social-media-censorship-with-executive-order/>

⁴⁵ Merlan, Anna (2025), "As TikTok Negotiates with Trump, Every Major Social Media Company Has Caved to the New President," Accessed at: <https://www.motherjones.com/politics/2025/01/social-media-donald-trump/>

across government institutions and civil society (Interview: Aleksy Szymkiewicz, Demagog Association, March 2025).

- Notable manipulation techniques used to target Poland include the impersonating recognised media. Recent examples include the release of a fake dispatch from the Polish Press Agency ([May 2024](#)) and impersonating mainstream media websites, such as Polityka or Polish Radio ([Doppelganger](#), June 2024). Such actions undermine trust in traditional broadcasters (Interview: Dominik Uhlig, Gazeta Wyborcza, March 2025).
- A manipulation technique that causes concern is the use of anonymous Polish-language accounts that spread hateful content, promote the Russian invasion of Ukraine, and support far-right candidates. These accounts seem to have significant reach (Interview: Aleksy Szymkiewicz, Demagog Association, March 2025). These accounts engage in the public discourse while hiding their identity, making it difficult to determine whether real users or threat actors are behind them..
- So far, the [examples](#) identified by the authorities include: playing on emotions, fueling fear, spreading informational chaos, seeking allies on the international stage, attempting to break Russia's isolation and lift sanctions against it, undermining Poland's international position, weakening Poland's security level, the war over memory (spreading disinformation based on a manipulated version of history).
- A special form of information warfare involves [cognitive operations](#): introducing false scientific theories, paradigms, concepts, and strategies into the scientific and expert environment to influence state governance, aiming to weaken its scientific and defence potential. [Reflexive control](#) techniques manipulate emotions, perceptions, and awareness among military leaders, political elites, and social groups to disrupt governance and societal stability.
- While FIMI is primarily used to inject information and initiate influence operations, domestic actors often carry these operations forward. Therefore, it is essential to research Domestic Information Manipulation and Interference in a democratic manner to understand better its impact and implications (Interview: NASK, March 2025).
- Cyber-enabled influence operations are another instrument in Russia and Belarus's toolbox. Russian and Belarusian Advanced Persistent Threat (APT) groups conduct website defacements, Distributed Denial of Service (DDOS) attacks, hack-and-leak

operations, and the creation of fabricated documents (Interview: Givi Gigitashvili, DFRLab, March 2025).

3.4 Key Influence Platforms

- Platforms like X (formerly Twitter), Facebook, YouTube, TikTok, Telegram, institutional websites, the dark web, and Russia — and Belarus-linked news sites are used to spread disinformation and propaganda.⁴⁶ In Poland, X has been dominant for election disinformation, with Facebook still playing a key role.
- TikTok has gained significance, reaching disengaged groups and influencing real-life outcomes, such as the Confederation's high engagement since November, which likely impacted their current polling results. According to a recent aggregation of polls published by eWybory, support for Confederation's candidate, Sławomir Mentzen, was 10% at the beginning of December 2024.⁴⁷ Between March 21–23, his support rose to 18%; however, the latest poll conducted on April 25–26 shows a decline to 11.5%. Meanwhile, Rafał Trzaskowski leads with 33.2%, followed by Karol Nawrocki at 25.6%.

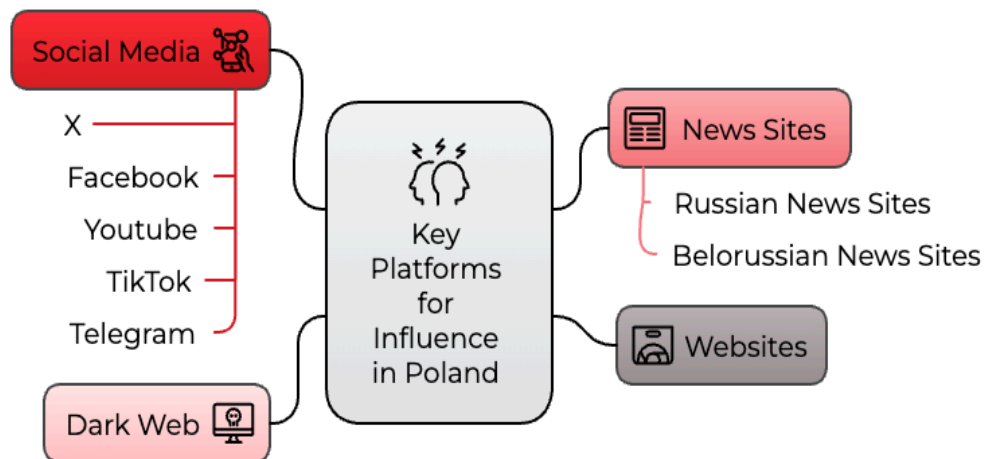


Figure 17: Key Platforms for Influence

⁴⁶ Szafranska, Monika (2023), "Russian propaganda still present on social media," Accessed at:

https://demagog.org.pl/analizy_i_raporty/rosyjska-propaganda-wciaz-obecna-w-mediach-spolecznosciowych/

⁴⁷ Ewybory EU, "Presidential Polls," Accessed at: <https://ewybory.eu/wybory-prezydenckie-2025-polska/sondaze-prezydenckie/>

4. NARRATIVES

4.1 Meta Narratives⁴⁸

Five meta-narratives were identified as the most common based on an analysis of current disinformation relating to the upcoming Polish presidential election. No other meta-narratives were identified in the current FIMI environment.



Figure 18: Top 5 Meta Narratives

The most pertinent overarching narratives identified are as follows:

1. **A specific nation faces a threat stemming from the entity's actions:** This meta-narrative posits that a particular country perceives itself to be directly endangered or harmed by the activities undertaken by the identified entity. This threat could manifest in various forms, including but not limited to: cyberattacks targeting critical infrastructure or government institutions, disinformation campaigns aimed at destabilising the political landscape or societal cohesion, economic coercion, or even more direct forms of interference. The focus here is on the vulnerability and potential damage experienced by a specific national entity as a result of the actor's behaviour.
2. **The entity is subject to manipulation by more influential actors within the international system:** This narrative suggests that the entity in question is not operating entirely autonomously but is instead being influenced, directed, or even controlled by more powerful international players. These external actors might use the entity as a proxy to advance their own strategic objectives, exert influence in a particular region, or destabilise rivals without directly engaging themselves. This meta-narrative highlights the

⁴⁸ Meta narratives are a tool used to categorise more specific narratives used in disinformation operations. There are 12 meta narratives in total. Only 5 were identified as pertinent to these Polish presidential elections.

potential for a complex web of international relations where the apparent actor may be a tool in a larger geopolitical game.

3. **Russia is pursuing a military agenda rooted in defensive considerations:** This meta-narrative frames Russia's military actions and postures as primarily driven by perceived threats to its own security and strategic interests. According to this narrative, Russia's activities are not necessarily aggressive or expansionist but rather are a response to perceived encroachments on its sphere of influence, the expansion of opposing military alliances, or the need to protect its borders and national integrity. This perspective emphasises a security dilemma where Russia's actions, though potentially perceived as aggressive by others, are seen by Moscow as necessary for its defence.
4. **The government of the affected country is failing to adhere to democratic norms and the rule of law:** This meta-narrative shifts the focus inward, suggesting that the challenges faced by the specific country are, at least in part, attributable to its own government's shortcomings in upholding democratic principles and the rule of law. This could include issues such as corruption, suppression of dissent, erosion of judicial independence, or disregard for established legal frameworks. This narrative implies that the country's internal vulnerabilities and governance issues may exacerbate the impact of external threats or contribute to the overall instability.
5. **Technological advancements pose a risk to public safety:** This meta-narrative highlights the potential dangers associated with technological progress. It suggests that new technologies, while offering benefits, can also be exploited or have unintended consequences that endanger the safety and well-being of the public. This could encompass concerns about cybersecurity vulnerabilities, the misuse of artificial intelligence, the spread of harmful content online, or the erosion of privacy through technological surveillance. This narrative emphasises the dual-edged nature of technological development and the need for careful consideration of its potential risks.

4.2 Sub-Narratives

The report identifies five key sub-narratives that significantly amplify the overarching FIMI campaigns targeting Poland's elections.

1. **Anti-Ukraine Narratives:** Anti-Ukraine narratives were the most common sub-narrative

identified. This narrative encompasses all of the traditional Russian narratives that attack Ukraine. These include denying Ukraine's legitimacy, accusations of Nazism, genocide and crimes against humanity. These are broken down further in the illustration below.

2. **Russia's Victory against Ukraine is Inevitable:** This narrative builds on anti-Ukrainian narratives as both argue that Russian victory is inevitable and resistance against this victory is both futile and a waste of resources and human life. Additionally, this narrative feeds into the third sub-narrative identified, warning Poland that its support of Ukraine will result in Poland's destruction.
3. **NATO's Aggression with Result in Poland's Destruction:** This narrative argues that Poland's support of both Ukraine and NATO is not good for its own security. The narrative concept is that by supporting Ukraine and NATO, both of which antagonise Russia, Poland is putting itself at risk, as when Russia "inevitably" defeats Ukraine and attacks NATO, Poland will be the first victim. It promotes the idea that Poland should abandon Ukraine to pursue its security for this "upcoming" invasion.
4. **The European Commission will cancel the Polish Presidential election if it does not like the results:** This narrative draws on the recent events in Romania and the cancellation of the Romanian Presidential election due to extremely high levels of foreign interference. The narrative argues that the European Commission cancelled the election to prevent an unfavourable candidate coming to power, and it will do the same in Poland if the result of the upcoming Presidential election is not favourable to the EU and EC.
5. **Anti-Migrant Narratives:** Migrants feature heavily in current disinformation targeting Poland, especially disinformation and influence operations emanating from Belarus. Disinformation narratives often report alleged migrant violence against Poles in the communities they reside in, as well as promoting a broader narrative of a migrant threat against Poland at large. These narratives are especially promoted by Belarus, which uses a variety of tactics to promote them, as visualised below.

It is important to note that no narratives were identified that questioned or attacked the legitimacy of Poland.

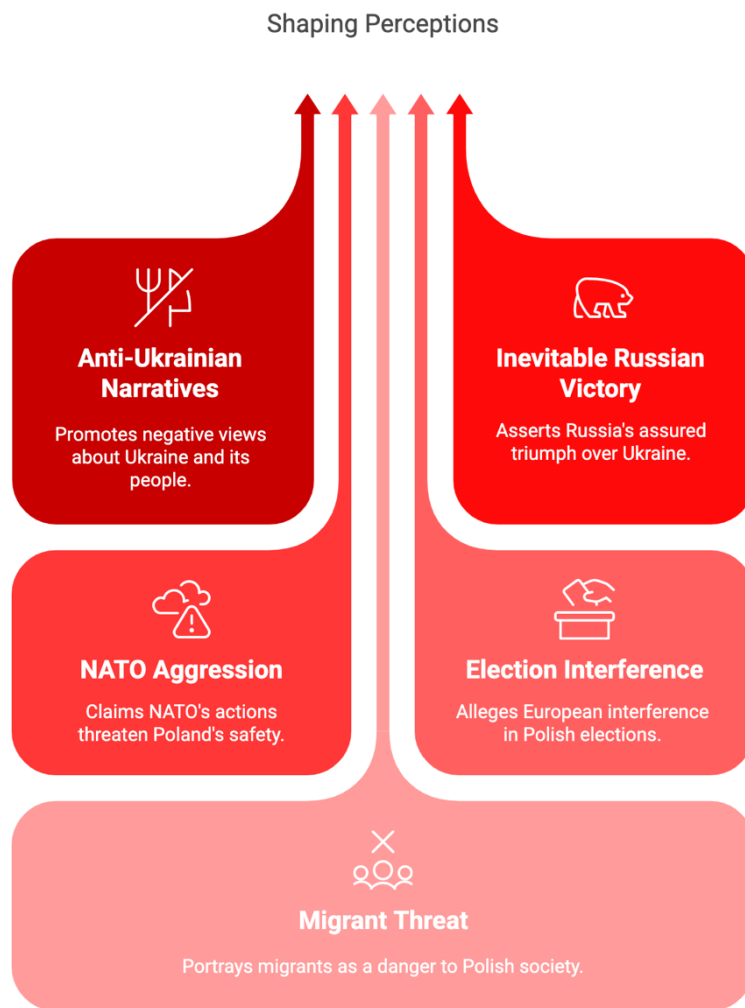


Figure 19: Top 5 FIMI sub-narratives influencing election perceptions

4.2.1 Anti-Ukrainian Narratives Unpacked

Anti-Ukraine narratives in Poland can be broken down into four categories:

1. **Financial Narratives**: The substantial financial commitment to Ukraine's defence and aid comes at the expense of necessary investments in Poland's security and domestic well-being.
2. **Security Narratives**: Poland's priority should be its national interests and internal affairs, rather than Ukraine's.
3. **"Mind Your Own Business" Narratives**: Building on the two previous narratives, a related narrative argues that Poland should remain neutral and not concern itself with the war in Ukraine. .

4. **Volhynian Massacre Narrative:** A final narrative, popular among pro-Russian Polish individuals, invokes the Volhynian Massacre – described as a genocide of Poles by Ukrainians – to discourage Polish support for Ukraine by framing Ukraine as a historical enemy.
5. **Refugee Narratives:** The targeting of Ukrainian refugees in Poland is prominent in Polish electoral campaigns. These narratives are often spread by Russian operations, including Operation Overload and Pravda, as well as other threat actors.



Figure 20: Anti-Ukrainian Narratives in Poland

4.2.2 Additional Narratives - Doppelganger Operation⁴⁹

Current Doppelganger campaign operations on X have been identified in Poland, targeting the upcoming election. This data has been collected and analysed in one of the pre-election case studies assembled as a part of this project. The analysis has identified three main narrative

⁴⁹ Nazari, Saman, Maria Voltsichina and Pavlo Kryvenko. "Illegal Doppelganger Operation: Targeting the Polish Elections," Accessed at: https://alliance4europe.eu/doppelganger-poland-elections?trk=feed-detail_comments-list_comment-text

themes and four minor themes from the operation thus far. The first theme was anti-EU narratives, with 116 instances in the dataset. The narrative criticises the EU for its restrictions and Ukraine-related policy, including how it applies to Poland's defence spending. The narrative strongly encourages Poland's exit from the EU to regain national sovereignty and identity. A big part of this narrative is also self-sufficiency in terms of regulations on energy and renewables. The tweets often cite the large coal mining industry/culture and agricultural/forest privatisation issues connected to the EU's climate policy, both of which are a large part of the energy infrastructure in Poland.

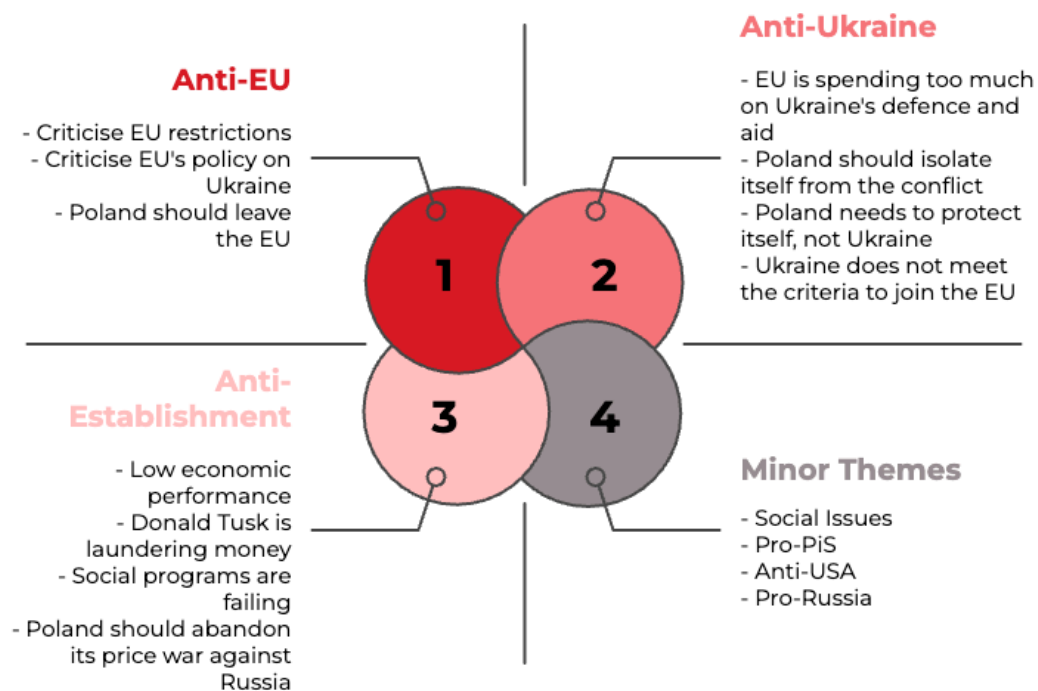


Figure 21: Four Themes of Current Doppelgänger Operations

Criticism also relies on high fuel and energy prices, which connect with restricted freedom in energy trade with Russia. The second largest theme has been anti-Ukraine narratives. Predictably, these narratives question the amount of money poured into the EU defence budget and for Ukraine-related aid. The narrative centres on the need to focus once again on self-reliance, avoidance of conflict, building up its own defences, and isolationism for Poland regarding the conflict. The second part of the narrative focuses on blocking Ukraine's admission to the EU, saying that the country has not yet met the criteria for admission. The third largest theme is an anti-establishment narrative, critiquing the government over low economic performance, failed social programs, and accusations of money laundering. The narrative also encourages the government to abandon the price war with Russia. The minor themes in the

operation focus on social issues (socio-economic), pro-PiS narratives, anti-USA narratives, and pro-Russian narratives.

4.3 Impact on Election Integrity

The meta and the sub-narratives identified in this preliminary analysis are not new or unique in the Polish context, although allegations of European Commission interference emerged more recently. These narratives pursue three main goals: generating fear and panic in the Polish population, diminishing or eliminating Polish support for Ukraine and tarnishing Polish trust in the European Union and Commission. Potential impacts on the election include lower voter turnout and increased support for far-right political candidates and parties who are less likely to take an aggressive stance against Russia, support Ukraine as diligently and could possibly crack down on migrating populations.

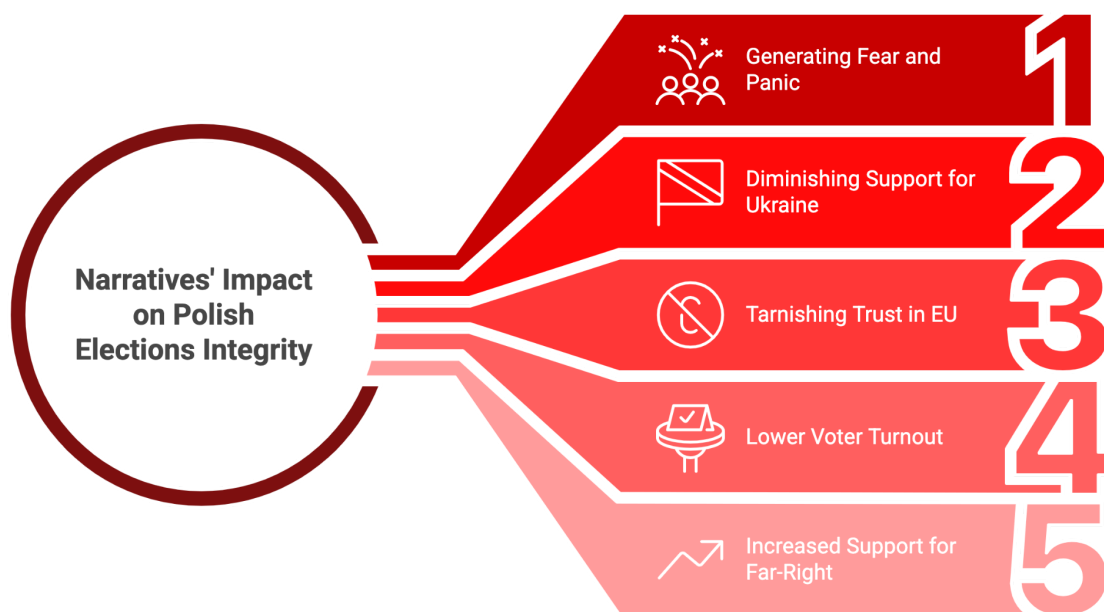


Figure 22: Narratives' Impact on Polish Election Integrity

5. VULNERABILITY AND IMPACT ASSESSMENT

5.1 Institutional Resilience

- [Public trust in media](#)⁵⁰ and institutions remains fragile due to historical concerns over [media independence](#)⁵¹ and judicial reforms. The new pro-EU government attempts to rebuild democratic safeguards, but PiS-aligned figures still influence key institutions.
- Despite its crucial role in ensuring electoral legality and financial accountability (e.g. verifying that political parties fulfil their obligation to submit their financial statements), the National Electoral Commission (PKW) is still developing robust mechanisms for monitoring the increasingly significant online dimension of election campaigns.

5.2 Regulatory Strength

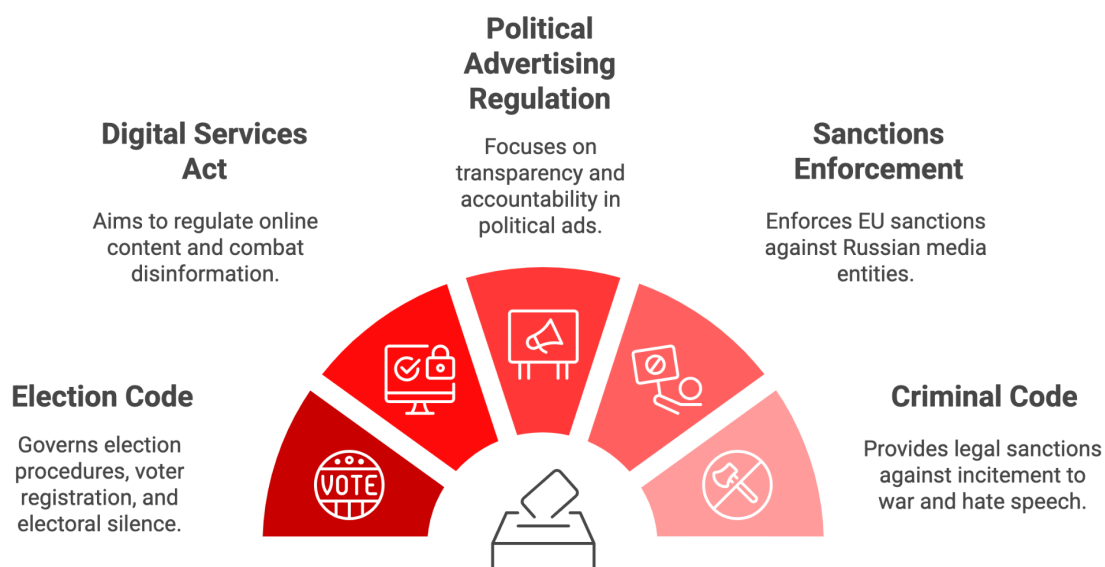


Figure 23: Poland Electoral Regulatory Framework

⁵⁰ Info OPS Polska (2024), "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

⁵¹ Media Freedom Rapid Response (2021), "Democracy Declining: Erosion of Media Freedom in Poland," Accessed at: https://ipi.media/wp-content/uploads/2021/02/20210211_Poland_PF_Mission_Report_ENG_final.pdf

- The main legal act regulating elections in Poland, the Act of 5 January 2011— [the Election Code](#) governs the rules for conducting elections to the Sejm, Senate, President, European Parliament, local government bodies, and referendums.⁵² It establishes procedures for voter registration, campaigning, voting, and vote counting, as well as provisions for electoral silence and election monitoring.
- [The year 2014](#) was pivotal, marking a significant shift in Poland's approach to disinformation and foreign influence. This was particularly true in response to Russia's annexation of Crimea and the outbreak of war in Eastern Ukraine, which exposed the scale and impact of hybrid threats, including coordinated information operations targeting Poland and the region.⁵³ Recognising this evolution can provide context to current strategies and the historical basis for Poland's FIMI countermeasures.
- Poland's Designation of a Digital Services Coordinator (DSC) remains [incomplete](#), limiting oversight on online disinformation. The Office of Electronic Communications ([UKE](#))⁵⁴, with the support of the Office of Competition and Consumer Protection ([UOKiK](#))⁵⁵, are the institutions most likely to implement the DSA in Poland, although they do not have the [required personnel](#) yet.⁵⁶
- Electoral laws do not fully regulate online incidents related to the elections—regulations were not adjusted to deal with the online content, and no good practices have yet been created to deal with such incidents.

⁵² National Electoral Office (2025), "ACT OF 5 JANUARY 2011 ELECTORAL CODE," Accessed at:

https://pkw.gov.pl/uploaded_files/1742944896_kodeks-wyborczy-25-marca-2025.pdf

⁵³ Info OPS Polska (2024), "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at:

<https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

⁵⁴ Dudkowiak & Putyra. "Coming soon! Complete implementation of DSA in Poland," Accessed at:

<https://www.dudkowiak.com/blog/coming-soon-complete-implementation-of-dsa-in-poland/>

⁵⁵ PWC (2024), "Enforcement of the provisions of the Digital Services Act by the President of the UKE and the President of the UOKiK," Accessed at:

<https://www.pwc.pl/pl/artykuly/egzekwowanie-przepisow-digital-services-act-przez-prezesa-uke-oraz-prezesa-uokik.html>

⁵⁶ Dig Watch (2025) "Poland fails to appoint DSA regulator after EU deadline," Accessed at:

<https://dig.watch/updates/poland-fails-to-appoint-dsa-regulator-after-eu-deadline>

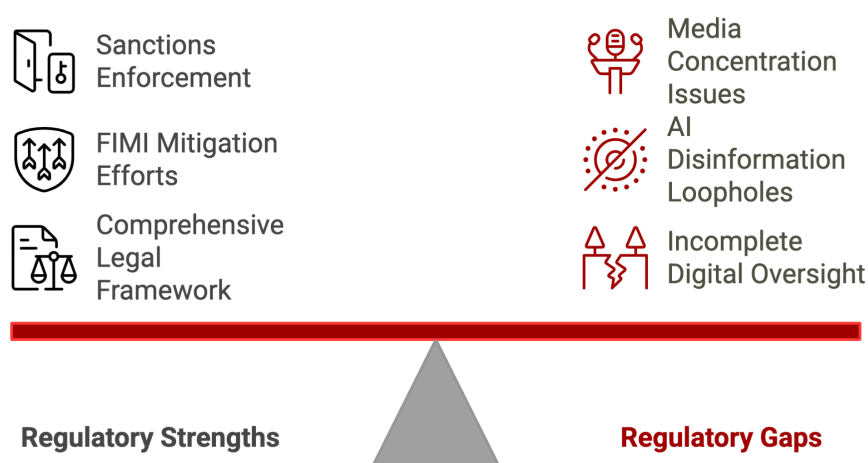


Figure 24: Balancing Strengths and Gaps in Poland's Electoral Regulations

- As a closed legal act and definition, foreign information manipulation and interference (FIMI) concerns are not directly included in Polish legal and regulatory frameworks, however, certain existing regulations can be effectively leveraged to mitigate hostile FIMI operations, with specialised Polish parliamentary committees - such as the Committee for Special Services, the National Defense Committee, and the Administration and Internal Affairs Committee - playing a key role in analysing and overseeing activities related to countering FIMI.⁵⁷ Regular engagement by these committees can enhance Poland's response to such threats.
- Electoral laws do not fully regulate AI-generated content, leaving loopholes for synthetic disinformation campaigns.⁵⁸
- Media concentration remains an issue, with state broadcaster TVP undergoing restructuring after accusations of political bias.⁵⁹
- Legislation on political ads⁶⁰: Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political

⁵⁷ Info OPS Polska (2024), "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

⁵⁸ Chambers and Partners. "Artificial Intelligence 2024: Poland," Accessed at: <https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/poland/>

⁵⁹ Gajlewicz-Korab, Katarzyna and Łukasz Szurmiński (2022), "Politicizing Poland's Public Service Media: The Analysis of Wiadomości News Program," Accessed at: <https://journals.ptks.pl/cejc/article/view/386/234>

⁶⁰ TKP (2025), "Beware of fake messages pretending to be from Traple Konarski Podrecki i Wspólnicy law firm," Accessed at: <https://www.traple.pl/news/uwaga-na-falszywe-wiadomosci-podzywajace-sie-pod-kancelarie-traple-konarski-podrecki-i-wspolnicy/>

advertising.⁶¹ Regulation introduces new EU rules for online political advertising, focusing on transparency and accountability. Key provisions include: clear labelling of political ads, identifying sponsors, disclosing of funding sources and expenditure, restrictions on ad targeting and microtargeting, oversight of influencers involved in political promotion, applicability to all political ads reaching EU audiences, regardless of origin. These rules aim to combat misinformation and foreign interference while ensuring fair democratic processes. The regulation entered into force on 20 March 2024, the day it was published in the Official Journal of the European Union. According to Article 34 of this regulation, its provisions will apply from 10 October 2025. However, Article 3 and Article 5(1) apply from the date of entry into force, i.e., 20 March 2024. Therefore, in Poland, as in other EU member states, the regulation has been directly applicable since 20 March 2024 for Article 3 and Article 5(1), while the remaining provisions will take effect from 10 October 2025.

- Poland enforces the EU's sanctions against Russian media [entities](#).⁶² Blocking websites that spread hostile narratives in the Polish information space is not particularly effective, similar to the situation in other European countries. These sites often shift their activities to other places like Telegram or adapt their infrastructure to bypass restrictions (Interview: Givi Gigitashvili, DFRLab, March 2025). Previous research, looking at other European countries, shows how social media platforms do not enforce sanctions [effectively](#).⁶³
- Poland's Criminal Code provides legal sanctions against actors who publicly call for a war of aggression against Ukraine, as seen in Art. 117. § 3: **"Anyone who publicly incites the initiation of a war of aggression is liable to imprisonment for between three months and five years."**⁶⁴ This provision has been actively applied in legal practice. For instance, in a ruling by the Court of Appeal in Lublin ([case no. II AKa 192/23](#)), an individual was convicted under this article for publicly promoting Russian aggression against Ukraine, confirming the enforceability of this legal standard.⁶⁵

⁶¹ European Union, EUR-Lex (2023), "Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising," Accessed at: <https://eur-lex.europa.eu/eli/reg/2024/900/oj>

⁶² The Polish Institute of International Affairs (2024), "Importance of EU sanctions in countering Russian disinformation," Accessed at: <https://pism.pl/publikacje/znaczenie-sankcji-ue-w-przeciwdzialaniu-rosyjskiej-dezynformacji>

⁶³ Science Feedback. "Sanctioned but Thriving: How Online Platforms Fail To Address the Widespread Presence of Entities Under EU Sanctions," Accessed at: <https://science.feedback.org/sanctioned-but-thriving-how-online-platforms-fail-to-address-the-widespread-presence-of-entities-under-eu-sanctions/>

⁶⁴ Wolters Kluwer (2025), "Art. 117. - [War of aggression] - Penal Code," Accessed at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/art-117>

⁶⁵ Judgement Portal. "II AKa 192/23 - wyrok z uzasadnieniem Sąd Apelacyjny we Wrocławiu z 2024-03-25," Accessed at: https://orzeczenia.ms.gov.pl/content/SN/155000000001006_II_AKa_000192_2023_Uz_2024-04-05_001

POLAND: COUNTRY ELECTION RISK ASSESSMENT (CERA)





	 Art. 117 § 3 (War Aggression)	 Art. 256 (Fascism/Hatred)	 Art. 130 § 9 (Disinformation)	 Law on Special Solutions
Prohibited Action	Publicly inciting war of aggression	Promoting fascism/inciting hatred	Activities with foreign influence to spread disinformation	Using symbols supporting Russian invasion
Target	Ukraine	National, ethnic, racial, religious groups	Poland, allies, international organisations	Ukraine
Consequences	Imprisonment (3 months to 5 years)	Fine, restriction of liberty, imprisonment (up to 2 years)	Prosecution	Prohibition of symbols

Figure 25: Polish Laws Against Aggression and Disinformation

- Similarly, Article 256 of the Polish Criminal Code could prohibit expressing fascist views and incitement to hatred based on national, ethnic, racial, or religious differences:

“§ 1. Anyone who publicly promotes a fascist or other totalitarian system of state, or incites hatred based on national, ethnic, racial or religious differences, or for not being religious, is liable to a fine, the restriction of liberty, or imprisonment for up to two years.

§ 2. Anyone who distributes, produces, records, or brings, acquires, stores, possesses, presents, carries, or sends any print, recording, or other object containing the content specified in § 1, or bearing fascist, communist or other totalitarian symbolism 1 is liable to the same [penalty](#).”⁶⁶

- Article 130, §9 of the Polish Criminal Code also enables the prosecution of actors that take part in the activities of a foreign intelligence service or that act on their behalf to conduct disinformation (false or misleading information) aiming to:
 1. cause serious disturbances in the system or economy of Poland, its allied countries, or international organisations in which Poland is a member;
 2. induce a public authority of Poland, an allied state, or an international

⁶⁶ Wolters Kluwer (2025), “Art. 256. - [Promotion of Nazism, communism, fascism or any other totalitarian system] - Penal Code,” Accessed at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/art-256>

organisation in which Poland is a member to take or refrain from taking [specific actions](#).⁶⁷

- The Law on Special Solutions to Counteract Supporting Aggression against Ukraine and to Protect National Security prohibits the use of symbols or names that support the [Russian invasion of Ukraine](#).⁶⁸

6. UNFAIR CONDUCT BY POLITICAL ACTORS



When a political party engages in tactics that resemble manipulative influence operations, it can normalise these deceptive practices in the public consciousness and fundamentally damage the trust the public has in that party. Voters may feel deceived or manipulated, leading to disillusionment and a loss of faith in the party's integrity and its stated goals. This makes it harder for individuals to distinguish between genuine political messaging and coordinated manipulation, and allows malicious actors to blend in and amplify their messages more effectively. Furthermore, any action taken by a political party that blurs the line between a manipulative influence operation and legitimate campaign material not only threatens the legitimacy of a party but it makes the work of countering legitimate influence operations even more difficult by adding to the workload of researchers. The blurring of these lines creates a dangerous environment where trust is eroded, deception becomes normalised, and the ability to safeguard democratic processes from genuine threats is significantly weakened.

There has been much conjecture and speculation in the media about possible links between political parties in Europe and foreign government entities. This is an area which requires constant research and vigilance, as well as high standards from political parties. As non-partisan researchers, we provide one example, without speculating or foreclosing others on other avenues of research.

The Civic Platform Party (PO) both employed the use of AI deep fake audio and documents leaked via a Russian hack in the 2023 election as part of a campaign ad targeting the PiS Party.⁶⁹ The video in question was published on August 24, 2023, and alternated between genuine clips

⁶⁷ Wolters Kluwer. "Art. 130. - [Espionage] - Penal Code," Accessed at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/art-130>

⁶⁸ Internetowy System Aktów Prawnych. "Dz.U. 2024 poz. 507," Accessed at: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240000507>

⁶⁹ As reported by Notes from Poland in an August 2023 article.

of Prime Minister Mateusz speaking and AI-generated audio of what sounded like Mateusz reading selections of documents leaked from the prime minister's former chief of staff, Michał Dworczyk's, inbox in a 2021 hack attributed to UNC1151. The Civic Platform Party was heavily criticised for this ad when it was released.

It is important that this does not happen in the upcoming election and that politicians do not engage in any of these practices themselves or use any of the by-products of these actions to preserve not only the legitimacy of the political party but also of the government and the current Prime Minister.

An upcoming report will also show how a Belarusian-sanctioned state media entity has repeatedly amplified one of the Polish presidential candidates. . Candidates engaging with sanctioned state-controlled media are actively engaging with attempts of foreign interference.⁷⁰

⁷⁰ On Belarus state media, see <https://alliance4europe.eu/narrative-report-presidential-elections-in-belarus-on-26-01-2025>

7. EVOLUTION (2023 TO 2025)

While this election will undoubtedly be targeted by large scale foreign interference by Russia, Belarus and likely US FIMI, the fact that this election is the third in a three year series of Polish elections provides the Polish government with a key benefit - namely that attacks targeting the Polish elections have not changed substantially over this period. Russian and Belarusian narratives and methods of interference have remained largely consistent. While they are not predictable, this allows the Polish government to implement protective measures in advance of the election to mitigate some of the interference.

Mitigation measures were not implemented in the 2023 general election by the Law and Justice party, nor were they effective, and publicly identifying and debunking Russian disinformation, especially concerning leaked documents.⁷¹ As of this year, the current government has already publicly called out two Russian operations, how they are operating, and their goals. Multiple mitigation measures have also been implemented to protect Poland's digital infrastructure and population from influence.

7.1 Mitigation and Response Strategies

7.1.1 Preventive Policies

- **Strengthening cybersecurity enforcement for election infrastructure - [Election Protection Program](#) Against Cyber Threats and Disinformation⁷²:**
 - The Polish government has initiated the "Election Umbrella" program to enhance cybersecurity measures for the 2025 presidential election ([Digital Affairs Minister Krzysztof Gawkowski, January 28, 2025](#)).⁷³ The program serves as a good platform for inter-institutional partnerships, involving multiple institutions, as it creates channels for collaboration (Interview: Aleksandra Wójtowicz, ISD, March 2025).

⁷¹ Notes from Poland (2023), "Opposition criticised for using AI-generated deepfake voice of PM in Polish election ad," Accessed at: <https://notesfrompoland.com/2023/08/25/opposition-criticised-for-using-ai-generated-deepfake-voice-of-pm-in-polish-election-ad/>

⁷² Service of the Republic of Poland (2025), "Election Protection Program against Cyber Threats and Disinformation," Accessed at: <https://www.gov.pl/web/cyfryzacja/program-ochrony-wyborow-przed-cyberzagrozeniami-i-dezinformacja>

⁷³ Service of the Republic of Poland (2025), "Election Protection Program against Cyber Threats and Disinformation," Accessed at: <https://www.gov.pl/web/cyfryzacja/program-ochrony-wyborow-przed-cyberzagrozeniami-i-dezinformacja>

- o A key component is the “Safe Elections” project ([Bezpiecznewybory.pl](https://bezpiecznewybory.pl/)), coordinated by NASK-PIB.⁷⁴
- o [The Election Protection Program](#) includes informational activities such as meetings on disinformation, training for Electoral Committees, the National Electoral Office (KBW), and journalists, as well as educational materials and campaigns on reporting disinformation content.⁷⁵
- o Activities of the Internal Security Agency (ABW): As part of the [Election Protection Program](#), the ABW will focus on identifying vulnerabilities to cyberattacks and ensuring the protection of key applications related to the organisation of elections.⁷⁶ Additionally, the ABW’s activities include counteracting intelligence, terrorist, and diversionary threats; identifying disinformation campaigns; monitoring the cybersecurity landscape in Poland; assessing the security of information systems and networks operated by the National Electoral Office (KBW); and testing applications that support the electoral process. The ABW will also conduct specialised training for the National Electoral Office (KBW), focusing on social engineering techniques that foreign services may use to disrupt the electoral process.
- o Social media platforms are monitored by the National Research and Academic Network (NASK) for election-related disinformation through its [Disinformation Analysis Centre](#), which analyses false information, identifies its sources, responds to it, and assesses its potential impact on society and democratic processes.⁷⁷
- o Military Counterintelligence Service (SKW) counters influence operations targeting the Polish military’s [interests](#).⁷⁸

⁷⁴ Bezpieczne Wybory. “Don’t Let your voice be taken away! Report Disinformation Here,” Accessed at: <https://bezpiecznewybory.pl/>

⁷⁵ Ministry of Digitization. “Program ochrony wyborów PARASOL WYBORCZY,” Accessed at: <https://www.gov.pl/attachment/a19eb0ae-fe5c-4d49-bafb-58e331881adf>

⁷⁶ Service of the Republic of Poland (2025), “Election Protection Program against Cyber Threats and Disinformation,” Accessed at: <https://www.gov.pl/web/cyfryzacja/program-ochrony-wyborow-przed-cyberzagrozeniami-i-dezinformacja>

⁷⁷ NASK (2024), “The role of institutions in combating disinformation. The vision of the NASK Disinformation Analysis Center,” Accessed at: <https://nask.pl/magazyn/rola-instytucji-w-zwalczaniu-dezinformacji-wizja-dzialania-osrodka-analzy-dezinformacji-nask>

⁷⁸ Info OPS Polska. “Foreign Information Manipulation and Interference Threats and Answers in Poland,” Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

- o The Ministry of National Defence (MOD) conducts counter-disinformation operations in the media and online environment. MOD manages Poland's national cyber defence [capabilities](#).⁷⁹
- o The Ministry of the Interior and Administration (MSWiA) responds to FIMI threats in the context of public order and internal security. They also work to inform the Polish public about FIMI [threats](#).⁸⁰
- o Government Security Centre (RCB), the crisis response agency of Poland, has developed response scenarios for hybrid threats, potentially including FIMI [campaigns](#).⁸¹
- o The Ministry of Foreign Affairs (MFA) has a special envoy designated to address [FIMI](#). They have also recently built a Counter FIMI team in their Strategic Communication Department.⁸²

⁷⁹ Info OPS Polska. "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

⁸⁰ Info OPS Polska. "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

⁸¹ Info OPS Polska. "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

⁸² Info OPS Polska. "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

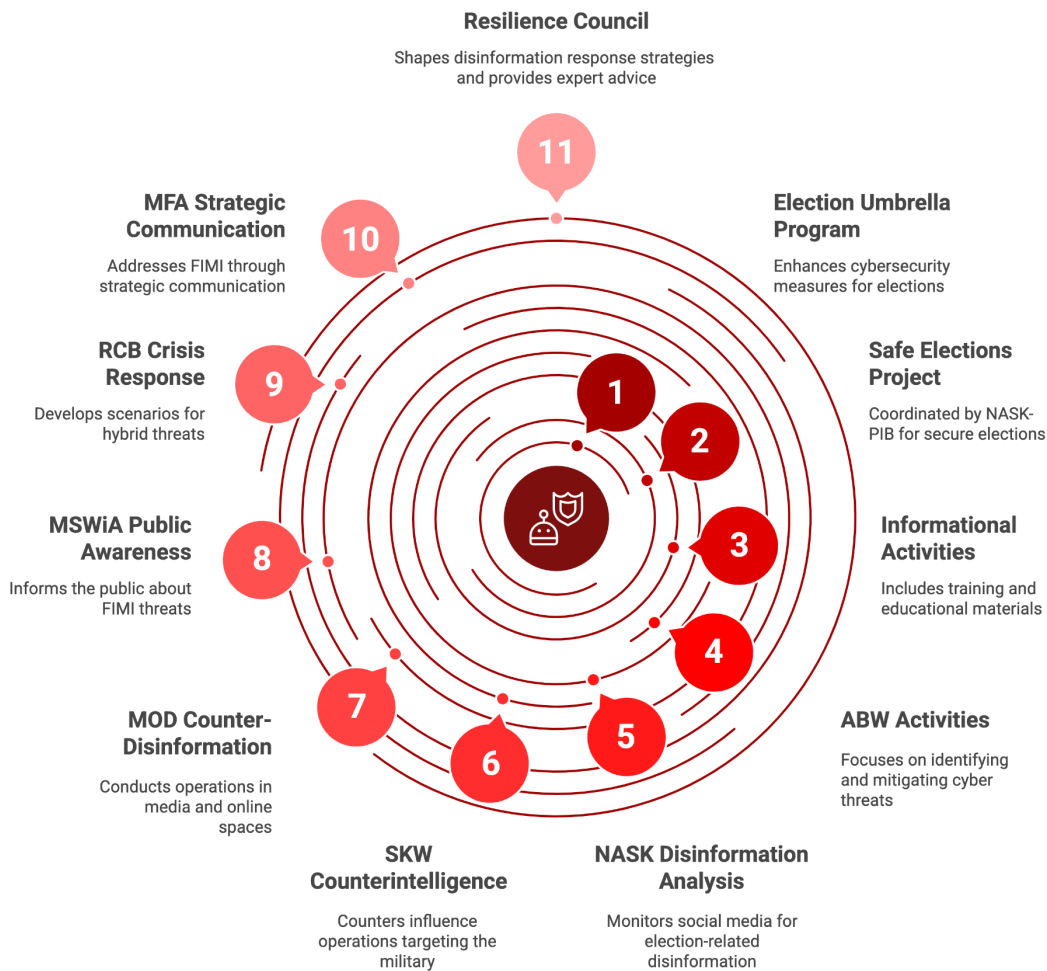


Figure 26: Poland's Election Protection Program against Cyber Threats and Disinformation

7.1.2 The Polish Resilience Council

The Polish Resilience Council is a recently formed advisory body bringing together government, academia, civil society, and business experts to collaboratively address the challenge of international disinformation and build societal resilience against it as well as to develop perspectives and proposals for effective countermeasures, particularly in the context of elections and broader democratic processes.⁸³ This initiative, formally established by the Foreign Minister on September 11, 2024, convened its inaugural

⁸³ Ministry of Foreign Affairs of Poland (2025), "Council for Resilience, joint initiative by MFA and civil society organisations against international disinformation, begins operation," Accessed at: <https://www.gov.pl/web/diplomacy/council-for-resilience-joint-initiative-by-mfa-and-civil-society-organisations-against-international-disinformation-begins-operation#:~:text=Republic%20of%20Poland,News,against%20international%20disinformation%2C%20begins%20operation>

meeting on April 3, 2025. The Council is seen as a model, and the experiences and best practices learned from it may be useful for setting up similar councils in other EU countries.⁸⁴

7.1.3 Real-time Monitoring and Countermeasures

The countermeasures implemented during Polish elections adopt a multi-faceted approach, representing a layered defence against the various threats that can undermine democratic elections. These countermeasures can be broken down into key areas:

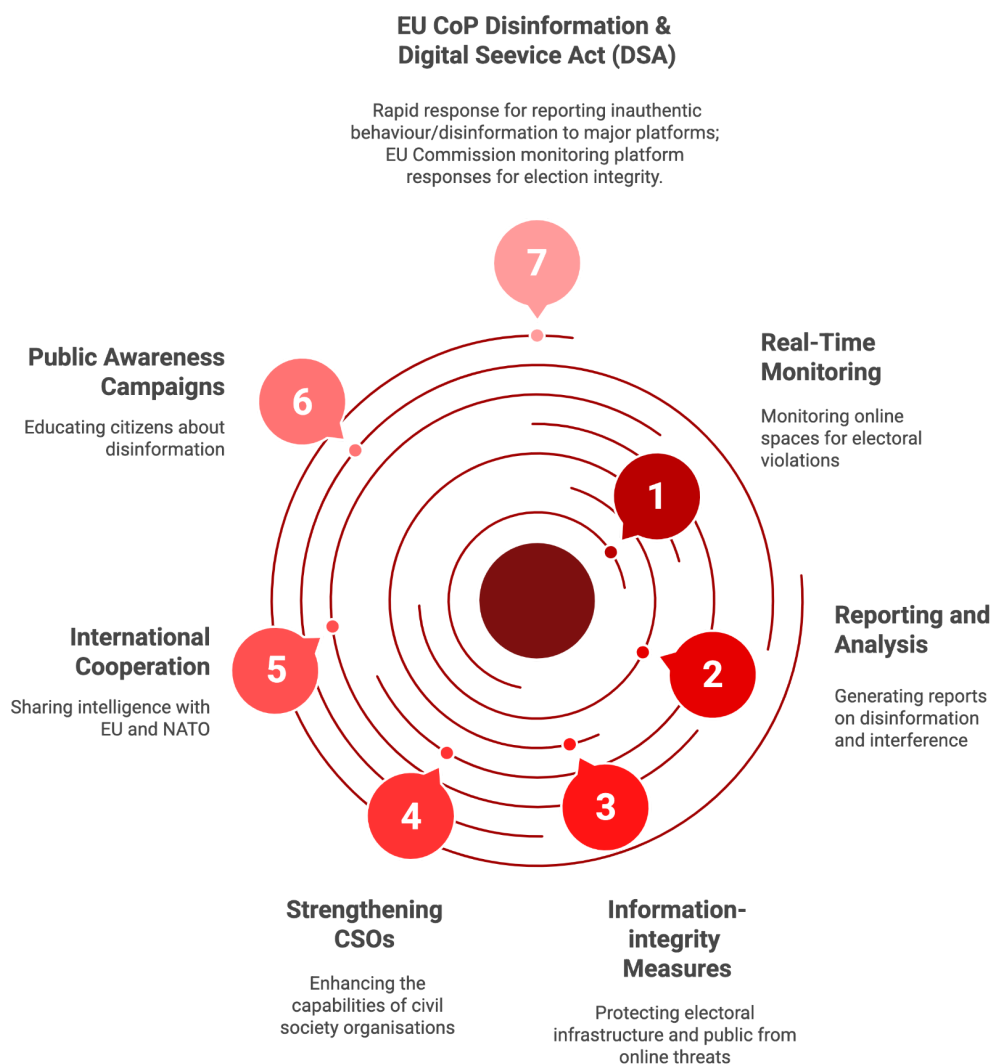


Figure 27: Poland's Multi-Faceted Electoral Countermeasures

⁸⁴Chłóń, Tomasz and Robert Kupiecki, "Towards FIMI Resilience Council in Poland. A Research and Progress Report," Accessed at: <https://docs.saufex.eu/Towards%20FIMI%20Resilience%20Council%20in%20Poland.pdf>

- **Real-time Monitoring** - The Ministry of Digital Affairs and NASK (National Research Institute) actively monitor online spaces for violations of "electoral silence" (a period of campaigning blackout before elections). This involves scanning social media, news sites, and online forums. **This real-time monitoring aims to provide an early warning system, allowing authorities to react quickly to emerging threats and maintain the integrity of the electoral process.**
 - They track the online activities of election committees and candidates, watching for suspicious patterns or coordinated disinformation campaigns.
 - Illegal content, such as hate speech or calls for violence, is identified and flagged for removal.
 - Sophisticated bot networks, designed to artificially amplify certain messages, are detected and neutralised.
 - They also monitor online activity from anti-system groups that may be spreading disinformation.
- **Reporting and Analysis** - Analytical reports are generated detailing instances of electoral disinformation and suspected foreign interference. These reports provide crucial information for policymakers and security agencies, enabling them to understand the scale and nature of threats. They help to build a comprehensive picture of the threats facing the elections, allowing for informed decision-making and targeted countermeasures.
- **Information-integrity Measures** - The Bezpiecznowybory.pl and the "Safe Elections" project aim to protect the electoral infrastructure and the public from online threats. The "Safe Elections" project works in tandem with the Bezpiecznowybory.pl platform. While Bezpiecznowybory.pl empowers citizens to report disinformation and access verified information, the "Safe Elections" project focuses on the back-end collaboration with tech platforms to prevent the spread of such content at scale.
 - **Bezpiecznowybory.pl (Safe Elections)** - [Bezpiecznowybory.pl](https://x.com/CYFRA_GOV_PL/status/1884211149853581712), launched in [February 2025](#), platform acts as a central hub for citizens to report disinformation and access verified election information.⁸⁵ It allows citizens to both report disinformation and access verified election-related information. The platform also offers tools such as free domain security scanning, notifications on password

⁸⁵ Ministry of Digitisation. X Post. Accessed at: https://x.com/CYFRA_GOV_PL/status/1884211149853581712

leaks, and resources for administrators to enhance their cybersecurity awareness. [CERT Polska](#) also provides further cybersecurity tools.⁸⁶

- o **Tech Platform Cooperation** - The "Safe Elections" project's primary goal is to **foster stronger collaboration between the Polish government and major technology platforms** to proactively **detect and remove inauthentic content** that has the potential to **manipulate public opinion** during election periods, such as the upcoming 2025 presidential election.⁸⁷

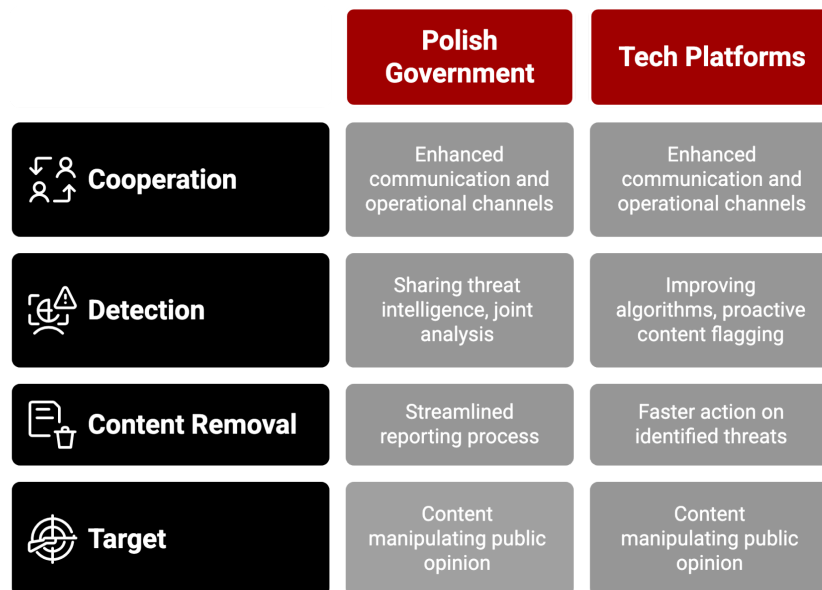


Figure 28: "Safe Elections" Project Breakdown

- o **Strengthening Civil Society Organisations (CSOs)** - CSOs play a vital role in monitoring and exposing disinformation, and strengthening their capacity is crucial for a healthy democratic process. Efforts are made to enhance the capabilities of CSOs that work to dismantle influence operations infrastructure. This involves providing resources, training, and support to help these organisations identify and counter disinformation campaigns.⁸⁸
- o **International Cooperation** - Foreign interference is often a transnational issue, and international cooperation is essential for effective countermeasures. Poland

⁸⁶ Service of the Republic of Poland. "Incident reporting," Accessed at: <https://www.gov.pl/web/baza-wiedzy/zglaszanie-incyidentow>

⁸⁷ Republic of Poland (2024), "Bolstering cybersecurity and combating disinformation - Prime Minister meets the vice chair and president of Microsoft," Accessed at: <https://www.gov.pl/web/primeminister/bolstering-cybersecurity-and-combating-disinformation>

⁸⁸ Ahead of the Presidential Elections, Debunk.org and Alliance4Europe provided training to 28 researchers from over 15 organisations on monitoring and responding to FIMI during elections.

engages in **cross-border intelligence sharing with the EU⁸⁹ and NATO⁹⁰ to counter foreign interference**. This cooperation allows for the exchange of information and best practices, enhancing the collective ability to respond to threats.

- o **Public Awareness Campaigns** - An informed public is more resilient to disinformation, and disinformation awareness campaigns are crucial for protecting the integrity of the electoral process. Public awareness campaigns are launched to educate citizens about the dangers of disinformation and how to identify it. These campaigns aim to promote media literacy and critical thinking skills. One such campaign was launched ahead of the election by the PZU Foundation, encouraging critical [thinking](#).⁹¹ Another example is the “[Nie pozwól sobie odebrać głosu!](#)”⁹² [campaign](#) led by NASK, which addresses not only misleading content but also the emotions that accompany and fuel such manipulations.⁹³
- o **Code of Practice on Disinformation (CoP Disinformation) and Digital Services Act (DSA)** - The European Union Code of Practice on Disinformation has activated its rapid response system, allowing signatories of the code to report inauthentic behaviour and disinformation to Meta, Google, and [TikTok](#).⁹⁴ Furthermore, the European Commission’s DSA enforcement team is, as part of their regular activity, [monitoring](#)⁹⁵ the Very Large Online Platforms’ responses to potential threats towards the integrity of the [elections](#).⁹⁶

⁸⁹ European Union External Action Service. “Factsheet: Rapid Alert System,” Accessed at:

https://www.eeas.europa.eu/node/59644_en#:~:text=The%20Rapid%20Alert%20System%20is,disinformation%20campaigns%20and%20coordinate%20responses.

⁹⁰ NATO (2025), “NATO’s approach to counter information threats,” Accessed at:

https://www.nato.int/cps/en/natohq/topics_219728.htm?

⁹¹ Mazurkiewicz, Maia. LinkedIn. Accessed at:

https://www.linkedin.com/posts/maia-mazurkiewicz_czystyprzekaz-activity-7321140585459773440-jF9x?utm_source=social_share_se&utm_medium=member_desktop_web&rcm=ACoAABWk9ucB7OQ2-2WugSMsGNwh0OoCxxYld-c

⁹² NASK (2025), “Don’t let your voice be taken away. A campaign that goes deeper,” Accessed at:

<https://www.nask.pl/aktualnosci/nie-ozwol-sobie-odebrac-glosu-kampania-ktora-siega-glebiej>

⁹³ NASK (2025), “The voice that someone is trying to take away from you. NASK launches a disinformation campaign,” Accessed at:

<https://nask.pl/aktualnosci/glos-ktory-ktos-probuje-ci-odebrac-nask-rusza-z-kampania-o-dezinformacji>

⁹⁴ European Commission. “The 2022 Code of Practice on Disinformation,” Accessed at:

<https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

⁹⁵ European Commission (2024), “Commission Publishes Guidelines under the DSA” Accessed at:

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707

⁹⁶ European Union, EUR-Lex. “Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC,” Accessed at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>

7.1.4 Post-Election Evaluation

- **Election observation missions:** The [OSCE](#) Office for Democratic Institutions and Human Rights (ODIHR) usually prepares reports after each election in OSCE member states, including Poland.⁹⁷ These reports assess the electoral process, highlighting its strengths and weaknesses. They analyse the effectiveness of the process, identify challenges, and provide recommendations for improvement.
- Additionally, ODIHR verifies the accuracy of election results and the integrity of the voting process to ensure fairness. The reports also examine key aspects, such as transparency in campaign financing, potential irregularities and manipulations, the impact of disinformation and media influence on the elections.
- **Post-election reviews** are made harder by the lack of a designated DSC who can evaluate what measures worked and did not work (Interview: Aleksy Szymkiewicz, Demagog Association, March 2025).

8. ELECTION RISK CATEGORISATION

8.1 Systemic/Structural Risks (Pre-Election Phase)

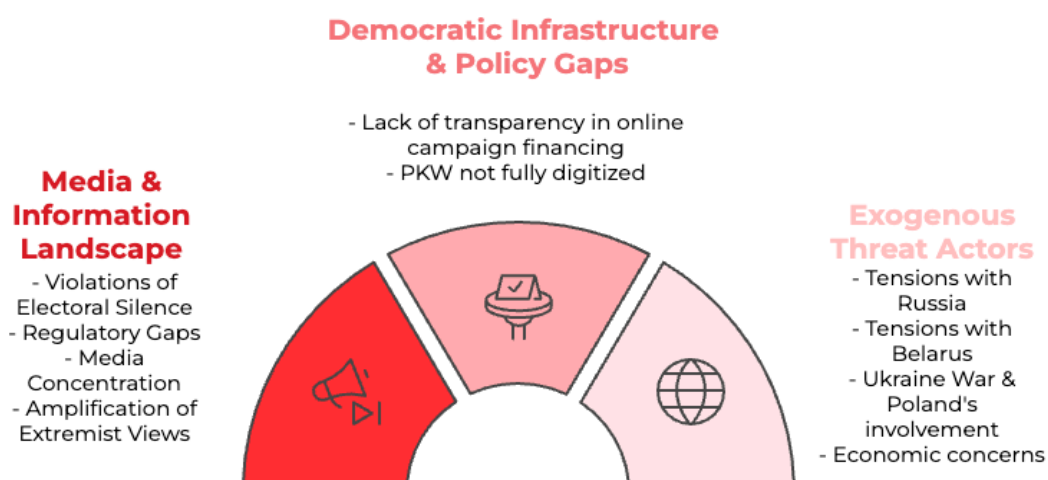


Figure 29: Systemic and Structural Risks

⁹⁷ Office for Democratic Institutions and Human Rights. "Republic of Poland, Presidential Election, ODIHR Special Election Assessment Mission Final Report," Accessed at: <https://www.osce.org/files/f/documents/6/2/464601.pdf>

8.1.1 Media and Information Landscape

- **Violations of electoral silence** - Electoral silence, the period immediately preceding an election during which campaign activities are prohibited, has been violated for years (Interview: Dominik Uhlig, Gazeta Wyborcza, March 2025). The rise of social media and online platforms has made enforcing these restrictions more complex, leading to debates about the relevance and enforceability of electoral silence in the [internet age](#).⁹⁸
- **Regulatory gaps** - Incomplete implementation of the Digital Services Act (DSA) and national media laws. 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 (Interview: NASK, March 2025).
- **Media concentration** - Efforts to restructure state media are ongoing; however, these initiatives continue to face significant [trust issues](#).⁹⁹ The concentration of media ownership and perceived political influences has raised concerns about [media independence](#) and the equitable representation of diverse political perspectives.¹⁰⁰
- **Narratives amplifying extremist viewpoints** - The media landscape has seen an increase in narratives that amplify extremist views. Such content can polarise public opinion and undermine democratic discourse, posing risks to social cohesion and the integrity of the electoral process.

⁹⁸ Musiał-Karg, Magdalena (2020), "Election Silence in the New Media. The Question of Whether Election Silence is Justified in the Era of New Media in the Context of Public Opinion Polls," Accessed at:

<https://czasopisma.marszalek.com.pl/images/pliki/ppk/58/ppk5801.pdf>

⁹⁹ Info OPS Polska (2024), "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at:

<https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

¹⁰⁰ Media Freedom Rapid Response (2024), ""Depoliticizing Poland's Media Landscape: Mission Report On The Challenges Of Reforming Poland's Captured Media Landscape By The Media Freedom Rapid Response Assessing The Progress Of Media Reform In 2024," Accessed at: <https://www.mfrr.eu/wp-content/uploads/2024/12/MFRR-Poland-Report-2024.pdf>

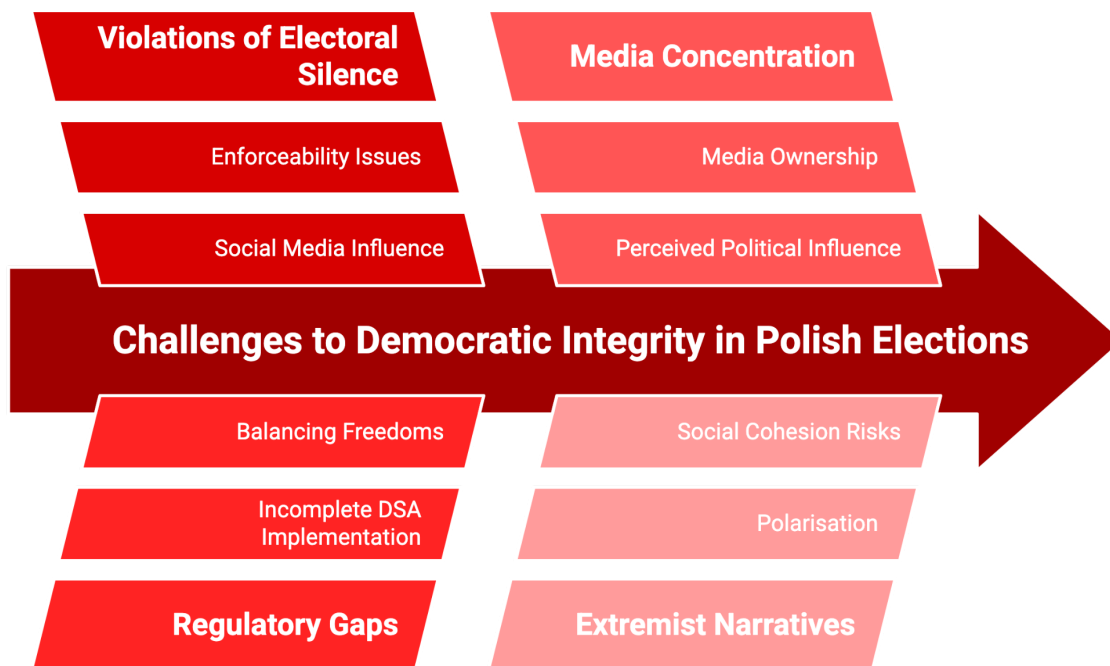


Figure 30: Challenges to Democratic Integrity in Polish Elections

8.1.2 Democratic Infrastructure & Policy Gaps

- While Polish law strictly prohibits foreign funding and mandates financial disclosures, enforcement challenges may arise. Lack of transparency in online campaign finance creates a risk of law violations, particularly through private entities funding political ads that align with a party's messaging.
- The Polish National Electoral Commission (PKW) is not fully digitalised, which creates cybersecurity vulnerabilities in the election infrastructure. Potential risks include phishing attacks and data leaks targeting officials, as seen in past incidents like the Ghostwriter campaigns (2020–2023).

8.1.3 Exogenous Threat Factors

- Geopolitical tensions with Russia and Belarus are fueling disinformation campaigns.

- The future of Ukraine—and Poland’s role in its security—is likely to become a key topic that could be exploited by FIMI actors and Poland’s foreign adversaries (Interview: Givi Gigitashvili, DFRLab, March 2025).
- The Polish government recently dropped measures to limit the impact of inflation, which could lead to economic concerns that shape voter discontent in Poland.¹⁰¹

8.2 Election-Specific Threats (Live Monitoring Phase)

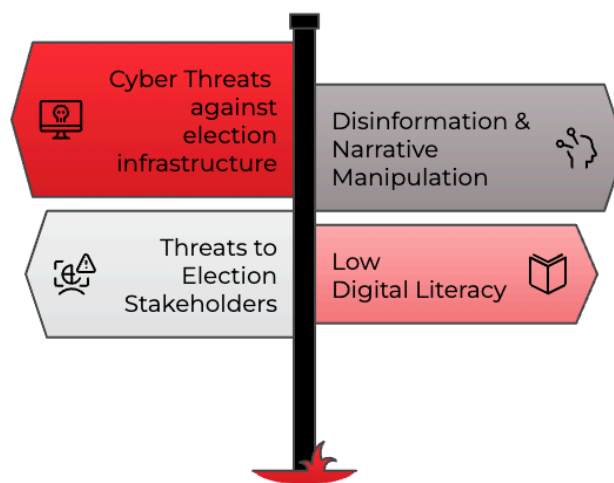


Figure 31: Election-Specific Threats

8.2.1 Cyber Threats & Election Infrastructure Attacks

- The Belarusian-linked hacker group Ghostwriter has conducted several major cyberattacks against Poland in 2020-2021. One example includes the group hacking into the then-chief of the chancellery for Poland’s Prime Minister, and stealing a large amount of

¹⁰¹ Wecek, J. (2025). “The government announces the end of this aid. The calculations will change after the elections.” Accessed at: <https://www.fakt.pl/pieniadze/rzad-oglasza-tarcz-antyinflacyjnych-co-z-rachunkami-za-prad-i-gaz-mamy-prognozy/te9lmf2>

both state and private materials. Content from these hacks was then leaked ahead of the Polish Presidential Elections.¹⁰²

- Ahead of the 2023 Polish presidential elections, fifteen Russian hacker groups carried out a series of Distributed Denial of Service (DDoS) attacks against Polish websites, including websites of financial institutions and government entities¹⁰³.
- Polish websites have also been hacked and used to spread influence operation content. A recent instance in 2024 involved the hacking of the Polish Press Agency, which resulted in the publication of a false article asserting Poland's intent to mobilise former soldiers and citizens for the conflict in Ukraine.¹⁰⁴

8.2.2 Disinformation & Narrative Manipulation

- According to [NASK](#), the main threats to the 2025 Polish elections include AI-generated disinformation (deepfakes, fake graphics, and manipulated videos), the use of bots to spread false narratives, and the involvement of influencers in misinformation campaigns.¹⁰⁵ These tactics exploit emotions and fears, making public awareness and media literacy crucial in countering election manipulation.
- Most FIMI narratives rely on sentiment amplification, pushing messages that exploit existing societal fault lines. (Interview: Givi Gigitashvili, DFRLab, March 2025)
- Belarusian and Russian FIMI actors might claim that the elections are fraudulent or "they were stolen if the far-right candidates don't win" , as in previous elections (Interview: Mateusz Zadroga, Fakenews.pl, March 2025).
- If the polling numbers before the election are widely different from the election results, the integrity of the elections might be questioned by foreign and domestic influence operations (Interview: Aleksy Szymkiewicz, Demagog Association, March 2025). To prevent the legitimacy of the elections from being called into question, it is essential to release the results of any investigations into pre-election irregularities or manipulation in

¹⁰² Gigitashvili, G. (2025). "How foreign actors targeted Polish information environment ahead of parliamentary elections". Accessed at: <https://dfrlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/>

¹⁰³ Ibid.

¹⁰⁴ Uhlig, D. (2024). "Fałszywa depesza o mobilizacji. Kto na niej korzysta, by podgrzać nastroje?" Accessed at: <https://wyborcza.pl/7,75398,31032904,falszywa-depesza-pap-o-mobilizacji-wroci-rosyjska-propaganda.html>

¹⁰⁵ NASK (2025), "Deepfakes, Influencers, and Bots: The Biggest Threats to the 2025 Elections," Accessed at: <https://nask.pl/aktualnosci/deepfake-influencerzy-i-boty-najwieksze-zagrozenia-wyborow-2025>

the information space and implement appropriate measures before announcing the final outcome (Interview: Givi Gigitashvili, DFRLab, March 2025).

8.2.3 Physical & Digital Threats to Election Stakeholders

- Harassment targeting journalists has, during the rule of the Law and Justice party, been a significant concern in Poland, according to Konrad Siemaszko, at the Helsinki Foundation for Human Rights.¹⁰⁶ Media entities faced a barrage of Strategic Lawsuits Against Public Participation (SLAPPs).¹⁰⁷ Poland was identified in 2022 as the country with the most SLAPP cases in Europe, mainly targeting journalists, media outlets, and civil society.¹⁰⁸
- Protests turning violent are another risk to the security of the elections. One recent example includes the Farmers' protest in 2024, where protesters attacked police.¹⁰⁹

8.2.4 Low Digital Literacy & Increased Vulnerability

- As evidenced by the "[Poufna Rozmowa](#)", Polish politicians, who often communicate via private emails, are prone to cyberattacks due to low digital literacy.¹¹⁰ This makes them vulnerable to hacking, phishing, and other cyber threats.
- There is a notable gap in formal education on disinformation analysis, making it difficult to recruit skilled personnel and find subject matter experts in this field (Interview: NASK, March 2025).
- Addressing FIMI requires improved coordination between agencies and intelligence services, despite challenges arising from differing mandates and prerogatives. It is crucial to involve NGOs more closely with government efforts, as collaborating with civil society organisations (CSOs) is essential. Government institutions aren't collaborating with researchers from high-quality NGOs as much as they could (Interview: NASK, March 2025).

¹⁰⁶ Media Defence (2025). "Freedom of expression in Poland: legal harassment against journalists and widening political control over the media." Accessed at: <https://www.mediadefence.org/news/hfhr-poland-freedom-of-expression/>

¹⁰⁷ Ibid.

¹⁰⁸ Dabrowska-Cydzik, J. (2023). "250 SLAPP lawsuits per year in Europe. Poland is the inglorious leader". Accessed at: <https://www.virtualnemedial.pl/artykul/slapp>

¹⁰⁹ AP News. (2024). "Polish government blames hooligans for violence at farmer protests". Accessed at: <https://apnews.com/article/poland-farmers-protest-violence-police-1fc19283e9a83b765d0bf099346135b4>

¹¹⁰ Gigitashvili, Givi. (2023). "How foreign actors targeted Polish information environment ahead of parliamentary elections," Accessed at: <https://dfrlab.org/2023/12/13/how-foreign-actors-targeted-polish-information-environment-ahead-of-parliamentary-elections/>

9. PRIORITY INTELLIGENCE REQUIREMENTS (PIRs)

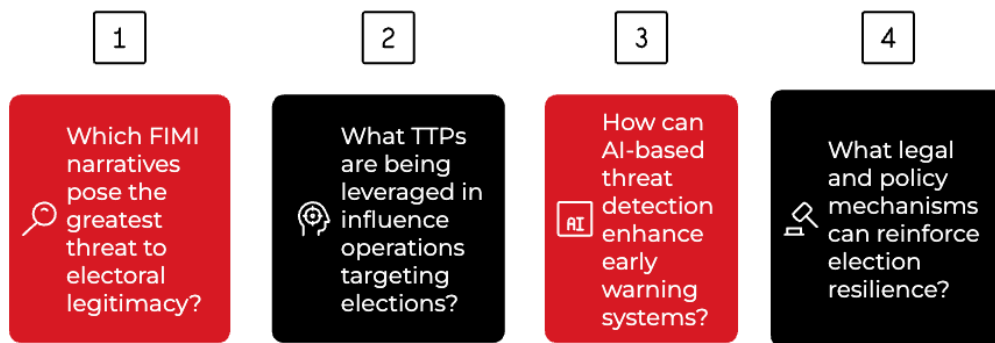


Figure 32: Priority Intelligence Requirements

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

- Allegations of election fraud (e.g., manipulation of ballots, foreign interference).
- Anti-EU narratives portray the government as controlled by Brussels.
- Anti-Ukraine narratives undermine Poland's [NATO commitments](#) and support for Ukraine.¹¹¹

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

- [AI-generated disinformation](#) (deepfakes, synthetic voices).¹¹²
- [Impersonation of legitimate Polish media to spread misleading content](#).¹¹³
- [Coordinated inauthentic behaviour \(CIB\) using bot networks](#).¹¹⁴
- Cyber-enabled influence operations, hack and leak, DDOS, and Website defacement (Givi Gigitashvili, DFRLab, March 2025).

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

- Automated detection of deepfake content in real time.

¹¹¹ Service of the Republic of Poland (2024), "Disinfo Radar," Accessed at: <https://www.gov.pl/web/rcb/disinfo-radar>

¹¹² NASK. "Deepfakes, Influencers, and Bots: The Biggest Threats to the 2025 Elections," Accessed at:

<https://nask.pl/aktualnosci/deepfake-influencerzy-i-boty-najwieksze-zagrozenia-wyborow-2025>

¹¹³ Media and Journalism Research Center (2025), "Regulation of Social Media and Elections in Europe," Accessed at:

<https://journalismresearch.org/2024/12/regulation-of-social-media-and-elections-in-europe/>

¹¹⁴ Center for Security and Emerging Technologies (2021), "AI and the Future of Disinformation Campaigns

Part 1: The RICHDATA Framework," Accessed at:

<https://cset.georgetown.edu/wp-content/uploads/CSET-AI-and-the-Future-of-Disinformation-Campaigns-Report.pdf>

- AI-driven sentiment analysis to track polarising narratives.
- Fact-checking automation integrated into election monitoring systems.

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

- Full implementation of DSA oversight and increased funding for election security.
- Transparency in campaign finance laws to prevent foreign funding loopholes.
- Mandatory disclosure of AI-generated political content in election campaigns.
- [Harmonisation of disinformation regulations](#) among EU member states, ensuring that all countries adopt common standards and approaches to combating FIMI.¹¹⁵
- Closer collaboration between government agencies and civil society to detect and counter Influence Operations (Interviews: NASK, March 2025; Givi Gigitashvili, DFRLab, March 2025, Aleksy Szymkiewicz, Demagog Association, March 2025).
- Easing data access for researchers from social media platforms (Interview: Givi Gigitashvili, DFRLab, March 2025, Aleksy Szymkiewicz, Demagog Association, March 2025).

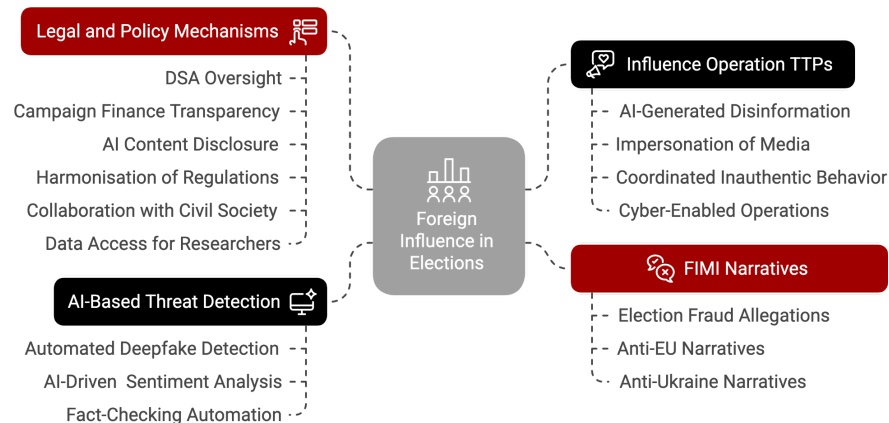


Figure 33: Summary of Priority Intelligence Requirements

¹¹⁵ Info OPS Polska (2024), "Foreign Information Manipulation and Interference Threats and Answers in Poland," Accessed at: <https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/>

10. CONCLUSION

The upcoming Polish Presidential Elections in May 2025 face a threat from Foreign Information Manipulation and Interference. Building on lessons from past elections and acknowledging the current geopolitical climate, this report has highlighted critical vulnerabilities across disinformation narratives, cyberattacks, physical threats, and the erosion of institutional trust. The identified high likelihood and impact of several FIMI tactics, particularly those leveraging existing societal divisions and exploiting social media platforms, underscore the urgency of proactive intervention.

The analysis points to Russia and Belarus as likely key actors employing sophisticated strategies, including the amplification of divisive narratives, cyber intrusions, and even direct attempts to recruit Polish citizens for disinformation campaigns. Addressing these multifaceted threats demands a cohesive and collaborative response from Polish authorities, electoral bodies, civil society, media, and digital platforms.

Continuous monitoring, dynamic risk assessment, and robust engagement among all stakeholders are essential to safeguarding the democratic process, ensuring a fair and transparent election, and ultimately bolstering Poland's resilience against foreign interference. This report's findings serve as a crucial call to action to prioritise and implement effective mitigation strategies in the lead-up to this critical democratic event.

