FIMI -ISAC

Foreign Information Manipulation and Interference - Information Sharing and Analysis Centre

www.fimi-isac.org

FIMI-ISAC Collective Findings I: Elections

October 2024

TABLE OF CONTENTS

1 Introduction 3
1.1 Overview of the FIMI-ISAC 3
1.2 Importance of understanding FIMI in elections 3
1.3 Sources and methodology 3
1.4 Table of case studies 4
2 Narratives 8
2.1 Type A Narratives 10
2.1.1 Anti-immigrant narratives 10
2.1.2 Discrimination and Hate Speech 11
2.2 Type B Narratives 12
2.2.1 Anti-West narratives 12
2.2.2 Electoral fraud narratives 12
2.2.3 Health Disinformation 13
3 DISARM:Tactics, Techniques, and Procedures (TTPs) 14
3.1 Content production TTPs 14
3.2 Establishment of legitimacy 15
3.3 Content dissemination TTPs 15
3.4 Other Relevant TTPs 16
4 Conclusions 17
4.1 Summary of findings 17
4.2 Implications for future elections and disinformation strategies 18

SUMMARY

- This report illustrates the FIMI-ISAC's data-sharing approach to provide a more comprehensive view of foreign information manipulation and interference (FIMI) in elections, merging individual analysis into a broader perspective encompassing contributions from multiple members.
- FIMI-ISAC reports are designed to collate data, insights and reports across member organisation into more easily digestible written products and structured data using common standards and tools such as STIX, DISARM and OpenCTI.
- Anti-immigrant and discriminatory narratives are prominent, with several case studies demonstrating how these themes are used to sow discord and foster xenophobia, often leveraging societal prejudices to deepen divisions.
- FIMI targeting democratic institutions, including electoral fraud narratives and health disinformation, aims to undermine trust in electoral processes and public health systems, exploiting lingering anxieties post-pandemic and existing societal tensions.
- Advanced tactics, techniques, and procedures (TTPs), including AI-generated content, selective editing, and the use of trolls and bots, highlight the evolving sophistication of campaigns and the need for enhanced countermeasures and collaborative monitoring.
- The continued reappearance of well-known divisive narratives and repetitive tactics across various geopolitical contexts underscores the critical need for a comprehensive, multifaceted approach to safeguard democratic processes and information integrity against FIMI threats.

1 Introduction

In 2024, nearly half the world's population is estimated to vote in a historic wave of elections that will shape global governance for decades. The integrity of these democratic processes faces unprecedented challenges from increasingly sophisticated tactics and widespread false narratives and conspiracy theories, underscoring the critical need for a robust defence against foreign information manipulation and interference (FIMI). This report is a summary review of reports related to FIMI in global elections produced by FIMI-ISAC members in the first half of 2024, with a focus on the June 2024 EU Parliamentary elections. The report identifies narratives and TTPs (tactics, techniques, and procedures) and is part of an ongoing collaborative initiative dedicated to safeguarding democratic processes and ensuring election integrity.

1.1 Overview of 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.

1.2 Importance of understanding FIMI in elections

Elections are critical moments for democratic societies and ensuring their integrity is paramount. FIMI campaigns can pose a significant threat to this integrity, with actors seeking to manipulate public opinion, influence voter behaviour, and undermine trust in electoral processes. These campaigns are increasingly advanced and can take various forms, including spreading false or misleading information about candidates, voting procedures, or election results, using coordinated, inauthentic behaviour to boost certain narratives artificially, and attempting to exploit social divisions to polarise the electorate. By dissecting the narratives and TTPs used in these operations, researchers and policymakers can better anticipate, identify, and mitigate the impact of disinformation campaigns. Understanding the FIMI threat can also inform the development of international norms and effective countermeasures, including robust content moderation policies for online platforms, ultimately strengthening the resilience of electoral systems against malicious influence operations.

1.3 Sources and methodology

This report is a compilation of case studies provided by FIMI-ISAC members and their partners, including VOST, Global Disinformation Index (GDI), Italian Digital Media Observatory (IDMO), Debunk.org, Fundación Maldita.es, EU DisinfoLab, Alliance4Europe, Mediapooli, and the Alliance for Securing Democracy at the German Marshall Fund. While this report is meant to be illustrative and not exhaustive,

it thoroughly examines member-documented FIMI cases over the first half of 2024, identifying recurring narratives and TTPs and categorising them for comprehensive analysis. Unless otherwise noted, the case studies highlighted in this report are drawn from publicly available reports or data submitted by FIMI-ISAC members. While not all cases examined are definitive instances of FIMI, they encompass lessons applicable to FIMI scenarios and election integrity efforts more broadly. Moreover, these case studies provide insights into the tactics and strategies employed by threat actors, offering a foundation for developing robust countermeasures for future elections.

The subsequent sections of this report delve into specific narratives and TTPs, linking them to pertinent case studies and offering quantitative insights where possible. This structured approach aims to clearly understand the methods used in FIMI campaigns and their implications for democratic processes. By highlighting the interconnectedness of disinformation activities and potential foreign influence operations across various regions and electoral contexts, the report underscores the critical need for continuous monitoring, information sharing, and collaborative countermeasures. This report and the ongoing work of the FIMI-ISAC and its members serve as a foundation for developing robust strategies to combat FIMI-related threats, ensuring the integrity of democratic processes worldwide in an unprecedented year of global elections.

1.4 Table of case studies

Title	Summary	URL
AI-Generated conversation in Lithuania	An AI-generated deepfake conversation between Lithuanian and Palestinian MFA ministers intended to erode public trust in these figures and suggested unethical negotiations.	https://www.youtube.com/watch?v=VETBP91ztK8
Fake Hulu trailer	A disinformation campaign created a fake Hulu trailer implying Western politicians' drug use by leveraging selective video editing and contextual manipulation.	Debunk.org
Operation Doppelganger	Cloning of media and government websites to spread anti-Ukrainian and pro-Russian content linked to Russian companies Struktura and Social Design Agency.	https://www.disinfo.eu/doppelganger-operation/

Disinformation in Portuguese elections	Various instances of anti-immigrant sentiment and false claims during the Portuguese elections, including manipulated videos and decontextualised content to incite fear and discord.	https://www.lusa.pt/article/42921391
Spain EU election fraud narratives	Campaigns promoting null votes and spreading conspiracy theories about delayed election results undermine the electoral process's legitimacy in Spain.	https://maldita.es/malditodato/20240703/integridad-electoral-elecciones-europeas-efcsn/ https://maldita.es/malditobulo/20240609/falsas-estrategias-papeleta-elecciones/
Italy EU election disinformation	Disinformation suggesting electoral fraud in the EU elections intertwined with anti-NATO and pro-Russian narratives in Italy.	-
Gendered disinformation in EU elections	Misogynistic rhetoric targeting female candidates during the 2024 European elections aims to undermine their credibility and reinforce traditional gender biases.	https://www.disinformationindex.org/blog/2024-06-10-gendered-disinformation-in-the-european-parliamentary-elections/
Eurovision 2024 disinformation	A campaign portraying Eurovision as an EU propaganda tool promoted anti-LGBTQ+ rhetoric and polarised public opinion against EU-level decisions.	-
Health disinformation targeting migrants in Spain	False claims linking migrants to health risks like an epidemic of ringworm and scabies in Catalonia aimed to promote anti-immigration sentiments.	https://maldita.es/migracion/20240703/analisis-desinformacion-elecciones-europeas/ https://maldita.es/migracion/bulo/20240426/generalitat-alerta-tina-sarna-cataluna/ https://maldita.es/malditobulo/20240103/video-musulman-orina-cerdo-paises-bajos/

Civil unrest in New Caledonia	Disinformation tying local unrest to broader anti-Western conspiracy theories suggested U.S. orchestration for strategic control.	-
Operation Overload	Coordinated efforts to overwhelm fact-checkers and news organisations with false verification requests used trolls and bots to amplify disinformation.	https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf https://www.disinfo.eu/outreach/our-webinars/20-june-operation-overload-please-check-how-pro-russian-propagandists-try-to-manipulate-newsrooms/
YouTube ads in Portugal	YouTube political ads targeted the political centre, paid by a mysterious company.	https://covertlyyours.substack.com/p/what-happens-in-the-americas-doesnt
Sanctioned Russian Media Entities and Individuals Accessible on TikTok	The week before the European elections, TikTok channels linked to EU-sanctioned Russian state-controlled media and media personalities remained accessible to EU-based audiences.	Sanctioned Russian Media Entities and Individuals Accessible on TikTok - Alliance4Europe
Benin-based FB Page Attacking Macron & Ukraine	A Facebook page running ads targeting France with anti-Macron and anti-Ukrainian content appeared to be operated from Benin with ads paid for with Canadian dollars.	Benin-based FB Page Attacking Macron & Ukraine - Alliance4Europe
The largest disinformation and scam attack ever recorded in Lithuania. Part I	In Lithuania, online scammers are creating copies of major news portals, fake Facebook accounts and inviting people to invest in fake investment platforms in order to extort money from citizens of Lithuania and neighbouring countries.	https://www.debunk.org/the-largest-disinformation-and-scam-attack-ever-recorded-in-lithuania-part-i

The large-scale scam attack also exploits well-known Lithuanian and foreign personalities. Part II	Unidentified persons are exploiting the brands of LRT, LNK, Delfi, InfoTV, the Estonian national broadcaster, ERR, the Estonian newspaper, Eesti Päevaleht, as well as Ignitis and Orlen Lietuva by creating fake copies of their accounts, which show fake ads under the name of these brands.	https://www.debunk.org/the-large-scale-scam-attack-also-exploits-well-known-lithuanian-and-foreign-personalities-part-ii
WeRedirect APT. The Large-Scale Scam Attack: Exposing the Elaborate Tactics of Online Scams Part III	In the third instalment of the investigation into the biggest scam and disinformation attack in Lithuania to date, our analysts uncover the intricate technique of “cloaking” used by the scammers. This method makes detection of the scam even more challenging, as it involves creating many different websites or web pages and, depending on specific criteria, redirecting different users to different content.	https://www.debunk.org/weredirect-apt-the-large-scale-scam-attack-exposing-the-elaborate-tactics-of-online-scams-part-iii
Doppelganger journalist FIMI incident from Belarus National State TV against Lithuanian president elections 2024 candidates	Two Lithuanian presidential candidates were deceived by a fake email address into giving interviews to Belarus National State TV, where their statements were manipulated to align with Belarusian state propaganda. The incident, which aimed to undermine the credibility of the Lithuanian election and portray Lithuania as a Western puppet, involved the creation of a false persona posing as a journalist from a reputable outlet. This disinformation campaign aired on Belarus-1 TV just days before the election.	https://www.debunk.org/doppelganger-journalist-fimi-incident-from-belarus-national-state-tv-against-lithuanian-president-el

Operation targets French snap elections using AI-generated content	A campaign targeted the French legislative snap elections, impersonating political parties and leveraging AI-generated content sharing disinforming content, identified as a new iteration of Operation CopyCop.	https://dfrlab.org/2024/07/04/operation-targets-french-snap-elections-using-ai-generated-content/

2 Narratives

A set of pervasive narratives emerged in analysing flagged case studies identified by FIMI-ISAC members during the first half of 2024. These narratives, designed to manipulate public opinion, undermine democratic processes, and exacerbate societal divisions, demonstrate sophistication and cross-border coordination. Our analysis extends beyond election-specific content to encompass a wide range of narratives with the potential to influence voter decisions and behaviours.

The following sections provide a detailed categorisation and analysis of these critical narratives and illustrate their impact and prevalence across diverse geopolitical contexts. By examining their interconnectedness and adaptive nature across political landscapes, we aim to provide an understanding of the evolving threat of foreign information manipulation and interference.

The narratives identified in member organisation case studies represent an evolution of long-standing FIMI/disinformation strategies frequently deployed by state-sponsored actors and their proxies. These narratives serve a dual purpose: exploiting societal vulnerabilities and advancing broader geopolitical objectives to undermine Western influence and democratic governance.

Recognising the connections between narratives and their historical precedents enables researchers, policymakers, and civic society to:

1. Develop more robust early warning systems to detect emerging FIMI/disinformation trends;
2. Design targeted counter-narratives that address the root causes of societal vulnerabilities;
3. Implement proactive measures to bolster democratic institutions against subversion attempts;
4. Foster international cooperation to share best practices in combating cross-border disinformation campaigns;
5. Educate the public on critical media literacy skills to enhance resilience against manipulation.

By adopting a comprehensive, multifaceted approach informed by this deeper understanding, societies can build more robust defences against the ever-evolving tactics employed in FIMI attacks. This proactive stance not only protects democratic values but also preserves social cohesion in the face of persistent attempts to sow discord and division.

Our analysis revealed two narrative types: Type A narratives exploit societal vulnerabilities to sow discord, while Type B narratives systematically erode trust in democratic institutions. These narratives, deployed

by threat actors, work in tandem to manipulate public opinion and undermine the foundations of democratic governance.

Type A narratives intrinsically link to a critical FIMI vulnerability threat that actors exploit. These narratives forcefully assert that outsiders and those deviating from the majority pose an imminent threat to established societal norms and values. This deliberate manipulation of societal fears capitalises on and intensifies existing prejudices, dramatically amplifying xenophobia, racism, and other forms of discrimination. By weaponising these fears, disinformation campaigns fracture communities, incite social unrest, and systematically erode social cohesion. Historically, state-sponsored disinformation campaigns have consistently and effectively employed these tactics to destabilise adversaries from within, fostering deep-seated internal conflicts and pervasive distrust.

Russia's strategy in various disinformation campaigns is a prime example of this exploitation. Russian influence operations have consistently and methodically sowed discord by propagating narratives that not only highlight but also exacerbate societal divisions in Western countries. The anti-immigrant narrative prevalent in the case studies represents a calculated evolution of this strategy, where immigrants are deliberately framed as direct threats to national security, cultural identity, and economic stability. By targeting vulnerable groups and inflaming existing tensions, these campaigns aim to divert attention from internal governance issues and redirect public focus towards fabricated external threats.

Type B narratives systemically erode trust in institutions and aggressively target the foundations of democratic governance. These disinformation attacks assault public confidence in electoral processes, government institutions, and public health systems. By cultivating pervasive cynicism, scepticism, and disengagement, these narratives create an environment where misinformation thrives, and authoritarianism is presented as a comparatively legitimate alternative to democracy.

The intricate connection between Type A narratives and Type B is evident in how Type A narratives seamlessly integrate into broader anti-Western rhetoric. These campaigns simultaneously criticise Western societies for embracing 'non-traditional' cultures – immigrants, LGBTQ+ and other marginalised groups and paint those same groups as active opponents of Western liberal values. This creates a powerful narrative that Western influence is morally questionable and fundamentally destructive to traditional societal norms." This dual narrative strategy amplifies the impact of disinformation by simultaneously undermining the integrity of societal groups and the Western democratic systems that uphold their rights.

Historically, Russia has employed these tactics to destabilise opponents, as seen in the 2016 U.S. elections and various European electoral processes. These campaigns attack the credibility of democratic systems by weaponising conspiracy theories to delegitimise Western governance models while promoting authoritarian frameworks as superior alternatives. Health-related disinformation campaigns, such as those falsely linking immigrants to public health risks, further exploit this strategy by eroding trust in public health authorities and sowing panic and division within societies.

The disinformation narratives identified in the following case studies represent a calculated evolution of state-sponsored actors' long-standing disinformation strategies. These narratives exploit societal vulnerabilities and advance broader geopolitical objectives to dismantle Western influence and democratic governance. Recognising the intricate connections between these narratives and their historical precedents is crucial for researchers and policymakers. This understanding enables the development of robust countermeasures to anticipate, neutralise, and ultimately defeat the ever-evolving tactics deployed in FIMI campaigns, safeguarding the integrity of democratic institutions and societal cohesion.

2.1 Type A Narratives

2.1.1 Anti-immigrant narratives

Anti-immigrant narratives are a pervasive theme in disinformation campaigns globally, often leveraged to sow discord, foster xenophobia, and normalise “white supremacy”. These narratives typically portray immigration as an economic burden and a threat to the native population’s culture or religion by linking immigrants to crime, joblessness, and cultural degradation. During the first half of 2024, several case studies highlighted this narrative's persistence and adaptation to current events.

In Portugal, disinformation campaigns were used during the national parliamentary elections. A video falsely claimed that “Gypsies” attacked a caravan belonging to the Chega party, a national conservative populist party. The claim aimed to incite ethnic tensions and garner sympathy for the party. The video spread rapidly and was primarily amplified through social media and influencers associated with the party. Another instance happened during the EU parliamentary elections, and involved anti-immigrant sentiment through a decontextualised video from Syria used to incite fear of Islamisation and anti-immigration sentiment in Portugal. The video, which has been used extensively to spread anti-Muslim sentiment, shows the destruction of a statue of the Virgin Mary and is 11 years old. It was spread without proper context and generated generalisations and offensive comments about the Muslim community.

In Spain, a disinformation campaign exploited anti-immigrant sentiments through the use of manipulated content and localised narratives. A key example of this was an edited video, originally created by a Dutch user, which falsely depicted a Muslim individual urinating on pork products in a supermarket. This inflammatory content rapidly spread across Instagram before being replicated by Spanish accounts on other online platforms.

Despite the original creator's intention to demonstrate the ease of fabricating online content and to raise awareness about digital disinformation, the video's dissemination outpaced its disclaimer. As a result, the manipulated footage, stripped of its original context, reached audiences in several European countries. This incident underscores the viral nature of sensationalist content and the challenges of containing the spread of disinformation once it gains traction. The campaign effectively sowed mistrust and fear among the public, exacerbating existing tensions surrounding immigration and religious differences in Spain.

These narratives strategically exploit deep-rooted societal vulnerabilities and longstanding prejudices, rendering them exceptionally potent in shaping public opinion. By design, they fabricate a pervasive sense of crisis and imminent threat, manipulating cultural anxieties and societal biases to exacerbate existing divisions. Such narratives can increase anti-immigrant sentiment. Historically, these tactics have been instrumental in justifying increasingly stringent immigration policies and fueling nationalist movements. For instance, in the 2016 U.S. presidential election and the Brexit referendum, similar narratives led to a surge in support for isolationist policies. Across Europe and the United States, these disinformation campaigns have consistently correlated with a rise in reported hate crimes against minority communities. The pervasive nature of these narratives, often amplified by FIMI threat actors, creates echo chambers that can increase political polarisation, posing a significant threat to social cohesion and democratic processes. Those same FIMI threat actors also exploit actual instances of discrimination against immigrants to delegitimise Western countries and to deflect criticism of their own human rights records. In July 2024, for example, dozens of Russian embassy and diplomatic accounts promoted a joint report by Russia's and Belarus' Ministries of Foreign Affairs that took Spain to task for its treatment of migrants. That report used actual instances of intolerance in Spain towards immigrants to paint the country's human rights stance as hypocritical and to allege widespread discrimination against Russians in the country.

2.1.2 Discrimination and Hate Speech

Gendered disinformation and hate speech serve as potent weapons in the arsenal of information warfare, systematically marginalising targeted groups and deepening societal fractures with alarming efficiency. These narratives strategically interweave with other forms of prejudice, including anti-LGBTQ+ sentiment, xenophobia, and religious intolerance, to construct a complex, multi-dimensional framework of discrimination that can erode social cohesion and democratic values. By exploiting intersecting vulnerabilities, these campaigns can amplify their impact, potentially increasing discriminatory attitudes and significantly undermining the participation of marginalised groups in political processes.

In the context of the 2024 global elections, gendered disinformation emerged as a relevant threat to democratic processes in the European Union. Despite the EU's above-average female representation in Parliament, recent European elections saw a surge in online gendered abuse and disinformation targeting female leaders and candidates. These narratives, often laced with misogyny, racism, and elements of foreign information manipulation, disproportionately affect women in politics, with prominent figures like EU Commission President Ursula von der Leyen facing severe attacks. The campaigns range from overt misogynistic rhetoric to more subtle manipulations of social biases, with women of colour experiencing even higher levels of abuse. This trend not only undermines the democratic basis of the EU but also threatens to reverse progress in women's political representation, as evidenced by the resignation of several female politicians citing online abuse as a significant factor. The pervasive nature of these attacks highlights the urgent need for global leaders to address and combat gendered disinformation to protect the integrity of democratic processes and ensure continued female participation in politics.

While officially a non-political event, the Eurovision Song Contest (ESC) has become increasingly entangled in geopolitical tensions, social issues, and disinforming narratives, particularly in the 2024 edition. Eurovision's long-standing association with LGBTQ+ culture made it a target for illiberal state actors who use anti-LGBTQ+ rhetoric to undermine Western democratic values. Adversarial narratives surrounding the event were weaponised to delegitimise Eurovision and the European Union, potentially impacting the European parliamentary elections. These narratives, often amplified by extremist groups, conspiracy theorists, and state media, contribute to discrimination against the LGBTQ+ community, foster division and polarisation, and promote conspiracy theories that erode trust in democratic institutions. The convergence of these issues around Eurovision 2024 highlights the complex interplay between culture, politics, and disinformation in the contemporary European landscape.

2.2 Type B Narratives

2.2.1 Anti-West narratives

Anti-West narratives aim to erode trust in Western institutions and democratic processes. Often orchestrated by state-sponsored actors, these campaigns depict Western leaders as corrupt, incompetent, or morally bankrupt, leveraging traditional and emerging media platforms to maximise impact. Exposure to these narratives can decrease trust in democratic institutions and increase support for authoritarian alternatives.

A selectively crafted fake Hulu video documentary trailer employed advanced video manipulation techniques to falsely implicate Western politicians in drug use, demonstrating the potential of video editing and design hijacking to undermine public trust.

The "Doppelganger" operation cloned legitimate media and government websites, successfully reaching users with anti-Ukrainian and pro-Russian content, highlighting the vulnerability of trusted information sources.

Narratives surrounding civil unrest in New Caledonia were woven into broader anti-Western conspiracy theories, suggesting U.S. orchestration for strategic control with Russian state media amplifying these messages to portray Russia as a defender against Western colonialism.

2.2.2 Electoral fraud narratives

Electoral fraud narratives attack the foundational integrity of democratic processes, undermining public confidence in elections and delegitimising electoral outcomes. Often amplified by domestic and foreign actors, these campaigns can impact voter turnout and increase post-election unrest.

In Lithuania, AI-generated deep fake phone call conversations convincingly simulated unethical negotiations between political figures, eroding public trust in these individuals and the electoral process.

The narrative insinuated foreign interference in elections, leveraging geopolitical tensions to amplify its impact.

Disinformation narratives in Italy suggested that the European election process was rife with fraud, promoting abstention and undermining the legitimacy of the electoral process. These narratives were intertwined with broader geopolitical themes, including support for Russian aggression against Ukraine and discrediting NATO and the EU. Specific campaigns encouraged invalidating votes and propagated conspiracy theories about delayed election results, aiming to weaken public trust in democratic institutions.

In Spain, a coordinated social media and messaging app campaign circulated misleading advice regarding the European Parliament elections. Two invalidating procedures were promoted: putting ballots from different parties in the same envelope and writing messages on ballot papers. Both actions would result in null votes, which do not count towards seat allocation. Additionally, there were attempts to encourage writing the name of Begoña Gómez, the Spanish President's wife, on the ballots.

In France, a sophisticated disinformation campaign targeted Macron's party during the June legislative elections, employing multiple tactics to undermine voter confidence. A fraudulent website, designed to impersonate Macron's party, attempted to manipulate the electoral process by promising illegal financial incentives in exchange for votes. This operation was later linked to the broader, coordinated "Operation CopyCop," revealing a complex misinformation network linked to Russia.

The campaign's scope was further evidenced by the theft and manipulation of several hundred articles from reputable French news sources. These stolen articles were systematically rewritten using Large Language Model (LLM) technology, transforming their content into a distinctly negative stance against Macron's political party, according to recovered articles where the prompts to the LLM were found. This calculated misuse of AI technology to distort legitimate news content represents a dangerous escalation in disinformation tactics, hinting at an industrial-level production of false narratives to sway electoral processes.

2.2.3 Health Disinformation

Health-related disinformation campaigns pose a critical threat to public safety and social cohesion, with potentially devastating consequences during health crises. These narratives often intertwine false claims about diseases, vaccines, and medical treatments and are strategically crafted to erode trust in health authorities and generate widespread fear and confusion.

After the global pandemic, these campaigns evolved to exploit lingering anxieties about institutional responses to health crises. Threat actors capitalise on public scepticism towards EU and national health policies, using disinformation to decrease trust in government health initiatives and EU leaders.

These narratives often intersect with xenophobic sentiments, as evidenced by false claims linking migrants to public health risks. For instance, a disinformation campaign in Catalonia falsely reported an epidemic

of ringworm and scabies among immigrant communities. Similarly, there were false alerts about hepatitis A in Moroccan strawberries, amplified by influencers and politicians exacerbating anti-immigrant sentiments.

3 DISARM:Tactics, Techniques, and Procedures (TTPs)

In analysing the case studies from the first half of 2024, several DISARM TTPs emerged. These TTPs can be broadly categorised into those related to content production, establishment of legitimacy, content dissemination, and others. Understanding these TTPs can better counteract disinformation campaigns and their impacts.

3.1 Content production TTPs

1. Artificial Intelligence in content creation

- **T0087.001: Develop AI-Generated Videos (Deepfakes):** Used to create realistic but false audio and video content. For example, in Lithuania, unlabelled AI-generated deep fake phone conversations suggested unethical negotiations between political figures, eroding public trust.
- **T0086.002: Develop AI-Generated Images (Deepfakes), T0087.001: Develop AI-Generated Videos (Deepfakes) and T0085.003:** Develop Inauthentic News Articles: AI tools can create synthetic media that appear authentic. This was evident in various campaigns, where manipulated videos and images were used to mislead audiences. In the APT WeRedirect attack, many Western leaders' identities (faces and voices) were used with deep fake videos promoted over social media ads to mislead local audiences. The European Commission started investigations against META because of possible DSA violations. In France, an AI-Generated news website was created to promote a conservative agenda against Macron and to publish content from a known disinformation Russian sponsored outlet.

2. Manipulation and Editing

- **T0087.001: Develop AI-Generated Videos (Deepfakes) and T0087.002: Deceptively Edit Video (Cheap fakes):** This involves editing videos to misrepresent events or statements. In Portugal, the selective editing of a Bangladeshi immigrant approaching a right-wing politician was used to misrepresent the central message of the immigrant. Another example of selective video editing can be found in the fake Hulu video documentary trailer incident. This case study involves the use of authentic video interviews. Still, most of the interview scenes were professionally decontextualised and video edited to develop a realistic-looking fake video documentary trailer that falsely implicated various Western politicians in illicit activities, such as drug use.
- **T0086.003: Deceptively Edit Images (Cheap fakes):** Images are edited to mislead. Manipulated images were used to portray Eurovision 2024 as a propaganda tool for the EU, suggesting that it promoted an elite ideology disconnected from everyday concerns. The images were edited to include misleading captions and visual elements supporting the false narrative, distorting the public's perception of the event.

3. Decontextualisation

- **T0023.001: Reframe Context:** Using genuine images or videos out of context to mislead. This TTP was evident in the Spanish case, where a manipulated video purportedly showing a Muslim urinating on pork was spread to incite fear and mistrust.

3.2 Establishment of legitimacy

1. Impersonation and cloning

- **T0013: Create inauthentic websites (Cloning):** Cloning legitimate media and government websites to spread disinformation. The Doppelganger operation cloned media and government sites to spread anti-Ukrainian and pro-Russian content. APT WeRedirect also used media website cloning on a large scale.
- **T0099: Prepare Assets Impersonating Legitimate Entities:** Impersonating public figures to legitimate the disinformation message. This technique was used in Portugal with the impersonation, via deep fake, of the voice of a politician to legitimise content.Associating disinformation with reputable brands or platforms. The fake Hulu trailer leveraged Hulu's brand to lend credibility to its false narrative.
- **T0084: Reuse Existing Content, T0098.002: Leverage Existing Inauthentic News Sites and T0087.002: Deceptively Edit Video (Cheap fakes):** In the Hulu fake video documentary trailer case, existing content was repurposed and repackaged to create disinformation narratives. This includes manipulating interviews and public statements into a cohesive, misleading trailer format.

3.3 Content dissemination TTPs

1. Social media amplification

- **T0119: Cross (platform) Posting:** Posting the same content across multiple social media platforms to increase reach and visibility. This TTP was seen in several campaigns, including the anti-immigrant narratives in Portugal.
- **T0049.001: Trolls amplify and manipulate and T0049.003: Bots Amplify via Automated Forwarding and Reposting:** Trolls and bots are deployed to amplify content and create the illusion of widespread support. This technique helps artificially boost the visibility of disinformation. It was used in Operation Overload to give relevance to the content flagged to fact-checkers.
- **T0019.002: Hijack Hashtags:** In Italy, threat actors artificially pushed the election hashtag #ElezioniEuropee to spread disinformation.
- **T0018: Purchase Targeted Advertisements:** In Doppelganger and APT WeRedirect cases programmatic advertising in social media platforms is exploited at large.

2. Use of existing networks / content

- **T0098.002: Leverage Existing Inauthentic News Sites:** In the Lithuanian deep fake, the disinformation was amplified through a network of clone websites, primarily to avoid geoblocking (e.g., Ldiena.lt, 20min.lt, Blogorama.lt). This indicates a coordinated effort to spread the false narrative across multiple domains to enhance visibility and credibility.

- **T0049: Flooding the Information Space and T0049.003:** Bots Amplify via Automated Forwarding and Reposting: In Operation Overload, a group of social media accounts was used to amplify certain content in a coordinated manner to get attention from fact-checkers. Attention to the content was first raised via a network of fake email accounts, spamming the organisation's inboxes with requests for content verification.
- **T0002: Facilitate State Propaganda:** Eurovision conspiracy theories were not only spread by inauthentic sites but found their way into Russian state media, as well.
- **T0084: Reuse existing content:** In France, the threat actor leveraged existing content from a website identified and shut down by Operation Doppelganger, to reframe it into a new inauthentic news website.
- **T0102.001: Use existing Echo Chambers/Filter Bubbles:** The fake Hulu trailer was shared in pro-Russian communities. The primary channel spreading the video, НЕБОЖЕНА, is known for its pro-Russian and anti-Western narratives.

3.4 Other Relevant TTPs

1. Attacking the target

- **T0019: Generate information pollution and T0049: Flooding the Information Space:** Operation Overload discovered a coordinated effort to overflow fact-checking and other organisations' mailboxes with false verification requests.
- **T0083: Integrate Target Audience Vulnerabilities into Narrative:** In the gendered disinformation campaign during the EU elections, false narratives were coupled with specific threats and bullying.

2. Exploiting existing issues:

- **T0083: Integrate Target Audience Vulnerabilities into Narrative:** By targeting a sensitive issue on which division already exists, such as the Israel-Palestine conflict, gender issues, or racial tensions in New Caledonia, campaigns aim to exploit existing tensions and sensitivities to increase the narrative's resonance and spread.

3. Conceal purpose

- **T0128.002: Conceal Network Identity and T0129: Conceal Operational Activity:** In Portugal, YouTube ads against the centre parties were linked to shell companies and offshore entities to obscure the actual sponsors. Similarly, a pro-Russian Facebook page in France was found to be managed by administrators in Benin. APT WeRedirect is another large case that shows the use of concealed entities.
- **T0124.003: Exploit Platform TOS/Content Moderation:** Despite efforts by several social media platforms to reduce the spread of Russian malign influence, several overt Russian accounts, including on TikTok, were accessible to audiences in the EU. In Spain, disinformation regarding the elections was written with changes to escape moderation identification. This tactic was also noted in France, where pro-Russian and anti-Ukrainian pages used coded language to avoid detection.

- **T0128.002: Conceal Network Identity:** In the Lithuanian deep fake audio, the disinformation was strategically released over a short period (October 20-23, 2023), maximising the impact and ensuring rapid dissemination before authorities or fact-checkers could respond effectively.

4 Conclusions

The analysis of foreign information manipulation and interference (FIMI) cases and general disinformation campaigns identified during elections in Europe during the first half of 2024 reveals significant insights into the narratives and tactics used by disinformation actors. This report exposes the increasingly advanced methods employed by disinformation actors, highlighting the urgent need for enhanced countermeasures. The collaborative efforts of FIMI-ISAC members have provided crucial insights into these evolving threats, underscoring the critical importance of heightened vigilance and coordinated responses.

4.1 Summary of findings

The case studies in this report expose the wide-ranging and insidious narratives and tactics deployed in FIMI campaigns. Dominant narratives include anti-immigrant sentiment, institutional distrust, targeted discrimination, and harmful health disinformation. The report identifies an arsenal of tactics, including AI-generated content, sophisticated image manipulation, and coordinated inauthentic behaviour campaigns.

While deep fake content represents a new frontier, most TTPs and narratives are well-established in the disinformation landscape. Their persistent and widespread use demands immediate and forceful action from platforms and stakeholders. The report highlights the interconnectedness and repetition of narratives and TTPs across countries, geopolitical scenarios, and platforms, revealing a coordinated attack on democratic societies.

In March 2024, the European Commission (EC) published guidelines under the Digital Services Act (DSA) for the mitigation of systemic risks online during elections. The Commission recommended that Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) implement election-specific risk mitigation measures tailored to individual electoral periods and local contexts and cooperate with EU-level and national authorities, independent experts, and civil society organisations. Furthermore, the EC also recommended assessing the effectiveness of the measures through post-election reviews.

Despite these election guidelines, the proliferation of disinformation narratives during the EU elections signals that voluntary recommendations are insufficient to safeguard EU democratic processes. Consequently, as the DSA and Digital Markets Act (DMA) reach a critical enforcement stage, a whole-of-society approach becomes even more important to address these challenges.

4.2 Implications for future elections and disinformation strategies

The findings underscore the critical need to assess the existing measures for combating these campaigns. The continued deployment of well-known divisive narratives and repetitive tactics such as cloning news websites exposes vulnerabilities in current defence strategies.

It is imperative to develop and implement data-driven, proactive strategies to decisively counter prevailing narratives and TTPs. This includes dramatically enhancing public awareness, substantially increasing investment in research and open-source data collection tools, demanding fundamental platform design changes, and developing more sophisticated alert systems.

While disinformation campaigns will undoubtedly evolve, with threat actors adapting their methods to evade detection and countermeasures, the persistent reappearance of the same narratives and TTPs signals a failure in current defence mechanisms. This demands an urgent, comprehensive reevaluation of our approach to safeguarding democratic processes and information integrity.

Abbreviation	Description
FIMI	(Foreign) Information manipulation and interference describe a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative, conducted intentionally, and coordinated by state or non-state actors, including their proxies inside and outside their territory.
TTP's	In the context of FIMI, "Tactics, Techniques, and Procedures" are patterns of behaviour used by threat actors to manipulate the information environment to deceive. Tactics describe operational goals that threat actors are trying to accomplish. Techniques are actions explaining how they try to accomplish it. Procedures are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.
DISARM Framework	Disinformation Analysis and Risk Management is an open-source framework designed to describe and understand the behavioural parts of FIMI/disinformation. It sets out best practices for fighting disinformation through sharing data & analysis and can inform effective action. The Framework has been developed, drawing on global cybersecurity best practices.
OpenCTI	The Open Cyber Threat Intelligence Platform is a platform for processing and sharing knowledge for cyber threat intelligence purposes. It was developed by the French National Cybersecurity Agency (ANSSI) and the CERT-EU (Computer Emergency Response Team of the European Union).

STIX 2.1	Structured Threat Information Expression (STIX™) is a data format for encoding and exchanging cyber threat intelligence (CTI) and sharing insights on FIMI incidents.
Observables	Observables are concrete elements relevant to understanding how an incident unfolded, such as a tweet, a video on YouTube, or an article on a website. They can be represented via the URL under which they were found or as files.
Kill Chain	The Kill Chain is a model breaking down multiple stages of an attack perpetrated by a malign actor, allowing analysts to predict, recognise, disrupt or prevent the attack. It was originally a military concept further adapted for cybersecurity and can be applied to FIMI, too.