POLICY BRIEF

APRIL 2025

MANIFESTATIONS OF FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI)
EXECUTIVE SUMMARY, CONCLUSIONS AND RECOMENDATIONS

Recommended citation: Wright, David (ed.), Malak Altaeb, Tim Beyer, Annye Braca Joshua Bronson, Owen Conlan, Arsenio Cuenca, Marios Dikaiakos, Zaur Gouliev, Pablo Hernández, Richa Kumar, Evangelos Markatos, Raquel Miguel, Gary Munnelly, Alina Östling, George Pallis, Emmanouil Papadogiannakis, Demetris Paschalides, Pau Perea, Anna Pomortseva, Marianna Prysiazhniuk, Celia Ramos-Vera, Kristian Reeson, Elodie Reuge, Mario Reyes de los Mozos, Joakim Rosell, Maria Giovanna Sessa, Brendan Spillane, Dimosthenis Stefanidis, Niklas Strand, Jaakko Tyni, Ilkka Vuorikuru, David Wright (authors), Executive Summary, Conclusions and Recommendations, ATHENA, D1.1, 2025.

ACKNOWLEDGEMENT

This report is based on research conducted in the ATHENA project (November 2023 – October 2026), co-funded by the EU and UKRI under grant numbers 101132686 and 10107667 respectively. The latter applies to Trilateral Research. The authors are partners in the ATHENA consortium (An exposition on THe forEign informatioN mAnipulation and interference).

Co-funded by the European Union

DISCLAIMER

Views and opinions expressed in this policy brief are those of the authors only and do not necessarily reflect those of the European Union, the European Research Executive Agency (REA) nor UKRI. Neither the European Union nor UKRI can be held responsible for them.

EXECUTIVE SUMMARY

This report contains 32 case studies of foreign information manipulation and interference (FIMI). The authors examine the range of tactics, techniques and procedures (TTPs) that malign actors employ to deceive populations and undermine democracy. The authors seek to raise public awareness about FIMI. The case studies follow a structure for FIMI that we commend to other researchers as a step toward harmonisation of approaches and creation of a repository of FIMI case studies to better understand what attackers are doing.

The emphasis here is on *foreign.* Those engaged in FIMI activities are also often engaged in domestic disinformation (DIMI). There is, of course, lots of disinformation purveyed by domestic actors inside countries, e.g., the thousands of lies from the convicted felon and twice-impeached, twice-elected US President.[1] FIMI applies to disinformation purveyed by a foreign entity, whereas disinformation can be domestic or international. FIMI seems implicitly more serious, as it indicates interference in the affairs of another country, whereas disinformation does not necessarily imply a political agenda. FIMI implies the gravity of what foreign actors are trying to do outside their countries, whereas disinformation, while always to be called out, does not give any indications of the seriousness of the actions in question.

Our case study approach provides more granularity than other studies that aggregate FIMI attacks. Both approaches are necessary and useful. The case study approach provides more context for individual attacks that one doesn't necessarily find in FIMI studies that aggregate the findings of many attacks. The case study approach provides more detail on the objectives of the FIMI attack, the threat actors, the TTPs used, the effectiveness of the attack, the countermeasures (if any) applied against the attack, and what conclusions and recommendations one can draw from the case study. The aggregate approach, however, arguably gives a better picture of just how widespread, how prevalent, how big a problem FIMI has become.

Two-thirds of the case studies herein concern actions taken by Putin's Russia against other countries, notably Ukraine, especially since the Russian invasion in February 2022. While Russia appears to be far and away the most prolific of FIMI actors[2], our report includes case studies involving China, Iran, North Korea, Turkey, Saudi Arabia and India which have also engaged in FIMI. Our percentage of case studies involving Russia is about the same as those analysed by the European External Action Service (EEAS) in its first FIMI report.[3] Indeed, it is instructive to understand the range, scale and sophistication of TTPs used by the Russians.[4]

---

[1] See, for example, McQuade, Barbara, *Attack from Within: How Disinformation Is Sabotaging America*, Seven Stories Press, New York, 2024.

[2] "Russia continues to pose the greatest threat when it comes to election disinformation, authorities said, while there are indications that Iran is expanding its efforts and China is proceeding cautiously when it comes to 2024." Klepper, David, "Russia Is Relying on Unwitting Americans to Spread Election Disinformation, US Officials Say", AP News, 29 July 2024. https://apnews.com/article/russia-trump-biden-harris-china-election-disinformation-54d7e44de370f016e87ab7df33fd11c8. "Director of National Intelligence Avril Haines told Congress May 15 that China, Russia and Iran are the leading threats, but Russia stands out as the most active." Editorial Board, "From Iran and Russia, the Disinformation Is Now. The Target Is America", *Washington Post*, 19 Aug 2024. https://www.washingtonpost.com/opinions/2024/08/19/russia-iran-ai-disinformation-election/.

[3] European External Action Service (EEAS), "1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence", January 2023. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

[4] In this book, the authors often refer to "Russia", "the Russians", "China", "Iran", etc. While most of the case studies focus on FIMI perpetrated by the governments of the countries cited, often those governments outsource

Undoubtedly, other countries – the US, UK, France, Australia, etc. – also engage in FIMI, however, this report focuses on the FIMI cases generated by authoritarian regimes. We include case studies of FIMI that have been relatively successful as well as others that failed to gain much traction. Some FIMI attacks are more impactful than others, however, we have not selected case studies based only on their impact. In some cases, where FIMI attacks failed to gain traction, we are interested in why they didn't gain as much traction as those cases that were very impactful.

We commend this report to various stakeholders – FIMI researchers, policymakers, academics, civil society organisations. We hope it will raise stakeholder and public awareness about the range of TTPs that attackers employ and what countermeasures are effective in countering this insidious phenomenon.

The co-authors of this text are partners in the EU-funded ATHENA project (Nov 2023 – Oct 2026). The partners selected the case studies from a list of disinformation reports and articles in journals and newspapers that we had compiled in Zotero by the end of 2023. The number of items in the folder "Russian disinfo" was more than 10 times greater than those involving China. We took into account various criteria in making our selection, such as the variety of TTPs used, the availability of data and reports on which we needed to draw to construct the case studies, the scale of the FIMI attacks, the geographic dispersion, the presumed objectives of the attackers, their effectiveness and the countermeasures employed against them.

The case studies herein draw on the DISARM Foundation's framework.[5] There are various frameworks for analysing disinformation, but we chose the DISARM framework, as it is employed by others such as the EEAS, Viginum, the governmental agency in France charged with exposing disinformation in that country and others. The DISARM framework was based on the ATT&CK framework developed by the MITRE Corp in the US as well as the STIX format[6]. The ATT&CK framework concerns cyberattacks more generally and as many FIMI attacks are also cyber-based, it is another reason we adopted the DISARM framework. The authors of this report have had numerous interactions with officials from the DISARM Foundation who have been kind enough to give detailed webinars on their framework to the partners.

Chapter three of this report focuses on different frameworks that are pertinent to the analysis of disinformation, including those mentioned above as well as FIMI-ISAC, OpenCTI, MISP, Oasis Open, RAND, the Centre for Advanced Tactics to counter Disinformation (ADTAC), the Credibility Coalition, the Information Laundromat, the EU Code of Practice on Disinformation.

---

their FIMI activities to third parties. We have seen the phenomenon of disinformation-for-hire companies who offer their services to governments or their proxies. In other cases, some companies contribute to the FIMI activity, without necessarily coordinating with the government in question, more for financial motivations than political. Attribution to a specific government agency or department or unit is challenging. Hence, throughout the book when we refer to Russia or the Russians or China or the Chinese or whomever, we know the evidence (the observables) points to the government, its proxies, its collaborators and/or its companies and/or other groups or citizens with origins in the country referenced without knowing who specifically is responsible for generating and deploying the FIMI.

[5] https://www.disarm.foundation/framework

[6] https://oasis-open.github.io/cti-documentation/stix/intro.html

Chapter four consists of our 32 case studies. We presented this list at a face-to-face meeting of partners, the EC Research Executive Agency, DG Research and the EEAS. In the section that follows, we present a very brief summary of each of the case studies.

Chapter five consists of our analysis of the tactics, techniques and procedures used in the case studies and elsewhere. Chapter six is a synthesis of 20 interviews conducted by the authors with experts in disinformation. It summarises key issues pertinent to our study of FIMI. Chapter seven, the last, has our conclusions from undertaking the case studies as well as our recommendations directed to the European Commission and the DISARM Foundation.

FIMI case studies

The numbers of the case study summaries below correspond to their numbers in Chapter four.

4.2: Did the Russians dupe the US Republication Party?
Alexander Smirnov, a Ukrainian who claims to have had contacts with the GRU, the Russian military intelligence service, had been an agent for the FBI for some years before he claimed in 2020 to have evidence that Joe and Hunter Biden had each received bribes of US $5 million. Republicans took a redacted FBI statement as evidence of Biden's corruption and a reason to impeach him. In Feb 2023, the FBI said Smirnov had produced no evidence of Biden bribery.

4.3: How the Russian FIMI actors reacted to the US aid package
This case study focuses on Russia's FIMI, which touted the inevitability of victory over Ukraine even with the US's support and military and financial aid. The case portrays a campaign in response to the aid package approved by the US Congress in April 2024. Our analysis suggests two main narratives around the subject. The first one claimed Ukrainian statehood is false, as it relied on Western support and, second, the inevitability of Ukrainian defeat even with the military and financial support provided by the West.

4.4: Russian initiatives to use farmers' protests in Germany
In January 2024, Germany was scene of one of the largest farmer protests in the nation's history. Federal government plans to cut subsidies for the agrarian sector prompted farmers to demonstrate in cities and on highways to show their opposition to the plans. The demonstrations were a prime target for foreign intervention in the form of a FIMI campaign, as Russia linked them to German military aid to Ukraine.

4.5: Russian FIMI about burning the Quran in Sweden
Sweden applied to join NATO on 18 May 2022. This was a significant shift for the country, and a change in the balance of power around the Baltic, especially as Finland was also applying for membership in NATO. Throughout 2023 and 2024, an orchestrated campaign from Russian and Iranian sources tried to tie the Swedish state to several Quran burnings. This campaign focused on increasing conflict between Sweden and Muslim-majority countries while Sweden was trying to join NATO.

4.6: Russian FIMI about the (fabricated) "Lisa" rape case
On 11 January 2016, 13-year-old Lisa disappeared on her way home from school in Berlin. The next day, Lisa turned up again and told her parents that she had been abducted to a flat by three unknown "southerners" who could barely speak German, beaten several times and raped. The combination of Lisa's Russian German origin, the poor German language skills of her

parents and a bad crisis communication of the local authorities culminated in widespread protests fuelled by a Russian FIMI campaign in which the Russian Foreign Minister played a role that would rupture the social relationship between Russian-Germans and the rest of society.

4.7: Russian propaganda after Finland's transition to NATO

Finland's NATO membership in May 2023 was a response to the security threat posed by Russia's aggression against Ukraine. Historically non-aligned, Finland had maintained a "NATO option" as a political compromise. Despite expected protests from Russia, the reaction was limited to condemnation. However, there was a significant increase in asylum seekers at the Russian border, reminiscent of a 2016 incident. By late 2023, Finland closed several border crossings in response to the rising number of migrants. Suspecting Russian government intervention in pushing migrants to the border with Finland, the government cited national security and hybrid threats from Russia. Interior Minister Mari Rantanen indicated the situation could persist, and emphasised the need for firm, transparent decision-making, legislative readiness and EU solidarity to manage such crises effectively.

4.8: Russian FIMI framing the Finnish President before and after the election

Alexander Stubb, known for his pro-Western stance and criticism of Russia, has been negatively portrayed in Russian media, particularly following his comments on nuclear power and his stance during election debates. Russian narratives have framed him as hostile, with Kremlin spokespersons highlighting Finland's unfriendly position towards Russia. Stubb's call for European readiness in a *Financial Times* interview was depicted as war-mongering by Russian outlets, emphasising NATO's eastward expansion. High-profile figures like Stubb are vulnerable to hostile influence operations, necessitating robust media protection strategies and institutional support to mitigate disinformation and safeguard national security.

4.9: Russia Today (RT), its narratives and ideological biases

RT has functioned as one of the Kremlin's most effective weapons in its informational battlefield against Western democracies. Its main strategy is based on the adoption of an "anti-hegemonic" editorial line, with criticism of governments in Europe and the US, exploiting their vulnerabilities and increasing polarisation. RT shows how disinformation can be effective while adopting a particular ideological scope and not necessarily only spreading hoaxes.

4.10: A Wagner campaign targeting French Army in Mali

In collaboration with the Malian junta, the Wagner Group orchestrated a disinformation campaign aimed at covering up their involvement in a civilian massacre. By staging evidence, they deflected blame onto the French military, operating in Mali as part of Operation Barkhane. This FIMI attack brought together the physical and cyber realms. Wagner spread images of a mass grave, which they had staged. They promoted narratives exploiting the colonial heritage of France in Mali.

4.11: Russia uses bribery to spread disinformation

Since 2014, Russia has spent more than $300 million bribing foreign politicians, primarily in Europe, to spread pro-Russian narratives and undermine democratic processes. The bribery is part of a broader disinformation campaign that targets media and politicians, attempting to influence public opinion on its war against Ukraine and other issues. Key figures, including Viktor Medvedchuk and Artem Marchevskyi, have been key actors in orchestrating these efforts through platforms such as *Voice of Europe*. Law enforcement across Europe is investigating covert payments and propaganda networks linked to Russian state interests.

Countermeasures, such as sanctions and new legislation, are being developed to combat this growing threat to democratic integrity.

4.12: Russian interference in the Spanish election in July 2023

The Russian-speaking community based in Spain was the target of a FIMI campaign that disseminated false material through the Telegram platform, cloned websites and bulletproof hosting[7]. Its intention was to create mistrust among this group of people. The campaign's restricted focus meant that, despite its advanced methods, it had little effect on the larger Spanish electorate. The strategy was successful in confusing the targeted population, but it had little impact on the results of the national election.

4.13. Altered photo showing Zelensky holding a jersey with a swastika

In the first days after Russia's 2022 aggression against Ukraine, Russian-aligned actors used blogs, social networks and inauthentic news websites to spread a cheaply doctored photo of President Zelensky holding a jersey with a swastika, falsely portraying him as a Nazi sympathizer. Recycling a 2021 image, the actors aimed to flood digital space, degrade Zelensky and his institution, distract from Russian aggression and justify the invasion by reinforcing the Kremlin's "de-Nazification" narrative.

4.14: Disinformation about Zelensky buying a villa in Florida

In late 2023, a YouTube video featured an alleged Secret Service agent claiming that Zelensky was going to flee to the US, obtain citizenship and buy a villa in Florida funded by US aid. DC Weekly, linked to Russian propaganda, amplified the story with fabricated details. Coinciding with Zelensky's visit to secure US aid, US political influencers and Russian media, including RT and TASS, promoted the story to undermine Zelensky's image, divide US public opinion and undermine support for aid to Ukraine.

4.15: European Parliament report on FIMI in European elections

In June 2024, European citizens voted for the new European Parliament. This case study highlights a sophisticated disinformation campaign during the European Parliament elections, orchestrated primarily by the Voice of Europe. The campaign was backed by pro-Kremlin advocates Viktor Medvedchuk and Artem Marchevskiy, aiming to sway public opinion and undermine the European Union's democratic processes and its support for Ukraine. The Russians used multiple tactics, including distorted narratives, divisive rhetoric and strategic manipulation of social media platforms**.**

4.16: Doppelganger: Russian disinformation using media clones and more

Since February 2022, the Russian-origin "Doppelganger" operation—also known as RRN (for Reliable Recent News)—has targeted multiple countries to undermine support for Ukraine by impersonating media and institutions' websites and spreading disinformation. Despite the identification and sanctioning of the main actors, the operation has expanded with new actions and a complex obfuscation infrastructure to persist and target other international events. Doppelganger is linked to other Russian campaigns.

4.17: Russian disinformation about Russian attacks

The case discusses how Russia has used its FIMI campaigns to frame Ukrainian forces as responsible for the consequences of Russian missile attacks. The case explains how the shifting of responsibility has been instrumentalised since 2014 and reinforced after 2022 when the

[7] Bulletproof hosting refers to web hosting services that are designed to be highly resistant to takedowns.

large-scale phase of aggression began. In this case, Russia blamed the Ukrainian air defence for the damage caused by Russian missiles in Odesa in 2024. It shows how the Russian narrative tried to shift responsibility for war crimes and aggression onto Ukraine.

4.18: Russian FIMI against the Armed Forces of Ukraine

Russia's FIMI activities has targeted the Armed Forces of Ukraine (AFU) since its Russia's illegal annexation of Crimea in 2014. It has attempted to build a positive image for the Russian army while demonizing the AFU. The FIMI campaigns have run alongside military actions. The FIMI only grew after Russia's large-scale invasion of Ukraine in 2022. The disinformation campaigns against the AFU aimed to weaken societal trust in the army, demoralise its members and justify Russian actions domestically and internationally. These efforts sought to undermine Ukraine's defence capabilities and public morale while bolstering Russia's geopolitical and ideological narratives.

4.19: Russian disinformation about COVID-19 vaccines

Fazze, a Russian-co-owned website that describes itself as an "influencer marketing platform" connecting bloggers and advertisers, contacted YouTubers in France and Germany and offered them money to tell their followers that the Pfizer/BioNTech vaccine was responsible for hundreds of deaths. Fazze told the influencers to say that the death rate from Pfizer's vaccine was three times that from AstraZeneca's, which is technologically similar to Russia's Sputnik V vaccine. Although influencers in France and Germany quickly went public with Fazze's approach, influencers in India and Brazil published content (now deleted) compatible with Fazze's request.

4.20: Meta dismantles large-scale Chinese disinformation campaign

Many organised accounts of Chinese origin use social networks such as Meta to spread disinformation about other countries' policies and to change the narrative on different social issues such as the origin of COVID. Platforms such as Facebook (Meta) use disinformation detection algorithms to detect and eliminate these campaigns. However, these campaigns advance over time by redirecting Facebook users to other pages to make the campaigns more difficult to detect.

4.21: Facebook accounts in China impersonated Americans, Meta says

In the previous use case, we examined the campaign detected by Meta some years ago, while in this case, we see how it has evolved over time to the present. We also see how the methods followed by Chinese disinformation organisations remain the same given the difficulties for algorithms to detect them when using external pages.

4.22: PAPERWALL: Chinese websites pose as local news to target global audiences

The PAPERWALL campaign involves more than 100 websites operated from China, posing as local news outlets in 30 countries across Europe, Asia and Latin America. These sites disseminate pro-Beijing disinformation, often hidden within commercial content. Attributed to a PR firm, PAPERWALL shows China's increasing use of private firms to manage foreign influence operations. Despite the limited current exposure, the rapid proliferation of these sites presents long-term risks.

4.23: Chinese disinformation about the release of Fukushima water

On Friday, 11 March 2011, an earthquake of magnitude 9.0 hit Japan. The earthquake impacted the Fukushima nuclear power plant; large quantities of water were used to cool down the reactors damaged by the earthquake. This water was treated and stored in tanks. Japan, in

accordance with international practices, started releasing the treated wastewater into the Pacific Ocean in August 2023 at a slow rate of 130 tons of water per day. This release triggered a torrent of disinformation in some cases including pictures of dead fish and pollution and attributing them to the release of the Fukushima water. In retrospect, the pictures were from different regions of the planet, sometimes taken well before the release of the water, and completely unrelated to the Fukushima event.

4.24. Turkey's disinformation about North Cyprus as an independent state

Amid the Russia-Ukraine war, Russia's plan to deploy a mobile consular unit in the unrecognised "Turkish Republic of Northern Cyprus" (TRNC) led to false claims in Turkish and Turkish Cypriot media that Russia was opening a consulate, implying official recognition. This discourse, prominent from 2022 through 2024, fuelled discussions about increased Russian interest in the TRNC. The disinformation incident also spread on social media, with pro-TRNC groups pushing for the international recognition of TRNC.

4.25: Turkey's disinformation about a clash with the UN in the Cyprus buffer zone

Following Turkey's 1974 invasion, Cyprus was divided, creating a UN-controlled buffer zone between the Republic of Cyprus and the unrecognized TRNC. On 18 August 2023, a clash between UN peacekeepers and Turkish Cypriot forces in the buffer zone triggered a disinformation incident by Turkish and TRNC sources. They spread false narratives, portraying Turkish Cypriots as victims, misrepresenting UN actions and falsely claiming a Russian veto at the UN Security Council.

4.26: Varosha to Vegas: the real estate exploitation and disinformation tactics by TRNC

The TRNC has been illegally monetising Greek Cypriot properties in Turkish-occupied Cyprus, but these efforts have significantly intensified over the past year. Sensational narratives, such as transforming Varosha into the "Las Vegas of the Mediterranean", and false claims about King Charles III owning a luxury hotel and President Zelenskyy purchasing a casino have been used to manipulate public perception and attract foreign investment. Digital campaigns specifically target international buyers, while geopolitical manoeuvres, like rumoured Russian consular openings, create a facade of recognition. These tactics exploit legal vulnerabilities and geopolitical tensions to bolster the TRNC's legitimacy.

4.27: North Korea's disinformation campaigns

The United Front Department (UFD)'s Cultural Exchange Bureau, which reports to Kim Jong Un, has led North Korea's disinformation campaigns against its own people as well as against South Korea. It has used a variety of tactics and techniques. It mixes disinformation, propaganda, intelligence-gathering and subversion in a dangerous brew. In one incident, North Korean cyber trolls hijacked South Korean users' online accounts and posted an estimated 68,000 propaganda items.

4.28: Iranian interference in the US elections

Two Iranian nationals employed at the Iranian company, Emennet Pasargad, stole voter information data in US swing states prior to the 2020 US presidential elections. The stolen data was used to send false election messages and videos to threaten registered Democrat voters to vote for Donald Trump. The FBI was notified about the hacking and threatening messages and were able to block the unauthorised access of the hackers. The two Iranian nationals were charged with conspiracy to commit computer fraud and abuse, intimidate voters and transmit interstate threats. The Department of State's Rewards for Justice Program offered a reward of up to $10 million for information on or about the Iranian nationals' activities.

4.29: Saudi Arabia's anti-Iran campaign during the first Trump administration

This case study demonstrates how one country uses another's rhetoric to shape its own narrative and advance its strategic objectives through disinformation. It examines how Saudi Arabia exploited the Trump administration's anti-Iran stance (2017–2020) to further its own goals using FIMI techniques. By amplifying and distorting President Trump's anti-Iran statements, particularly his tweets, Saudi Arabia aimed to enhance its image while aligning its narrative with US policy and increasing negative sentiment towards Iran and undermining its Middle Eastern rivals.

4.30: Cyberwarfare and the Qatar blockade

The May 2017 cyberattack on the Qatar News Agency (QNA) illustrated the role of cyberwarfare in shaping public perception and igniting international tensions. Hackers disseminated fake statements attributed to Qatar's Emir, commending Iran and extremist organisations. These misleading claims intensified pre-existing strains between Qatar and its Gulf neighbours, leading to a diplomatic crisis. Consequently, Saudi Arabia, the United Arab Emirates, Bahrain and Egypt severed relations with Qatar and initiated a blockade that lasted for three and a half years.

4.31: The role of FIMI in Iraq's Tishreen protests

This case study examines how foreign actors, primarily Saudi-linked, used FIMI tactics to manipulate the narrative surrounding the 2019-2020 Iraqi protests[8]. False narratives were spread on social media aimed at discrediting Qatar and particularly pro-Iran factions in Iraq. The goal was to undermine the legitimacy of the protests and amplify anti-Iran sentiments, ultimately serving Saudi geopolitical objectives. The study identifies key FIMI tactics, such as the creation of inauthentic accounts, manipulation of the social media narrative and emotional appeals, all of which contributed to shaping public discourse and undermining the objectives of the protest movement.

4.32: India disinformation campaign following the Pulwama attack

The Indian disinformation campaign following the 2019 Pulwama attack, where a suicide bomber killed more than 40 security personnel, exemplifies contemporary information warfare. By portraying Pakistan as the primary aggressor, the campaign actively worked to undermine its international standing and diplomatically isolate the nation. These narratives escalated tensions and kept Pakistan on the FATF grey list[9]. By strategically manipulating conflicts and emotional responses, the operation effectively shaped public perception and political discourse. Its consequences—strained diplomatic relations, societal fragmentation and diminished media credibility—highlight the enduring challenges that disinformation poses in today's geopolitical landscape.

4.33: Turkey sought to undermine Sweden's bid for NATO membership

From 2022 to 2024, Turkey conducted a coordinated campaign to challenge Sweden's NATO membership bid, using disinformation to frame Sweden as a terrorist supporter, particularly concerning the Kurdistan Workers' Party (PKK). This strategy was synchronised with ongoing NATO talks, as Turkey wielded its veto power to coerce Sweden into agreeing to concessions like tougher anti-terror laws and considering extraditing individuals Turkey categorised as terrorists. Through state-controlled media, bot networks and social media narratives amplified

[8] The Tishreen protests in Iraq derived from the Arabic name for the month of October, "Tishreen Al-Awwal".
[9] The FATF is the Financial Action Task Force which puts the spotlight on countries with deficiencies in their measures to combat money laundering, terrorist financing and proliferation financing.

by hashtags such as #NATOVetoOnSweden, Turkey disseminated claims linking Sweden to terrorism, thereby undermining its global credibility and using this as a reason for its veto. The disinformation efforts were directed at both domestic and international audiences, using multiple languages for broader impact. Nevertheless, Sweden officially joined NATO in March 2024. This case study provides insight into how FIMI can influence international discussions and negotiations by leveraging strategic narratives and state-controlled information spaces.

Reverse engineering of TTPs

The case studies are followed by a chapter on the tactics, techniques and procedures (TTPs) used in the case studies and elsewhere. The chapter on TTPs was based on the DISARM Framework[10], from which we created JSON files[11]. Following is a screenshot of what the framework looks like.

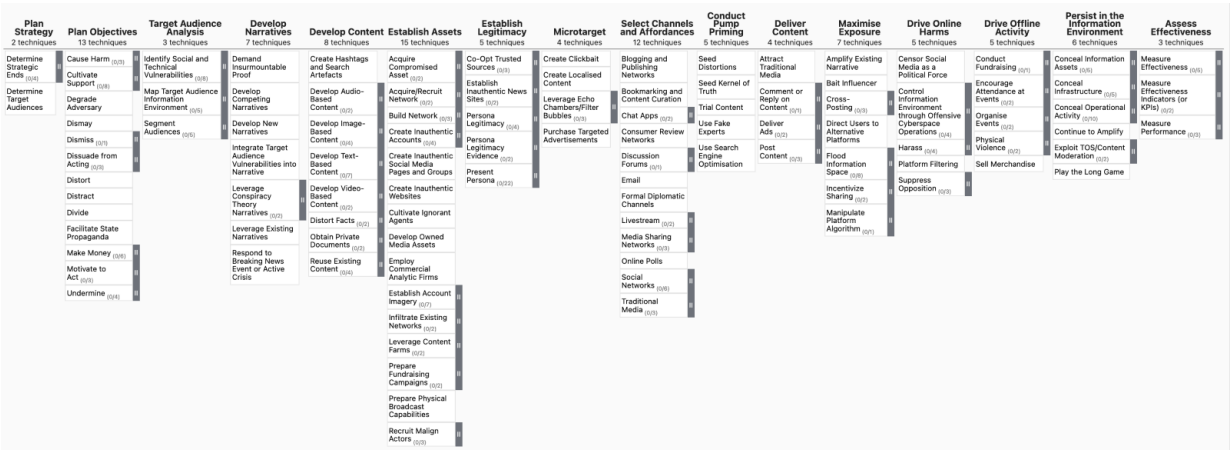

Fig. 1: DISARM Navigator

[10] https://disarmfoundation.github.io/disarm-navigator/

[11] JSON (JavaScript Object Notation) files are text-based files used to store and transmit structured data in a format that is both human-readable and machine-readable.

Complementing DISARM, we propose the **ATHENA FIMI analysis framework**, offering a robust methodology for identifying, gathering, storing and sharing TTPs through **observable** and **incident canvases**. These canvases employ design-thinking principles[12] to guide analysts in capturing detailed information about individual disinformation pieces and broader incidents, ensuring a thorough understanding of how disinformation campaigns are structured and executed. Key steps in this methodology include defining targets and threat actors, mapping information sources, gathering and verifying data, examining content, reverse engineering TTPs and reporting findings.

Analysis of TTPs in FIMI operations

We employed the ATHENA FIMI analysis framework to extract and analyse the TTP patterns from the 32 FIMI case studies. Our analysis unveiled critical patterns in the deployment of TTPs by various geopolitical actors and their proxies. These case studies, encompassing, among others, Russian, Chinese, Turkish, North Korean, Indian and Saudi disinformation efforts, reveal a sophisticated and strategic use of TTPs aimed at destabilising democratic institutions, manipulating public opinion and advancing geopolitical objectives. Proxies, such as state-affiliated media outlets and non-state actors, play a pivotal role in amplifying disinformation while maintaining plausible deniability. Predominantly, threat actors emphasise content creation and manipulation, particularly through social networks, employing techniques like "Undermine" (T0135[13]), "Divide" (T0079) and "Distort Facts" (T0076) frequently across campaigns. Additionally, strategic audience segmentation (T0072) and leveraging existing narratives (T0003) amplify the reach and impact of disinformation efforts, often exploiting echo chambers and filter bubbles (T0102) to reinforce polarised narratives. Our TTP analysis highlights several key insights relevant to FIMI campaigns:

- **Understanding evolving disinformation strategies**: Disinformation campaigns are highly adaptive and strategic, consistently combining specific TTPs to enhance their operational impact. The frequent use of "Develop Text-Based Content" (T0085) alongside "Social Networks" (T0104) indicates a sophisticated approach to crafting and disseminating misleading information. This adaptability underscores the necessity for dynamic and flexible countermeasures that can evolve in tandem with threat actors' strategies.

- **Targeted tactics in specific contexts**: Disinformation campaigns are meticulously tailored to specific geopolitical contexts, such as Russia's efforts against Ukraine or Turkey's campaigns targeting Cyprus. These operations use tactics like "Segment Audiences" (T0072) and "Leverage Existing Narratives" (T0003) to exploit local vulnerabilities and align with broader strategic objectives. Understanding these targeted approaches is crucial for developing context-specific interventions that address the unique aspects of each disinformation campaign.

- **Recurring themes across multiple actors**: Multiple state actors employ similar TTPs to achieve their goals, such as "Distort Facts" (T0023) and "Amplify Existing Narrative" (T0118). This uniformity suggests the need for international cooperation and

[12] Gobble, MaryAnne M., "Design thinking", *Research-Technology Management*, Vol. 57, 1987, pp. 59 - 62. https://www.tandfonline.com/doi/abs/10.5437/08956308X5703005

[13] The DISARM Navigator applies codes, like those here, to the various tactics, techniques and procedures used by attackers. We reference these codes throughout this report.

coordinated strategies to address the transnational nature of FIMI campaigns. Collaborative efforts can enhance the effectiveness of detection and mitigation measures by leveraging shared insights and resources.

- **Amplification through echo chambers**: Disinformation campaigns frequently exploit echo chambers and filter bubbles (T0102), where manipulated content reinforces pre-existing biases without challenge. Techniques like "Flood Information Space" (T0049) and "Cross-Posting" (T0119) ensure that disinformation spreads rapidly within these closed networks. Addressing the algorithmic reinforcement of echo chambers on social media platforms is essential for mitigating the amplification of disinformation.

- **Use of multimedia to enhance credibility**: The strategic combination of text-based (T0085) and image-based content (T0086) with video elements (T0087) enhances the credibility and persuasiveness of disinformation. This multimedia approach makes false information more believable and harder to detect, necessitating advanced detection technologies that can analyse and verify content across multiple media types simultaneously.

- **Role of proxies in FIMI campaigns**: Proxies, such as state-affiliated media and non-state actors, extend the reach and complexity of disinformation campaigns while complicating attribution efforts. Techniques like "Create Inauthentic News Sites" (T0098) and "Create Fake Experts" (T0009) are frequently employed by proxies to build credible facades for spreading disinformation. Countermeasures must include strategies to identify and disrupt these proxy networks, as well as to enhance transparency and accountability in media operations.

Deepfakes and generative AI in TTPs

Deepfake technology exemplifies the integration of advanced AI into TTPs, significantly enhancing the capability of threat actors to create and disseminate deceptive content. Generative AI models like ChatGPT, Stable Diffusion and Midjourney facilitate the creation of highly realistic text, images and videos, which are pivotal in executing sophisticated disinformation strategies. These tools enable threat actors to automate content generation, making it easier to produce large volumes of convincing fake media that can be seamlessly integrated into influence operations.

The evolution of deepfakes from basic face-swapping to complex multi-modal forgeries demonstrates the significant advancements in generative AI. These technologies not only enhance the realism of fabricated content but also increase its scalability and distribution efficiency. The DISARM framework has recently updated its TTP taxonomy to include generative AI techniques, in recognition of the escalating threat posed by deepfakes in FIMI operations.

Real-world implications of deepfakes are substantial, with instances such as fake audio clips of US President Joe Biden and fabricated videos of UK’s Sir Keir Starmer highlighting the potential to disrupt political processes and erode public trust. These manipulations can influence election outcomes, incite social unrest and distort public discourse, posing severe threats to societal stability and democratic integrity.

Detection and mitigation of deepfakes involve a range of methodologies, including physical inconsistencies, fingerprint analysis, spatial and frequency-based techniques, and end-to-end AI models. Deepfake detection tools are essential for identifying synthetic media, although challenges remain in maintaining detection accuracy against continuously advancing deepfake technologies. Enhancing these detection capabilities requires ongoing research, diverse and comprehensive datasets, and the integration of robust AI-driven solutions.

Addressing the deepfake threat demands a multifaceted approach that includes technological advancements, regulatory measures and public awareness initiatives. Strengthening collaboration between technology developers, policymakers and researchers is crucial to develop effective countermeasures. Additionally, implementing ethical guidelines and fostering media literacy can help mitigate the impact of deepfakes, ensuring the resilience of democratic institutions and maintaining public trust in an increasingly digital world.

The interviews

The authors conducted 20 interviews with experts from various fields, including political science, security studies and social data analysis, who noted the complex and interdisciplinary nature of FIMI. The interviews revealed that there is disagreement on whether FIMI should be considered a technological or historical phenomenon, with different experts focusing on different aspects, such as practical, theoretical and geopolitical dimensions. However, there was a consensus on the need for a more unified approach to enhance research and improve frameworks for combating FIMI.

The interviews highlighted the increasing sophistication of FIMI, which has evolved beyond the creation of false narratives to manipulate existing societal divisions and exploit fears. This shift is fueled by geopolitical events, the rise of digital platforms and the growing role of AI and social media. Foreign state actors often collaborate with local groups to amplify divisive content, complicating attribution efforts. The shift from isolated incidents to coordinated, long-term disinformation campaigns requires an interdisciplinary collaboration across sectors and experts. To effectively address these challenges, strategic, long-term frameworks are needed that can counter the evolving tools and tactics used in disinformation campaigns.

Information manipulation has become a powerful tool in shaping geopolitical events, with state-sponsored campaigns from Russia, China, Iran and others identified as significant sources of FIMI. Governments, particularly of countries such as Ireland, the UK and Poland, are facing challenges in countering FIMI and hybrid threats, especially during elections and international security crises. Industry researchers and journalists have noted the changing tactics of these campaigns, including the manipulation of domestic and international narratives, with particular focus on ongoing conflicts such as the war in Ukraine. The role of digital technologies, social media and AI in spreading disinformation is central to these challenges, with AI both enabling the creation of false content and offering potential tools for detecting it. However, interviewees felt that the rapid development of generative AI models could overwhelm efforts to manage the sheer volume of manipulated content, while the Internet's profit-driven nature exacerbates the spread of fake information, limiting democratic discourse.

Traditional methods like human fact-checking are increasingly insufficient in the face of fast evolving FIMI campaigns. The use of advanced techniques such as narrative laundering, deepfakes, AI-driven content and closed platforms like Telegram makes tracing the origin of

disinformation a serious challenge. Such tactics complicate attribution, especially when perpetrators use tools like Tor to mask their identities. Countries such as Russia, China, Turkey and Iran have been identified as key sources of disinformation in specific regional contexts. The increasing availability of AI-powered disinformation tools makes campaigns more cost-effective and scalable, further complicating detection and attribution. To combat these challenges, our interviewees advocated improved attribution methods, better detection tools and greater cross-sector collaboration.

The interviews also underscored the multidisciplinary nature of FIMI research, with stakeholders from government, academia, media and industry all playing a role in tackling the issue. While collaboration is crucial, there are challenges in aligning objectives and coordinating efforts across sectors, especially during crises like elections or pandemics. The interviews also led to several key recommendations for improving efforts to combat FIMI. First, there is a need for a comprehensive, accessible framework for FIMI analysis. This framework should address the long-term, coordinated nature of FIMI campaigns and identify the social and political vulnerabilities they exploit. Second, efforts should be made to promote public awareness and enhance digital literacy, helping citizens to recognise manipulated information and understand the role of AI and algorithms in shaping the information landscape. Third, fostering international, cross-sectoral cooperation and training is crucial to countering state-sponsored disinformation campaigns, particularly from Russia, China and Iran. Governments, industry, academia and media must work together to develop coordinated strategies and support cross-disciplinary research initiatives. Finally, the need to enhance attribution methods and transparency is critical and more funding should be allocated to research focused on improving attribution, and social media platforms should be more transparent in their handling of disinformation.

The key conclusion we draw from the interviews is that addressing FIMI requires a multifaceted approach that combines technological innovation, interdisciplinary collaboration and strategic, long-term planning. As disinformation continues to evolve, coordinated efforts across governments, industries and academia will be essential to mitigate its impact on democratic processes and public trust.

Lessons learned

The range of case studies in Chapter 4 indicates a proliferation and inventiveness of different tactics, techniques and procedures employed by FIMI attackers. The case studies show the high adaptability of FIMI campaigns. FIMI actors use a wide range of platforms and techniques to evade detection and continue to spread their messages. Defenders need constant vigilance and adaptation of countermeasures as malicious actors' tactics evolve.

Attribution is a challenge. Some attackers cover their tracks well or engage in deniability. FIMI analysis requires an understanding of the different types of attackers in disinformation campaigns and their motivations.

Russia and China particularly use private firms to conduct their foreign influence campaigns, obfuscating the connections with the governments.

The term “useful idiots” refers to individuals who unwittingly support a cause or agenda—often political or ideological—without fully understanding its implications, particularly when

that cause is manipulative or harmful. The phrase was used to describe Western sympathisers of Soviet communism during the Cold War. The term has evolved and is now used more broadly to describe people who, in their enthusiasm or naivety, support movements, organisations or regimes that ultimately manipulate or exploit them. It is often used pejoratively to describe people who are seen as naïve or gullible in the political arena.

Although FIMI is frequently associated with elections, it has a much broader reach and continues to thrive even after the completion of the past EU elections of 9 June 2024. There remains a growing threat to democratic society. Attackers effectively employed information warfare techniques (such as content distortion and exploiting breaking news events) to amplify distrust within the EU, weaken transatlantic alliances and promote politicians sympathetic to the Kremlin. The incidents indicate a concerted effort not only to discredit the EU's actions but also to impact election outcomes by influencing voter sentiment through disinformation.

Sometimes attackers exploit historical tensions, as the Chinese did regarding Japan's discharge of Fukushima water or as Turkey has done in attempting to gain international recognition for its breakaway state in northern Cyprus. Disinformation spreads fast and often continues to spread even when the fakery is exposed.

Various potential threat actors, including state-sponsored groups, criminal organisations, hacktivists and individuals with malicious intent sometimes work together without any agreements. They share the same objective, so they all work to achieve it, bringing to bear their particular specialities in FIMI.

Social media has been found to be the biggest source of FIMI propagation. Protected, in part, by the pseudonymity provided by social networks, and sheltered by an almost total lack of transparency, aggressors find in social networks a fertile ground to cultivate and proliferate their propaganda.

The actual impact of a FIMI campaign is uncertain. One way of measuring impact is by the number of impressions that social media posts get. However, the difficulty in measuring effectiveness is trying to disentangle what is local and what is amplified by interference. Russian disinformation efforts, particularly focusing on social media as a significant battlefield for information warfare[14], have been subject to extensive analyses by most Western countries' cybersecurity firms, intelligence agencies and academic research. However, the effectiveness of these campaigns and the impact of Western countermeasures remain subjects of ongoing analysis and debate.

Among the best defences against disinformation is transparency, effective communication and the use of counter-narratives that challenge disinformation targeting the European Union. Providing EU citizens with discursive elements so that they can evaluate different situations linked to disinformation implies being self-critical and taking seriously the relationship of trust between the European institutions and the societies of the different Member States.

The EU has developed several frameworks to combat disinformation, including the EU Cybersecurity Strategy[15] and initiatives through the European Centre of Excellence for

[14] For a prediction about information warfare, see Wright, David, "AI and Information Warfare in 2025", 2019 IEEE SmartWorld, pp. 317–322. https://ieeexplore.ieee.org/document/906041
[15] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Countering Hybrid Threats[16]. These bodies help coordinate responses to foreign interference across EU institutions and Member States, building resilience against cyberattacks and disinformation campaigns targeting elections.[17]

The European Parliament has also passed a resolution denouncing Russia's FIMI campaign in the wake of the Voice of the Europe scandal wherein some Putin- / Russia-sympathetic MEPs were paid for interviews on the Russian controlled medium.

Effective countermeasures against disinformation campaigns require a multi-faceted approach, involving cooperation between governments, private sector entities (especially social media platforms), civil society organisations (CSOs) and the public. EU DisinfoLab has advocated the need for a whole-of-society approach to countering FIMI. However, this whole-of-society approach "can be realistically achieved only if the large variety of actors engaged in countering FIMI speak a common language. Initiatives such as the DISARM and STIX frameworks constitute that common language, set up to normalise the monitoring, analysis, assessment and response to FIMI operations."[18]

Governments and international organisations should focus on media literacy initiatives to help citizens critically assess information and resist manipulation. Governments should establish rapid-response teams trained to debunk FIMI as soon as it emerges.

Governments and/or CSOs should launch campaigns to educate the public on how to critically assess news sources and check for the credibility of information and to critically evaluate the credibility and motives behind information sources. Individuals should be encouraged to seek alternative sources and question information in public campaigns.

Transparency and maintaining the public's trust are crucial elements in any response strategy. For specific actions taken in response to FIMI attacks, citizens and practitioners alike should be able to consult official sources or reports from credible research institutions, project consortia and think tanks that focus on disinformation and cybersecurity.

The EEAS should prioritise investment in multilingual tracking tools capable of detecting FIMI across different languages. This would allow for faster identification of manipulative content in different linguistic and regional contexts.

National governments should strengthen monitoring mechanisms, improve transparency and work more closely with fact-checking organisations to mitigate the impact of FIMI.

EU Member States should promote image and video fact-checking skills to help individuals identify manipulated content and other forms of digital deception. Educating users about FIMI tactics can help them act as a first line of defence, significantly reducing the spread and impact of false information.

---

[16] https://www.hybridcoe.fi/

[17] Koudelka, Michal, and Petr Fiala, "Czechs Bust Russian Network Paying off European Politicians", Radio Prague International, 28 March 2024. https://english.radio.cz/czechs-bust-russian-network-paying-european-politicians-8812632.

[18] Hénin, Nicolas, "FIMI: Towards a European Redefinition of Foreign Interference", EU-DisinfoLab, Brussels, p. 11. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf?utm_source=chatgpt.com

The EU should expedite the implementation of legislation modelled after the US Foreign Agents Registration Act (FARA), requiring foreign-funded entities to register, thereby increasing transparency. Moreover, swift enforcement of upcoming regulations on political advertising will help to curb foreign interference. Further sanctions should target individuals and entities involved in Russian FIMI efforts, particularly focusing on those responsible for running disinformation networks like Viktor Medvedchuk and the Voice of Europe.

The DISARM framework has several strengths: (i) it provides a common methodology for analysing disinformation events, (ii) it provides a common terminology, and (iii) it has been adopted by the EU for exchange of FIMI information with the United States.[19] As attackers create new ways of FIMI, the DISARM Framework needs to evolve too (and it has). In addition to the Red and Blue Frameworks, it would be useful to have another framework on prevention and pre-bunking linked to the Red and Blue Frameworks.

The DISARM Framework itself does not explicitly classify threat actors. The Framework focuses on identifying the tactics, techniques and procedures (TTPs) used in disinformation campaigns, regardless of the specific actor behind them. The DISARM Framework should continue to evolve, incorporating more information, in tandem with other MITRE matrices (D3FEND), defining threat actor groups, as well as obtaining the template for disinformation campaigns. This will help, through the application of AI-based tools, to analyse the different disinformation actions and attribute their authorship.

CONCLUSIONS AND RECOMMENDATIONS

In this final chapter, we have selected some conclusions and recommendations from the preceding chapters. We emphasise the word *some*. The following are only *some* of our findings and recommendations which are scattered throughout the book. There are far too many to reproduce here. It's why the reader is encouraged to read the whole book! Nevertheless, we emphasise the following points, which are organised thematically with the findings, conclusions and recommendations grouped together by theme or issue.

Inventiveness of attackers

The 32 case studies in Chapter 4 indicate a proliferation and inventiveness of different tactics, techniques and procedures used by FIMI attackers. The case studies show the high adaptability of disinformation campaigns. Disinformation actors use a wide range of platforms and techniques to evade detection and continue to spread their messages. For those responsible for shaping policies or designing countermeasures, understanding these evolving tactics is critical to developing effective interventions. Defenders need constant vigilance and adaptation of countermeasures as malicious actors' tactics evolve. Companies must be constantly innovating to be able to detect malicious behaviours. This includes investing in artificial intelligence, machine learning and other cutting-edge tools for identifying patterns, analysing data and predicting future trends. By integrating proactive and reactive measures, states and institutions can strengthen their resilience against cyberattacks, mitigating the impact of disinformation campaigns and safeguarding democratic processes.

The EU should support research on network analysis techniques to track and reveal the coordinated activities of accounts engaged in spreading disinformation. By mapping the relationships among these accounts, researchers can identify behavioural patterns that indicate an inauthentic nature and coordinated manipulation efforts. Social media platforms should also invest in advanced technology, including network analysis and corpus analysis, to detect and remove disinformation, including tracking hashtags and detecting manipulative language.

Deepfakes can recreate an individual's face, voice and body movements, making them indistinguishable from real media. They enable the production of falsified content that can be used to depict inauthentic scenarios, such as a public figure making false statements or committing actions they never took. While these techniques have not been prevalent in past disinformation campaigns, their potential for widespread manipulation is immense. AI-generated deepfakes can be deployed to incite social unrest, undermine trust in political figures or manipulate global narratives through convincingly false visuals.

The current analysis process is heavily manual, which is unsustainable given the increasing volume of FIMI incidents. A semi-automated approach is needed to assist analysts with real-time guidance during the analysis process, provide insights from previous cases, and algorithmically identify similar attack techniques. Such an approach could relieve analysts from repetitive tasks, enabling them to focus on higher-level interpretation and strategic responses. The incorporation and adaptation of tools and methodologies from the cybersecurity sector will improve the degree of automation in different phases of the analysis process, such as detection systems, modelling and responding to disinformation campaigns.

Attribution

Attribution is a challenge. Some attackers cover their tracks well or engage in deniability. FIMI analysis requires an understanding of the different types of attackers in disinformation campaigns and their motivations. The European Union Agency for Cybersecurity (ENISA) report on *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape* uses a classification based on attribution (technical or political) and whether the actors are state-sponsored or non-state-sponsored. This creates four categories:

- State-sponsored, technically attributable
- State-sponsored, politically attributable
- Non-state-sponsored, technically attributable
- Non-state-sponsored, politically attributable.[19]

Russia, China and others use third-party firms to conduct their foreign influence campaigns, obfuscating the connections with the governments. They outsource to smaller threat actors, effectively engaging in a proxy war for their mutual benefit. Thus, studying the role of proxies in information warfare is needed.

Enhancing attribution in FIMI requires addressing resource constraints, improving technological tools and fostering collaboration among governments, academics, journalists and other stakeholders. While challenges persist in tracing the origins of disinformation and identifying the actors behind it, a more coordinated and strategic approach, coupled with increased expertise, will help strengthen the ability to attribute and respond to these threats.

Governments and tech companies must invest in artificial intelligence and machine learning solutions to better track disinformation sources, analyse patterns, and identify networks behind malicious campaigns alongside clear, transparent attribution methodologies that allow for the swift identification and exposure of perpetrators.

Dangers of FIMI

The term "useful idiots" refers to individuals who unwittingly support a cause or agenda—often political or ideological—without fully understanding its implications, particularly when that cause is manipulative or harmful. The phrase was used to describe Western sympathisers of Soviet communism during the Cold War. The term has evolved somewhat and is now used more broadly to describe people who, in their enthusiasm or naivety, support movements, organisations or regimes that ultimately manipulate or exploit them. It is often used pejoratively to describe people who are seen as naïve or gullible in the political arena.

[19] Magonara, Erika, and Apostolos Malatras, "Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape", Report/Study, ENISA, 8 December 2022. https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

Researchers have found that LLMs can be deployed in influence campaigns to write persuasive political messages with minimal human oversight.[20] They demonstrated that AI-generated text could craft arguments for and against political candidates, manipulate public opinion or sow discord during elections. This has the potential to make disinformation campaigns more efficient and harder to detect than traditional methods. One potential scenario includes generating large volumes of persuasive, pro-candidate texts or creating false narratives about opponents, all while evading fact-checkers due to the human-like quality of the AI's output. The ability of LLMs to generate infinite variations of the same misleading content poses a significant challenge for fact-checkers and detection tools.

These cases underscore the real-world dangers of AI-generated text in the context of politics and disinformation. The ability to create large volumes of persuasive, deceptive content cheaply and at scale poses significant challenges to the integrity of political discourse and democratic processes. The misuse of LLMs highlights the dual-edged nature of these technologies; while they can be used to combat disinformation and misinformation, they also enable the generation of highly persuasive narratives that can mislead the public.

As disinformation campaigns grow more sophisticated, they will destabilise political environments and undermine public trust, necessitating a long-term and comprehensive approach to counter these threats effectively.

Impact on democracy

In Europe, according to the 2024 Reuters Institute Digital News Report, online sources, including websites and social media, are increasingly becoming primary news sources for Europeans, especially among younger demographics.[21]

EEAS found in its first FIMI report that impersonation techniques have become more sophisticated. It noted that incidents do not occur in just one language; content is translated and amplified in multiple languages. It found that FIMI remains mostly image and video-based. The dissemination of the doctored image of Zelenskyy holding a jersey with the swastika is consistent with a broader, long-running disinformation campaign linking Ukrainian leaders to Nazism, a narrative deployed by pro-Russian actors since the illegal annexation of Crimea.

Although the European Parliament elections concluded on 9 June 2024 in all EU countries, the disinformation hasn't disappeared with their conclusion. There remains a growing threat to democratic society. Attackers have effectively employed information warfare techniques (such as content distortion and exploiting breaking news events) to amplify distrust within the EU, weaken transatlantic alliances and promote politicians sympathetic to the Kremlin. The incidents indicate a concerted effort not only to discredit the EU's actions but also to impact election outcomes by influencing voter sentiment through disinformation.

[20] https://openai.com/index/forecasting-misuse. See also Goldstein, J.A., Sastry, G., Musser, M., DiResta, R., Gentzel, M. and Sedova, K., "Generative language models and automated influence operations: Emerging threats and potential mitigations", 2023. arXiv preprint arXiv:2301.04246

[21] https://reutersinstitute.politics.ox.ac.uk/journalism-media-and-technology-trends-and-predictions-2024?eicker.media

Sometimes attackers exploit historical tensions, as the Chinese did regarding Japan's discharge of Fukushima water. Similarly, Turkey exploited the historical ethnic and national tensions between Greek and Turkish Cypriots to deepen polarisation.

These campaigns leveraged social media to disseminate fake narratives, manipulate public opinion and destabilise target countries. The use of sophisticated tactics, such as the creation of inauthentic accounts, hashtag manipulation and the dissemination of emotionally charged content, enables FIMI actors to exploit existing societal divisions and amplify pre-existing biases. The consequences of these campaigns can extend beyond the online sphere, contributing to increased polarisation, violence and the undermining of legitimate political processes.

Unlike non-democratic regimes, democratic nations' openness and freedom make them susceptible to malign influence tactics, a weakness on which adversaries have adeptly capitalised.

The European Commission is currently pushing forward with plans for a new directive, as part of the Defence of Democracy Package modelled after the US Foreign Agents Registration Act (FARA), specifically targeting Russian and Chinese influence and requiring foreign-funded entities to register, thereby increasing transparency.[22] This legislation aims to safeguard democracies by imposing transparency obligations on entities seeking to shape public opinion and influence democratic processes.[23] Through enhancing transparency and accountability, such measures seek to mitigate the risk of undue foreign influence on European political systems.[24]

Further sanctions should target individuals and entities involved in FIMI efforts, particularly focusing on those responsible for running disinformation networks like the Voice of Europe. EU-wide alignment on sanctions, including those targeting oligarchs like Viktor Medvedchuk, is obviously desirable.

Tracking how FIMI spreads

Russian disinformation is usually disseminated first on the network of sites affiliated with Russia, hosted on Russian domains and via the messages of Russian-related bloggers, politicians and influencers. Russian-related social media platforms such as Telegram, Vkontakte and Odnoklassniki exploit the echo chamber effect to deliver messages. Telegram remains the most accessed Russian-affiliated platform. The case study about Zelinskyy's moving to the US is an example of how the Russian propaganda machine amplifies the dissemination of a disinformation narrative. It started with an anonymous recording posted on a marginal YouTube channel. A group of websites pretending to be media outlets circulated the disinformation and gave it credibility. Russian state media reproduced the disinformation and gave it further outreach. A group of influencers and popular personalities talked about what the Russian state media or Kremlin-controlled pseudo-media published. These influencers managed to popularise the message on social media and reach Republican-leaning US citizens.

---

[22] Wheaton, Sarah, "EU Commission Wants Registry for Foreign Lobbyists", *POLITICO*, 12 Dec 2023. https://www.politico.eu/article/eu-commission-wants-registry-for-foreign-lobbyists/

[23] European Commission, "Defence of Democracy – Commission proposes to shed light on covert foreign influence", press release, 12 Dec 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453

[24] Wheaton, op. cit.

Knowledge of the tactics and techniques used by attackers can serve as a basis for designing pre-bunking actions aimed at the public to explain how these disinformation agents operate. Pre-bunking can help citizens detect disinformation traits, become more alert and thus reduce the effect of disinformation campaigns.

Governments and fact-checkers need to monitor the propaganda agents used to sustain and popularise similar disinformation narratives and to study how they relate to each other. Also useful would be an up-to-date catalogue of websites that mimic media outlets commonly used to plant disinformation that is then amplified by other actors, including the Russian state media. When disinformative content is detected on these websites, speed is of the essence to mitigate the amplification process. The intervention of fact-checkers is necessary to debunk the falsehoods and provide evidence to prove lies are just that: lies. It is useful to conduct more research on how actors interact with each other when disseminating a disinformation narrative. Finding patterns of action can help anticipate the next steps state propaganda machines will take when they launch a disinformation campaign.

The EEAS should prioritise investment in multilingual tracking tools capable of detecting disinformation across different languages. This would allow for faster identification of manipulative content in different linguistic and regional contexts.

Others try to profit from a FIMI attack

Various threat actors, including state-sponsored groups, criminal organisations, hacktivists and individuals with malicious intent, sometimes work together without any agreements. They share the same objective, so they all work to achieve it, bringing to bear their particular specialities in FIMI.

Some cases (such as PAPERWALL) show that FIMI campaigns can serve both financial and political interests. The PAPERWALL findings confirmed "the increasingly important role private firms play in the realm of digital influence operations and the propensity of the Chinese government to make use of them".[25] Similarly, we saw in the case study (sec. 4.29) about Turkish-controlled Northern Cyprus that real-estate websites engaged with the narrative, aiming to influence perceptions of stability and investment potential in the TRNC. Their involvement underscores the intersection of political narratives with financial interests. The TRNC-based real estate agencies may have engaged in the same misinformation campaigns without being centrally orchestrated. They shared the same interests in pushing for international recognition of the separatist territory.

A similar phenomenon appears in the Saudi case study (see sec. 4.29). State-sponsored groups used governmental resources to advance geopolitical objectives, while criminal organisations exploited the situation for financial gain.[26] Ideologically motivated hacktivists and individuals with unclear motives also engaged in the attack.[27] This incident highlighted a disturbing trend

[25] Fittarelli, Alberto, "PAPERWALL Chinese Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content", *The Citizen Lab*, 7 Feb 2024. https://citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/

[26] Uddin, R., "Russia, Iran and Saudi Arabia Worst Countries for State-Sponsored Twitter Disinformation", *Middle East Eye*, 2022. https://www.middleeasteye.net/news/twitter-disinformation-state-sponsored-russia-iran-saudi-arabia-worst

[27] Abeshouse, B., "Inside the Wild West of Social Media", *b*, 8 February 2018.

in which ordinary individuals, in this case, Saudi citizens and right-wing Americans, played a role in spreading distorted narratives.[28]

Measuring FIMI's impact

The impact of a FIMI campaign is uncertain. One way of measuring impact is by the number of impressions that social media posts get. However, the difficulty in measuring effectiveness is trying to disentangle what is local and what is amplified by interference. Russian disinformation efforts, particularly focusing on social media as a significant battlefield for information warfare, have been subject to extensive analyses by most Western countries' cybersecurity firms, intelligence agencies and academic research. However, the effectiveness of these campaigns and the impact of Western countermeasures remain subjects of ongoing analysis and debate. A comprehensive understanding of the impact of FIMI and any resulting changes in people's behaviour or actions is worth pursuit.

The EU and Member States should assess the vulnerability of states to exploitation in the information space and to implement proactive plans to counteract various forms of disinformation. This approach differs from pre-bunking by allowing governments to prepare defensively for potential adversarial responses, particularly in contexts such as negotiations for military alliances. This preparation could be complemented by analysing the audience consuming such disinformation. Given the association with military alliances and national security, governments should consider how best to develop counternarratives that mitigate the risk of online harmful content designed to provoke emotional responses. Ensuring that harmful online content does not escalate into offline protests, riots or terrorism is vital.

Countermeasures that worked

Among the best defences against disinformation is transparency, effective communication and the use of counter-narratives that challenge disinformation targeting the European Union. Providing EU citizens with discursive elements so that they can evaluate different situations linked to disinformation implies being self-critical and taking seriously the relationship of trust between the European institutions and the societies of the different Member States. If trust deteriorates, victims of disinformation may not believe the content of a given FIMI incident, but they may also distrust the EU counter-narratives.

Pre-bunking will help citizens detect disinformation actions, become alert and thus reduce the effect of disinformation campaigns.

The case studies show the involvement of a wide range of FIMI actors, including state-owned media, private companies and opportunistic groups, showing the need for a **whole-of-society approach** to countering FIMI. EU DisinfoLab concludes that this whole-of-society approach "can be realistically achieved only if the large variety of actors engaged in countering FIMI speak a common language. Initiatives such as the DISARM and STIX frameworks constitute

https://www.aljazeera.com/features/2018/2/8/troll-factories-bots-and-fake-news-inside-the-wild-west-of-social-media

[28] Byman, Daniel L., "How Middle Eastern conflicts are playing out on social media", Brookings Institute, 2022. https://www.brookings.edu/articles/how-middle-eastern-conflicts-are-playing-out-on-social-media/

that common language, set up to normalise the monitoring, analysis, assessment, and response to FIMI operations."[29]

Speed is of the essence in case after case. In the case study of the doctored photograph of Zelenskyy (sec. 4.3), the rapid decline in the circulation of observables after the initial spike suggests that de-bunking efforts played a critical role in mitigating the impact of the disinformation. The Russian FIMI attack in Germany quickly collapsed the moment that it became clear that Lisa made up the story about the rape to cover up her bad grades in school (sec. 4.9). Quick and transparent communication in events like this play a key role in preventing and combatting FIMI.

Preventive surveillance measures, such as those employed by the French army to debunk the attack in Mali (sec. 4.13), can also be crucial. Open-source intelligence (OSINT) is of special importance to dismantle the TTPs that are behind FIMI attacks. Detecting bots and fake accounts or verifying the concordance between the publication times of several tweets that refer to the same event are some of the strategies that can help counter a FIMI attack.

Spain's defence against Russia's FIMI operation (sec. 4.12) to influence the national elections was strengthened by some EU initiatives like the Rapid Alert System[30] and the smooth intervention of fact-checkers and media, which effectively decreased the potential influence of the operation. This case also underscores the ongoing need for coordinated efforts to protect democratic integrity from evolving foreign interference tactics.

The EU has developed several frameworks to combat disinformation, including the EU Cybersecurity Strategy[31] and initiatives through the European Centre of Excellence for Countering Hybrid Threats.[32] These bodies help coordinate responses to foreign interference across EU institutions and Member States, building resilience against cyberattacks and disinformation campaigns targeting elections.[33]

The EU established the East StratCom Task Force[34], part of the European External Action Service (EEAS), to identify and expose pro-Russian disinformation targeting EU Member States.

The European Parliament has agreed a regulation harmonising political advertising requirements and banning foreign sponsorship of political ads before elections. The regulation includes provisions for clear labelling of political ads, improved access to financing information and the establishment of a public repository for online political ads and related data.[35]

---

[29] Hénin, EU DisinfoLab, op. cit., p. 11.
[30] https://www.eeas.europa.eu/eeas/factsheet-rapid-alert-system_en
[31] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[32] https://www.hybridcoe.fi/
[33] Koudelka, Michal, and Petr Fiala, "Czechs Bust Russian Network Paying off European Politicians", Radio Prague International, 28 Mar 2024. https://english.radio.cz/czechs-bust-russian-network-paying-european-politicians-8812632
[34] https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication-division-and-its-task-forces_und_en?s=2803
[35] European Parliament, "European Parliament legislative resolution of 27 February 2024 on the proposal for a regulation of the European Parliament and of the Council on the transparency and targeting of political advertising". https://www.europarl.europa.eu/doceo/document/TA-9-2024-0090_EN.html

Tighter regulations for digital influence

The European Commission is currently pushing forward with plans for a new directive, as part of the Defence of Democracy Package[36] modelled after the US Foreign Agents Registration Act (FARA), requiring foreign-funded entities to register and specifically targeting Russian and Chinese influence. This legislation aims to safeguard democracies by imposing transparency obligations on entities seeking to shape public opinion and influence democratic processes. Through enhancing transparency and accountability, such measures seek to mitigate the risk of undue foreign influence on European political systems. Moreover, swift enforcement of regulations on political advertising will help to curb foreign interference. Further sanctions should target individuals and entities involved in Russian FIMI efforts, particularly focusing on those responsible for running disinformation networks like Viktor Medvedchuk and the Voice of Europe.

The Russian "Doppelganger" operation showed how the abuse of the domain registration system or the European web infrastructure and software can be exploited by hostile actors for the purpose of foreign interference. The EU should strengthen the verification and legitimacy of EU-registered online domains and companies. It should implement stricter regulations in the domain name industry to protect legitimate entities from being impersonated. It should implement stringent measures for fact-checking content and identifying potential sources of disinformation early. It should ensure appropriate measures so that EU-registered software and infrastructure are not exploited for malicious covert influence operations without facing consequences.

Existing laws, such as the Digital Services Act (DSA) and General Data Protection Regulation (GDPR), should be enforced to their full extent to safeguard citizens. Access to platform data to European researchers (including non-academics from civil society organisations) working for the public interest under Article 40 of the DSA needs to be greatly improved.[37]

We need better transparency with respect to the supported content published in social media. Social media influencers should make it clear when they receive money for their posts. Sponsors should be registered with the social media to know who sponsors what kind of content. This will make it clear when foreign actors (or their proxies) sponsor the distribution of specific content in social media. Better regulation of these sponsors should help with transparency. Attempts to bypass the regulation should have legal consequences. Regulatory bodies and legal authorities must take proactive steps to pursue legal actions and enforce measures against entities spreading false narratives.

Ethical and privacy concerns around the collection and use of social media data remain insufficiently addressed. The absence of clear ethical guidelines can lead to privacy violations, undermining public trust. Robust ethical protocols that align with legal standards like the GDPR must be developed to guide FIMI analysis practices.

International cooperation

Effective countermeasures against disinformation campaigns require a multi-faceted approach, involving cooperation between governments, private sector entities (especially social media

[36] https://civic-forum.eu/our-work/defence-of-democracy

[37] Art. 40 concerns providing "access to data to vetted researchers… for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union".

platforms), civil society and the public. Given the rise of state-sponsored disinformation campaigns, particularly from authoritarian countries such as Russia, China and Iran, international collaboration is essential. Governments need to work together to develop coordinated strategies to identify, counter and mitigate the impact of these foreign threats, especially regarding political narratives and international relations. In addition, the interdisciplinary nature of FIMI requires a cross-sectoral collaboration with experts across government, industry, media and academia which will in turn encourage collaboration between fields such as political science, social data analysis, security studies and artificial intelligence. This cross-sectoral and international collaboration should support cross-disciplinary training and joint research initiatives to ensure a holistic understanding of FIMI and the development of interdisciplinary, collaborative data-sharing platforms and tools that could also support knowledge exchange, enabling better integration of technological, societal and geopolitical insights into the study and response to FIMI. These tools should be accessible and available to the public to identify and flag disinformation, including deepfakes and other manipulated content, helping to reduce confusion in the information space.

Governments should establish rapid-response teams trained to debunk FIMI as soon as it emerges. This can be supported by partnerships with fact-checking organisations, as exemplified by initiatives like #UkraineFacts. Strengthening international cooperation to facilitate swift information sharing across borders will help stem the flood of disinformation. Also vital is promoting global partnerships to share best practices on countering FIMI. The DISARM Framework is a good example. The use of international fact-checking databases should be encouraged to ensure swift identification of disinformation across different linguistic and cultural contexts.

European countries should deepen their cooperation in intelligence-sharing mechanisms to swiftly detect and disrupt foreign interference efforts, particularly ahead of elections. They should enhance cooperation with international bodies and third countries to prevent the relocation of disinformation operations to jurisdictions outside the EU's control. This includes coordinating sanctions and other measures to disrupt financial and logistical support for these campaigns.

Governments should strengthen international legal frameworks for prosecuting transnational disinformation campaigns. Enhanced cooperation between nations and the private sector, especially tech companies, is vital to detect, prevent and penalise attackers.

Gaps in current analysis practices

Analysts face challenges in collaborating effectively due to limited tools for participatory and real-time analysis. Improved collaboration platforms are needed to support the sharing of insights, coordinating efforts on complex cases and ensuring agility in response. Furthermore, inconsistent methodologies and lack of training may result in variability in analysis quality. To address this, standardised methodologies and frameworks are needed to ensure consistency, along with enhanced training programs.

The absence of version control in analysis workflows makes it difficult to document and manage the evolution of a case or incorporate differing viewpoints. Proper versioning systems are necessary to ensure that analyses are consistently reviewed, updated and accurately documented, which will facilitate collaboration and allow for comprehensive tracking of analytical progress.

There is no standardised approach to categorising or recording data, resulting in isolated analysis efforts that prevent cross-comparison of incidents. This hinders the ability to derive broader insights, especially for long-term campaigns. Establishing unified data formats and taxonomies, like DISARM, is essential for comparative analysis and to uncover trends across FIMI incidents.

Diverse tools and platforms currently in use do not communicate effectively, creating barriers to data sharing and comprehensive analysis. Improved interoperability through standardised APIs or data formats will enable seamless integration between systems, leading to more robust, integrative analyses.

Sharing knowledge

EU-funded projects such as ATHENA form clusters with other similar projects to exchange knowledge and leverage impact, but much more could be done to foster a network of projects focused on disinformation in Europe and beyond, in the US, Canada and elsewhere. Good practice should be shared globally to tackle the scourge of disinformation and FIMI.

Collaborating with organisations to expose disinformation enhances the public's understanding of the authenticity and credibility of the information to which they are exposed. By collaborating with fact-checking organisations, and promoting verified information through official channels, stakeholders can identify false narratives as part of a FIMI campaign.

National governments should strengthen monitoring mechanisms, improve transparency and work more closely with fact-checking organisations to mitigate the impact of FIMI. Fostering collaboration between researchers, governments and AI specialists is crucial. Researchers can provide valuable insights into the evolving tactics of disinformation campaigns and the psychological mechanisms that make them effective. Governments can leverage these insights to inform policy and support the development of countermeasures. AI researchers can contribute by developing advanced detection tools and creating innovative solutions for identifying and mitigating the spread of disinformation. By combining their expertise, these stakeholders can create a more comprehensive and effective approach to combating FIMI and safeguarding democratic processes.

A significant deficiency exists in how knowledge and insights are stored and shared. Valuable insights from past analyses are often inaccessible, leading to repeated efforts and missed opportunities to leverage prior work. The need for centralised, easily accessible knowledge repositories – ideally shared among different analysis teams – would allow analysts to search and retrieve data from previous cases efficiently.

To counter future FIMI attacks, stakeholders should invest in and enhance OSINT capabilities, particularly in detecting automated accounts and fake profiles. Analysing and tracing digital footprints, such as fake accounts and bots, OSINT becomes indispensable in countering these threats. Additionally, a coordinated effort between physical surveillance and digital intelligence gathering is essential to not only disrupt the tactics but also to prevent future dissemination of false information. Increased training in these areas for both military and civilian personnel involved in defence against FIMI attacks can further bolster these efforts.

Cybercriminals and governments are creative in their attack strategies, which strengthens the need for the DISARM Framework so that defenders and researchers can identify and compare the tactics and techniques used in disinformation campaigns. Understanding the attack strategies of different players will help in attribution. The development and adoption of comprehensive frameworks such as DISARM should be pursued to standardise the monitoring, analysis, assessment and response to foreign influence. The DISARM Framework should be updated to include tools for measuring the time needed to react to FIMI activities, predict the political consequences of disinformation campaigns and categorise threat actors. State-owned media networks and political influencers should be classified as separate communication tools in the Framework

Media literacy and public awareness

The Eurobarometer published in December 2023[38] showed that the main concerns for EU citizens in the context of the elections in Europe were related to people basing their voting decision on disinformation (78%), followed by elections being manipulated through cyberattacks (72%), foreign countries influencing elections covertly (70%) and people being pressured into voting in a particular way (65%).[39]

Fortifying democratic practices necessitates an increase in the public's media literacy through well-funded educational campaigns. EU Member States should promote image and video fact-checking skills to help individuals identify manipulated content and other forms of digital deception. This will help build long-term resilience to disinformation. The widespread use of reverse image search tools[40] to trace the origin of false content has proven valuable and should be widely promoted as a best practice. Disinformation campaigns are becoming more visually persuasive, making it imperative for policymakers to develop media literacy programs that equip the public with tools to critically assess both textual and visual information.

Educating users about disinformation tactics can help them act as a first line of defence, significantly reducing the spread and impact of false information. Promoting media literacy, especially in the verification of images and videos, will help the public to recognise and question the authenticity of the information they encounter. Children as well as adults will benefit from an education that helps them to critically analyse and question information. Governments and/or civil society organisations (CSOs) should launch campaigns to educate the public on how to critically assess news sources and check for the credibility of information and to critically evaluate the credibility and motives behind information sources. Moderated public forums, debates and media outlets that purposefully present balanced perspectives on contentious issues could foster critical thinking and decision-making.

[38] https://www.europarl.europa.eu/at-your-service/en/be-heard/eurobarometer/plenary-insights-december-2023
[39] European Commission, "Defence of Democracy – Commission Proposes to Shed Light on Covert Foreign Influence", press release, 12 December 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453.
[40] Reverse image search tools are used to verify the authenticity and origin of images. These tools allow users to upload or link to an image and find where it has appeared online, helping to identify whether the image has been reused, manipulated or misrepresented. For example, they can reveal if a photo claiming to show a current event was actually taken in a different location or time. Common tools include Google Reverse Image Search, TinEye and Yandex Image Search

Individuals should be encouraged to seek alternative sources and question information in public campaigns. Educational initiatives should enhance the ability to discern manipulative content and empower the public to identify credible sources. These programs should work in partnership with credible media organisations to provide accurate information and develop strategies for identifying and countering disinformation.

Informing the public about expected FIMI attacks is part of raising public awareness. This has been happening more often since the Russian invasion of Ukraine and especially in advance of the US elections in November 2024.[41] This is a welcome form of pre-bunking, advising the public in advance about an expected attack.

Given the growing complexity of FIMI and the increased reliance of social media and AI, there is a need to improve technological and digital literacy across all sectors and amongst the citizens. These efforts should focus on media literacy, helping citizens recognise and critically assess content, recognise manipulated information and understand the role of AI and algorithms in shaping the information landscape, especially in the context of political and international conflicts. Citizens should critically evaluate digital content and enhance their participation in mitigating the negative impact of manipulated information on democratic discourse.

Governments should establish partnerships with reputable media organisations to amplify accurate information. Government agencies, media regulatory bodies and educational institutions should provide journalists with comprehensive training to identify and effectively report misinformation. Collaboration with international journalism associations and experienced media professionals will ensure the training is robust, practical and aligned with global best practices.

Public awareness campaigns and social cohesion campaigns are needed to build a robust and trustworthy social fiber amongst people. It is crucial to promote media literacy programs that help people recognise false narratives and misinformation, especially on social platforms along with community-building initiatives for bridging political and social divides, fostering trust and collaboration among diverse groups. Efforts to strengthen social cohesion should focus on building shared identities and encouraging open dialogue to counter polarisation and there should be a long-term strategy focusing on enhancing social unity, resilience and a healthy public discourse.

Combatting FIMI requires a comprehensive strategy. Governments and international organisations must work together to share insights and formulate tactics against disinformation. Strengthening independent journalism and fact-checking efforts is vital to countering false narratives. Supporting civil society organisations that advocate for media literacy is critical. Ultimately, it is essential to educate individuals on how to critically evaluate online information and differentiate trustworthy sources from propaganda.

[41] "In recent weeks, the intelligence agencies have dramatically stepped up their alerts. Two weeks ago, they warned of post-election violence. Over the last 10 days, they have now issued three warnings about Russian attempts to undermine faith in the election. And Jen Easterly, the director of the Cybersecurity and Infrastructure Security Agency, said her organization would give regular updates Tuesday to inform the public of threats to the election." Barnes, Julian E., and Steven Lee Myers, "Russian and Other Groups May Try to Undermine U.S. Elections After Vote", *The New York Times*, 4 Nov 2024.
https://www.nytimes.com/2024/11/04/us/politics/election-threats-russia.html

Promoting transparent and inclusive political dialogue within countries is also crucial to address the root causes of social unrest and reduce vulnerability to external manipulation. By addressing the underlying causes of social unrest, promoting media literacy and holding perpetrators accountable, countries can strengthen their resilience against foreign information manipulation and interference to safeguard their democratic processes.