ENC ANALYSIS

ENC
ENCouncil.org
European Neighbourhood Council

Words and Wires: Understanding Foreign Information Manipulation and Interference (FIMI) and Why It Matters for the EU and Türkiye

November 2025

Author
Asuman Kubra Bas

Table of Contents

About the author

Asuman Kubra Bas is Head of Projects and Research at the European Neighbourhood Council. She oversees a number of active EU projects, as well as a group of researchers and coordinators, and she is responsible for key areas of planning, project implementation, research, and management. She holds a Master's degree in International Relations and a Bachelor's degree in Sociology. Her areas of expertise span EU foreign policy, business and human rights, youth, disinformation, and migration. She has contributed to numerous research studies, including co-authoring a chapter in Mediatized Discourses on Europeanization and Their Representations in Public Perceptions, published by Aranzadi (Thomson Reuters Spain).

Summary

This paper examines Foreign Information Manipulation and Interference (FIMI) as a growing hybrid challenge with implications for the European Union and its partners, including Türkiye. Drawing on the EEAS FIMI Threat Reports, open-source investigations, and new data on coordinated online behaviour, it discusses how such incidents unfold across Europe, the tactics through which they are carried out, and their broader significance for the EU and Türkiye. The paper concludes with recommendations for strengthening resilience through early coordination, behavioural monitoring, and cross-border cooperation within the emerging European Democracy Shield framework.

Introduction

As the global order is reshaped by geopolitical conflict, trade tensions, rising populism, and digital warfare, the European Union and Türkiye face renewed pressure to define their strategic roles and to safeguard their relationship amid emerging threats such as Foreign Information Manipulation and Interference (FIMI).

This evolving geopolitical landscape, marked by the erosion of transatlantic relations in the wake of the Trump 2.0 administration and a major war on Europe's borders, demands careful recalibration from both actors. In navigating this uncertainty, the EU and Türkiye, like many other states and regional actors, are becoming increasingly vulnerable to hybrid threats, including coordinated information manipulation campaigns and cyber-enabled influence operations.

Amid this turbulence, geography has once again become an important element in shaping international relations. The European Union and Türkiye stand out as natural partners, tied not only by proximity and history but also by intertwined economies, supply chains, energy corridors and regional connectivity. However, in an era defined by strategic competition and economic fragmentation, certain external actors may seek to obstruct closer EU–Türkiye alignment. They do so by exploiting existing divisions, amplifying societal and political tensions, and undermining trust through tactics such as FIMI and other hybrid threats. For Türkiye and the EU, these dynamics carry particular weight. Both operate in overlapping geopolitical spaces from the Black Sea to the Eastern Mediterranean where FIMI operations exploit regional crises, migration narratives, and defence debates to weaken cooperation and distort mutual perceptions.

As power competition increasingly unfolds online, the information space has turned into a domain where actors exert influence to advance their strategic goals. In this context, understanding how information is manipulated is no longer a peripheral concern but a strategic necessity. Yet, despite its growing relevance, the literature on FIMI in relation to the EU and Türkiye remains in its early stages. This paper approaches FIMI as a shared challenge for both actors. It begins by outlining the concept of FIMI, drawing on recent reports from the European External Action Service (EEAS) and emerging research. It then explores its implications for the EU and Türkiye and concludes with recommendations for strengthening resilience against these evolving threats.

What's FIMI?

Foreign Information Manipulation and Interference (FIMI) refers to deliberate and coordinated activities by foreign actors intended to distort the information

environment in target countries. These efforts go beyond simply spreading false or misleading content; they often involve selective framing, emotional manipulation, and the amplification of polarizing narratives aimed at eroding trust, fragmenting societies, and shaping political outcomes (EEAS, 2023).

Unlike traditional notions of disinformation or hybrid threats, FIMI is defined by its strategic intent and its reliance on deceptive, coordinated behavior. According to the European External Action Service (EEAS), what sets FIMI apart is not merely the content itself, but the methods through which it is disseminated. Because much of this content is not verifiably false, it is often difficult to detect through conventional fact-checking or moderation strategies (EEAS, 2025).

Recent investigations have illustrated how FIMI operates in practice. Across Europe, coordinated campaigns such as *Portal Kombat*, *Doppelgänger*, *CopyCop*, *Spamouflage*, *Ghostwriter* *and others* have been uncovered by institutions including France's VIGINUM, the European External Action Service (EEAS), and independent digital-forensics networks. These operations form part of a broader strategy to distort information environments, amplify social divisions, and undermine democratic trust.

In response to this challenge, the EU and its partners (including NATO StratCom and the Hybrid CoE) have adopted a behavior-first methodology, exemplified by the DISARM framework[1] (Hybrid CoE, 2022; EEAS, 2023). Rather than focusing solely on the content, this approach analyzes behavioral patterns such as cross-platform coordination, deceptive identity use, intent to manipulate, and inauthentic amplification.

The shift is increasingly urgent, driven both by the volatile geopolitical context outlined above and by the emergence of new technologies. FIMI actors have begun to incorporate generative AI tools into their campaigns. As noted in the 3rd EEAS Threat Report, "The use of AI by hostile actors increases the sophistication and scale of operations. This necessitates proactive behavioral detection systems, not merely reactive content moderation" (EEAS, 2025). Independent research supports this concern. A recent investigation by the Digital Forensic Research Lab (DFRLab) shows that synthetic imagery and deepfakes produced with AI are reducing the cost of influence operations while increasing their speed and credibility (DFRLab, 2025). The convergence of emerging technologies with an already unstable geopolitical environment underscores the need to move beyond reactive moderation and toward strategic, behavior-based detection frameworks.

[1] DISARM (Disinformation Analysis and Risk Management) is an open-source framework designed to describe and understand the behavioural aspects of FIMI and disinformation. It sets out best practices for countering manipulation through data and analysis sharing and supports more effective, coordinated action (EEAS, 2023).

FIMI campaigns are not random or opportunistic. They are structured around specific strategic aims. The EEAS categorizes these goals using the 5D framework: Dismiss, Distort, Distract, Dismay, and Divide. Some operations aim to discredit critical voices, while others try to reframe reality, redirect attention, intimidate opposition, or sow division within societies. Recognizing these intent-driven patterns is essential for building effective responses. It's not just about identifying *how* manipulation happens, but *why* and what its ultimate effects are on democratic societies and international partnerships.

FIMI in Action

To understand how FIMI work in practice, it's important to know the tactics and tools foreign actors use. FIMI actors employ a range of Tactics, Techniques, and Procedures (TTPs) that have become increasingly diverse and sophisticated. According to the first EEAS FIMI Threat Report, image-based and video-based content were among the most common techniques in 2022, often taking the form of misleading visuals, decontextualized footage, or emotionally charged memes (EEAS, 2023). However, these are just a subset of the broader TTP landscape, which also includes impersonation of trusted sources, emotional framing, cross-platform narrative repetition, and the coordinated use of fake accounts.

The EEAS alone recorded 100 FIMI incidents in 2022, 750 in 2023, and 505 in 2024. Its latest FIMI Threat Report identified 90 countries targeted in the 2024 sample. Ukraine remained the primary target of Russian-linked FIMI activity, accounting for 257 of the recorded incidents (nearly half of all analysed cases). Other major targets included France and Germany, with the latter's coalition government facing repeated manipulation efforts.

The report also highlights that elections and other high-salience events are particularly vulnerable to FIMI operations. From the European Parliament vote to Georgian Parliamentary elections and other states in the EU's neighbourhood, these events frequently attract foreign interference designed to undermine trust in democratic processes or promote alignment with the perpetrating actor's geopolitical interests. The years 2024 and 2025 have brought increased attention to this issue, as multiple states documented interference attempts linked to major electoral and policy developments.

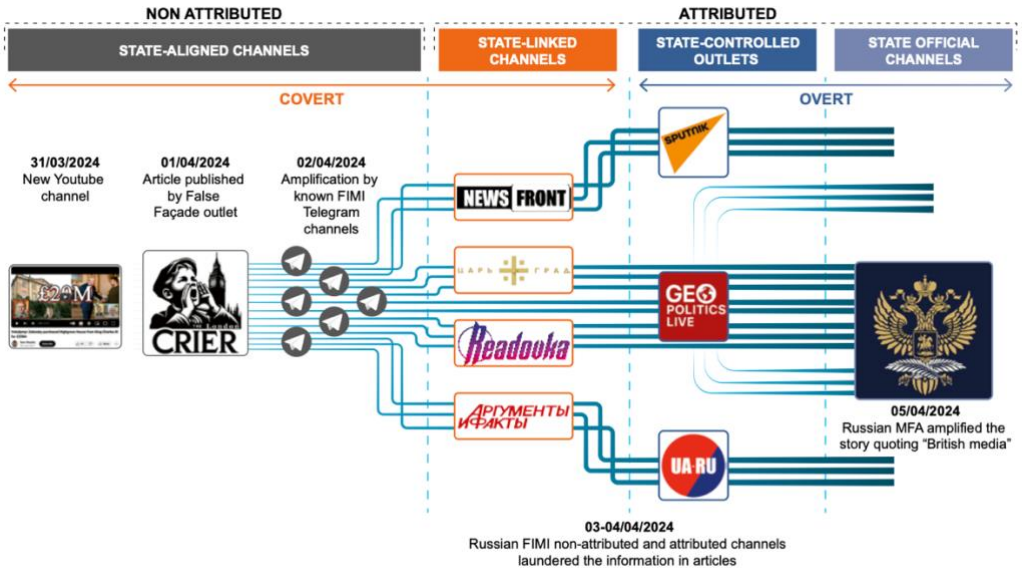
Beyond these aggregated findings, member states have also uncovered major FIMI campaigns. France's VIGINUM, established in 2021 to monitor foreign digital interference, exposed the Portal Kombat network in 2024. The investigation revealed at least 193 interlinked websites spreading pro-Kremlin narratives across Europe. Similar large-scale operations have been identified elsewhere. The Doppelgänger campaign cloned the websites of at least 17 authentic media outlets

including Bild, 20 Minutes and The Guardian to publish fabricated articles and videos that amplified pro-Kremlin narratives across Europe (EU DisinfoLab, 2022). Likewise, the Ghostwriter operation targeted NATO member states and countries in the EU's eastern neighbourhood through a combination of cyberattacks and information manipulation. By impersonating officials and spreading false narratives about alliance activities, it sought to undermine confidence in NATO and regional security (Cardiff University, 2023).

Beyond the EU, FIMI operations have also intensified in the Union's wider neighbourhood. For example, in Moldova's lead-up to the September 2025 parliamentary elections, analysts identified a multi-faceted threat environment: illicit funding, disinformation, large-scale bot and social-media campaigns, and cyber-enabled influence operations all featured prominently (DFRLab, 2025).

To illustrate how these campaigns function in practice, the EEAS visualised the transmission of a FIMI incident, using some of the tactics outlined above (see figure below). The example traces how a false claim, initially seeded through an unattributed YouTube channel, can move through covert "False Façade" outlets, state-aligned Telegram channels, and semi-official media before reaching official diplomatic accounts. This sequence captures the layered amplification process typical of FIMI where content gains credibility as it circulates through progressively more authoritative sources (EEAS, 2025).

Figure 1. Transmission of a FIMI incident



As the figure shows, FIMI tactics often combine several methods outlined above, including the use of fabricated or decontextualized media, impersonation, and cross-platform coordination. These interconnected stages make such operations

difficult to detect early and demonstrate why continuous monitoring and cooperation across institutions are necessary to mitigate their impact.

There are many other ways in which FIMI spreads. In some instances, manipulation does not start with fabricated media but through the gradual infiltration of online communities, where false narratives are introduced slowly to appear authentic. Other operations depend on coordinated botnets (bot networks) that inflate engagement and make marginal content seem widely accepted. FIMI actors also deploy clone websites that mirror trusted news outlets, as seen in the Doppelgänger campaign, and rely on cross-platform dissemination, circulating the same story across Telegram, X (Twitter), Facebook, and local-language news sites to reach different audiences simultaneously.

Why FIMI matters for the EU and Türkiye

Within the current geopolitical context, Türkiye stands out as a key defence partner, a NATO ally, an EU candidate country, and the central bridge of the Middle Corridor connecting the Caucasus and Central Asia to Europe. Both actors play pivotal roles in conflict-prone regions such as Eastern Europe, the Middle East, and the Eastern Mediterranean, where narratives can directly influence security outcomes. An open and trusted information space is therefore essential for fostering mutual confidence, and sustaining a long-term partnership on issues central to their shared interests. Despite many challenges, the EU and Türkiye have overlapping strategic priorities in areas such as NATO cooperation, the Customs Union, connectivity, energy security, supply chains, and engagement with the Caucasus and Central Asia.

Based on the EEAS's analytical framework, a recent research conducted by ENC examined posts on platform X (formerly Twitter) from 2022 to 2024 using both content and behavioral methodologies with a focus on three actors (Russia, China and Iran) that were previously involved in the FIMI operations according to the EEAS reports. The study focused on five major foreign policy and domestic events: the Black Sea Grain Initiative, Finland and Sweden's NATO accession, the 2023 twin earthquakes in Türkiye, the 2023–2024 Turkish elections, and key developments in the Middle East. Among the downloaded two million X items, including original posts, retweets, and replies related to the selected events, a final sample of 218,000 tweets were examined.

The findings indicate that foreign actors are active within Türkiye's information space. Among these, Russia emerges as the most prominent and persistent actor, maintaining visibility across multiple topics and adapting its narratives to local contexts in ways that resonate with Turkish audiences. Russian networks engage consistently and strategically, aligning their messaging with ongoing political,

economic, and regional discussions, which allows them to remain embedded in Türkiye's digital environment over time. This pattern is further supported by recent research on the Russia–Ukraine war, which demonstrates how false or misleading posts circulating on Turkish social media often reproduce pro-Russian perspectives and contribute to deepening societal polarization (Ulusan & Ozejder, 2024). In contrast, Chinese and Iranian operations are more selective. China displays a different pattern, adopting a more soft power–driven approach that prioritizes image-building and the projection of benevolence rather than direct political messaging.

For the selected events, actors did not seek to dominate conversations directly. Instead, they introduced narratives that resonated locally and were later amplified. Other studies also support this finding, showing that Russian outlets such as Sputnik Türkiye adapt narratives to local audiences, amplifying anti-Western sentiments and exploiting ideological divisions (Olszowska & Wasilewski, 2024). These operations relied on limited automation/botnets but achieved significant organic visibility through existing social and media networks.

For certain events and narratives, a convergence between foreign actors was observed. Other research has also identified similar patterns of alignment between Russia and China, highlighting how both actors increasingly coordinate or mirror each other's messaging in global information manipulation efforts (CEPA, 2024). This may indicate deliberate coordination in messaging among these countries or reflect Turkish users' receptiveness to multiple external narratives, given the diverse nature of Turkish society. More likely, it is a combination of both factors. In either case, this trend has important implications, as it suggests that third-party actors could increasingly coordinate their information manipulation efforts when their strategic interests align.

Conclusion and Recommendations

FIMI operations often target not only national information spaces but also the trust and cooperation between partner countries. For the European Union and Türkiye, both of which operate in overlapping geopolitical spheres, addressing this challenge is both a strategic and a practical necessity.

Member states have begun establishing dedicated institutions such as VIGINUM, while new research and monitoring networks are emerging across Europe. The recent launch of the European Democracy Shield (EDS) by the European Commission in November 2025 marks an important step in institutionalizing the EU's response to Foreign Information Manipulation and Interference. The initiative establishes a European Centre for Democratic Resilience, expands the European Digital Media Observatory and the European Network of Fact-Checkers, and

introduces an "incidents and crisis protocol" under the Digital Services Act to coordinate rapid responses to manipulation campaigns (European Commission, 2025). Importantly, it extends the EU's resilience framework beyond its borders, emphasizing cooperation with neighbouring and candidate countries. For the EU's partners, including Türkiye, this creates a timely opening to work on the topic together.

Building on this momentum, the following recommendations outline concrete steps for the EU and its partners to enhance resilience and cooperation against FIMI.

Recognize that FIMI is counterable and collaborate early: FIMI operations are not invincible. Evidence from recent cases, including the recent Moldovan elections, shows that coordinated responses, transparent communication, and rapid fact-checking can significantly reduce their impact. When democratic actors cooperate internally and externally, these operations lose much of their effectiveness. Early collaboration between partners in awareness-raising, FIMI monitoring, and public communication can help prevent their relations from becoming a target of manipulation and strengthen their ability to respond collectively when such operations occur.

Focus on tactics and behaviour without overlooking narratives: A behavioural methodology should not imply that narratives and their impact are overlooked. While detecting coordinated behaviour remains essential, FIMI research should increasingly integrate analytical components that examine how narratives evolve, resonate, and influence audiences. Understanding the behavioural patterns of manipulation is critical, but so is assessing the substance and emotional appeal of the narratives themselves.

Build understanding through a whole-of-society approach: Building resilience must begin with awareness, dialogue, and education. From citizens to scholars, a broad understanding of how FIMI functions is essential to developing informed responses. This requires integrating the topic into academic and policy debates, encouraging research that produces shared definitions, context-specific methodologies, and actionable insights. Incorporating FIMI-related topics into academic curricula, media literacy programs, and civil service training could promote a shared conceptual foundation. Encouraging interdisciplinary research between communication studies, political science, and data science can also produce tailored analytical frameworks and detection methodologies.

Strengthen and connect networks: Many European and national mechanisms countering information manipulation are still relatively young. Existing coordination structures within the EU are advancing, but similar cooperation with neighbouring regions, including Türkiye, remains limited. Building stronger

connections between institutions, researchers, and civil society across the EU–Türkiye framework can enhance the overall effectiveness of defensive efforts.

In the end, addressing FIMI is not just a matter of information integrity; it is an investment in democratic resilience. As manipulation tactics continue to evolve, building detection systems and fostering cooperation across borders will be essential. By treating information integrity as a shared responsibility, the EU and its partners can strengthen the democratic foundations that foreign manipulation seeks to erode.

Bibliography

- Al Jazeera. (2025, September 29). *Moldova's pro-EU party wins election hit by Russian interference claims.* [Al Jazeera News]. https://www.aljazeera.com/news/2025/9/29/moldovas-pro-eu-party-wins-election-hit-by-russian-interference-claims

- Cardiff University – Security, Crime and Intelligence Innovation Institute. (2023, February 8). *West ill-prepared to deal with evolving cyber threats, report concludes.* https://www.cardiff.ac.uk/news/view/2699454-west-ill-prepared-to-deal-with-evolving-cyber-threats,-report-concludes

- Center for European Policy Analysis (CEPA). (2024). *Sino-Russian convergence in foreign information manipulation and interference.* https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/

- Digital Forensic Research Lab (DFRLab). (2025, May 1). *The evolving role of AI-generated media in shaping disinformation campaigns.* Atlantic Council. https://dfrlab.org/2025/05/01/the-evolving-role-of-ai-generated-media-in-shaping-disinformation-campaigns/

- Digital Forensic Research Lab (DFRLab). (2025, September 9). *Risk assessment: Moldova's electoral environment in 2025.* Atlantic Council. https://dfrlab.org/2025/09/09/risk-assessment-moldovas-electoral-environment-in-2025/

- European Commission. (2025, November 12). *European Democracy Shield: Protecting elections and democratic processes.* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660

- European External Action Service (EEAS). (2023). *1st EEAS report on Foreign Information Manipulation and Interference (FIMI) threats.* https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

- European External Action Service (EEAS). (2024). *2nd EEAS report on Foreign Information Manipulation and Interference (FIMI) threats.* https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

- European External Action Service (EEAS). (2025). *3rd EEAS report on Foreign Information Manipulation and Interference (FIMI) threats.* https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

- EU DisinfoLab. (2022, September 27). *Doppelgänger: Media clones serving Russian propaganda.* https://www.disinfo.eu/doppelganger/

- Global Affairs Canada – Rapid Response Mechanism. (2024). *Spamouflage: Coordinated information operations linked to China*. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2024-spamouflage.aspx?lang=eng

- Hybrid CoE. (2022). *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework "DISARM" (Hybrid CoE Research Report No. 7)*. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-7-foreigninformation-manipulation-and-interference-defence-standards-testfor-rapid-adoption-of-the-common-language-and-framework-disarm/

- Kırdemir, B. (2020). *Exploring Türkiye's disinformation ecosystem*. EDAM. https://edam.org.tr/wp-content/uploads/2020/07/Exploring-Turkeys-Disinformation-Ecosystem-by-Baris-Kirdemir.pdf

- Recorded Future. (2024). *Russia-linked CopyCop uses LLMs to weaponize influence content at scale*. https://www.recordedfuture.com/research/russia-linked-copycop-uses-llms-to-weaponize-influence-content-at-scale

- VIGINUM – Secrétariat général de la défense et de la sécurité nationale (SGDSN). (2024). *Portal Kombat Network: Analysis of a pro-Russian influence operation targeting Europe*. https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

- VIGINUM – Secrétariat général de la défense et de la sécurité nationale (SGDSN). (2025). *Report on information manipulation threats and artificial intelligence*. https://www.sgdsn.gouv.fr/files/files/Publications/20250207_NP_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_EN_0.pdf

- Ulusan, B., & Özejder, E. (2024). *Russian disinformation in Turkey*. Disinfo in MENAT. https://disinfoinmenat.com/raports/russian-disinformation-in-turkey/