CMC Finland

Volume 16: 2/2026

Divide and Control: An Overview of Foreign Information Manipulation and Interference (FIMI)

Sampo Collander

CMC Finland Working Papers analyse civilian contributions to peace operations and include recommendations for developing practical capabilities.

Author

Sampo Collander

A University of Turku alumnus (MA), the writer is well-experienced in international crisis management. He has served as a Military Officer in Information and Psychological Operations in Lebanon, Kosovo and Afghanistan. He has also worked as a Public Information Officer in Civilian CSDP Missions in Georgia and Somalia, and for OSCE's mission in Ukraine as a Reporting and Political Analysis Officer.

Contact

research@cmcfinland.fi

ISSN 1797-1667

Layout and print: Grano Oy

Table of contents

Since war started in Ukraine in 2014, Foreign Information Manipulation and Interference (FIMI) has emerged as a critical issue in European security and foreign policy discussions. It is important to note that FIMI as a concept is much broader than just disinformation and, as a systematic policy, was first defined by the EU. Russia and China, in particular, seek to undermine democratic institutions and distract societies by fostering mistrust and division. Rather than just exploiting occasional opportunities to interfere, they utilise FIMI as a strategic instrument of their foreign policy. To maximise impact, FIMI activities are often synchronised with major events, such as political summits, elections, national emergencies, or official state visits, to maximise public attention.

The rapid spread of disinformation and malicious information across borders is facilitated by social media platforms, online news ecosystems, and instant messaging applications. This digital reach ensures that FIMI is a global threat.

This paper draws on the latest research and policy documents to provide a brief introduction to FIMI: defining what it is, identifying the actors involved, and explaining their methods and motivations. It also examines the potential impacts of these activities and the actions taken to counter them. The focus is on the European Union and its crisis management missions related to the Common Security and Defence Policy (CSDP). While this brief does not claim to be an exhaustive analysis, it aims to provide the basic knowledge and key terminology necessary to grasp this complex subject.

1 FIMI: What Is It?

The concept and technical term FIMI, or Foreign Information Manipulation and Interference, was developed and is typically used most by the European Union and its member states. The European External Action Service (EEAS) defines it as follows:

> “FIMI is a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.

> FIMI often seeks to stoke polarisation and divisions inside and outside the EU while also aiming to undermine the EU's global standing and ability to pursue its policy objectives and interests."[1]

To be categorised as FIMI, an activity must meet five criteria: **Harmful, Mostly Non-illegal, Manipulative, Intentional, and Coordinated.**[2]

While disinformation is a primary tactic, FIMI encompasses a much broader range of tools. The defining characteristic of FIMI is the use of manipulative techniques rather than an expression of opinion or the dissemination of traditional propaganda. It is designed not just to persuade, but to confuse, divide, and destabilise targeted societies in order to advance the geopolitical goals of a state actor.[3]

It is crucial to distinguish FIMI from the healthy friction of a democratic society. Public debate, dissenting opinions, and political persuasion are essential components of democracy. FIMI refers to activities that are manipulative and coordinated. It is important to recognise what does not constitute FIMI. For example:

- **Individual errors:** A single authentic account sharing misleading or false information.
- **Legitimate dissent:** Dissenting opinions about the national or EU politicians published in reliable, independent media outlets.
- **Satire and Art:** Isolated limericks, cartoons, or memes depicting the government or the EU in a negative light.[4]

---

[1] European External Action Service, 2026. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
[2] European External Action Service, 2026. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
[3] Cyber Risk GmbH, 2026.
[4] Cyber Risk GmbH, 2026.

Key Terminology

- **Attribution:** The process of identifying the specific actor, group, or nation-state responsible for a cyberattack, espionage incident, or other security event, such as information manipulation or interference.
- **Cognitive Warfare:** Operations that target the cognition of individuals, groups, and societies to influence decision-making and behaviour. Unlike psychological operations, cognitive activities are directed at the subconscious mind and emotions.[5]
- **Disinformation:** False or misleading content created and spread with the intent to deceive, secure economic or political gain, or cause public harm.[6]
- **Doxing:** The practice of researching and publishing private or identifying information about an individual on the internet with the intent to publicly expose, shame, or harass the target.[7]
- **Foreign Influence:** Activities including traditional diplomacy, registered lobbying, cultural or educational exchanges, and the open dissemination of information and values. When conducted transparently, foreign influence is a legitimate part of international relations.[8]
- **Foreign Interference:** Influence efforts that deliberately obscure their source or intent. This may involve clandestine funding of political actors, coordinated disinformation campaigns, cyber operations against media infrastructure, or the use of foreign-directed proxy entities.[9]
- **Foreign Information Manipulation and Interference (FIMI):** A mostly non-illegal pattern of behaviour that threatens or negatively impacts values, procedures, and political processes. It is manipulative, intentional, and conducted in an intentional and coordinated manner by state or non-state actors, including their proxies.[10]
- **Hybrid Threats:** An array of harmful activities ranging from influence operations to hybrid warfare. Methods include, e.g., information manipulation, cyberattacks, economic coercion, covert political manoeuvring, and the threat of military force.[11]

---

[5] van der Klaauw, 2023.
[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On the European democracy action plan, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN.
[7] European Institute for Gender Equality, 2026.
[8] Cyber Risk GmbH, 2026.
[9] Cyber Risk GmbH, 2026.
[10] 1st EEAS Report on Foreign Information Manipulation and Interference, 2023.
[11] The European Centre of Excellence for Countering Hybrid Threats, 2024 (a).

- **Information Operations (InfoOps):** A staff function used to analyse, plan, and integrate information activities. The goal is to create desired effects on the will, understanding, and capability of adversaries and audiences in support of mission objectives.[12]
- **Malinformation:** Factual information that is used out of context or shared with the specific intent to cause harm.[13]
- **Misinformation:** False or misleading content shared without harmful intent. Although the sender may act in good faith (e.g., sharing a story with family or friends), the effects can still be damaging to the public information environment.[14]
- **Misinformation Raid:** An operation aimed at artificially amplifying a controversial topic, often through coordinated keywords or hashtags, to increase visibility and manipulate trending algorithms.[15]
- **Psychological Operations (PSYOPS):** Planned activities using methods of communication and other means to influence the perceptions, attitudes, and behaviours of targets, thereby affecting the achievement of political and military objectives.[16]
- **Strategic Communications (StratCom):** The purposeful use of communication by an organisation to fulfil its mission or reach a specific goal.[17]
- **Tactics, Techniques, and Procedures (TTPs):** Patterns of behaviour used by threat actors to manipulate the information environment to deceive. Tactics describe operational goals of threat actors; techniques are actions explaining how they try to accomplish them. Procedures are the particular sequences of techniques that reveal a specific intent or "signature."[18]
- **Threat Actor:** An individual, group, organisation, or government that poses a security threat. Motives vary from financial gain and espionage to the disruption of democratic processes and political influence.[19]
- **Typosquatting:** A form of social engineering where actors register domain names that are slight misspellings of well-known websites to mislead users into visiting a malicious or fraudulent site.[20]

---

[12] NATO, 2023 (a).
[13] Cyber Risk GmbH, 2026.
[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On the European democracy action plan, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN.
[15] VIGINUM, 2024.
[16] NATO, 2023 (b).
[17] Oxford Bibliographies, 2026.
[18] 1st EEAS Report on Foreign Information Manipulation and Interference, 2023.
[19] EUvsDisinfo, 2026.
[20] VIGINUM, 2024.

2 Tactics, Techniques, and Procedures

FIMI operations exploit the openness of liberal democratic societies, and weaponise freedom of speech and the internet to facilitate manipulation. In essence, FIMI is very difficult to execute in countries where there is no freedom of the press. For example, historic examples of influence through media, such as the radio stations Voice of America or Free Europe, contain elements of FIMI, but lack its systematic methods and utilisation of multiple channels in a coordinated way. The primary goal of a FIMI operation is not necessarily to convince the recipient of a specific falsehood, but to confuse and exhaust them. Often, multiple, even conflicting narratives are spread simultaneously. This strategy does not aim to present an "alternative truth," but rather to saturate the public discourse with noise, ultimately blurring the very concept of objective reality itself.[21]

Disinformation is more effective when it blends factual information with partially true or entirely false claims. A wide array of distracting techniques is employed, such as:

- Quoting sources out of context or creating misleading headlines.
- "Drowning" facts in emotional appeals.
- Utilising "fake experts" or assembling fraudulent panels to create a false impression of consensus.
- Presenting the opinion of a single individual or fringe organisation as a representative societal consensus.[22]

The broader purpose of FIMI is to exacerbate societal divisions, undermine the credibility of governments and democratic institutions, and compromise the integrity of elections. Beyond shaping global narratives, these operations seek to suppress the voices of journalists, dissidents, and civil society organisations through coordinated bullying, harassment, and threats.[23]

The following sections present the different tactics and procedures used by the main threat actors, with some real-life examples.

---

[21] Cyber Risk GmbH, 2026.
[22] Hiršs, 2025.
[23] 2nd EEAS Report on Foreign Information Manipulation and Interference, 2024.

2.1 Russian Strategic Objectives and Tactics

In their report for ISW, "A Primer on Russian Cognitive Warfare," Nataliya Bugayova and Kateryna Stepanenko claim that the Kremlin's primary cognitive objective is to compel the international community to accept Russia's foundational premises. To support its strategic aims, Russia utilises a comprehensive array of narrative-delivery tools beyond traditional digital networks, including mainstream media, international conferences, multilateral frameworks, diplomatic channels, and high-profile public statements.[24]

These activities are executed by a sophisticated network of state and private actors closely integrated with the Russian Presidential Administration. A central entity in this network is the Social Design Agency (SDA), also known as Structura. The SDA was responsible for the notorious Operation Doppelgänger, which involved the creation of cloned news websites designed to impersonate legitimate European newspapers.[25] The SDA/Structura network has widely promoted narratives claiming that military support for Ukraine is futile, that Ukrainians are "barbaric Nazis," and that Western sanctions are ineffective. Furthermore, the agency has been directly involved in efforts to manipulate and disrupt electoral discourse in several countries.[26]

Russia's objectives centre on fracturing EU and NATO unity to advance its authoritarian model and superpower ambitions. This strategy includes destabilising democracies in former communist EU states and the United States. Since the early 2010s, Russia's strategic narrative has revolved around a "war with the West."

In 2022, the vast majority of Russian-linked FIMI attacks were designed to distort and reframe narratives regarding the invasion of Ukraine.[27] By the time of the 2024 European elections, these incidents had expanded to target specific organisations and individuals rather than countries.[28] Heads of state, high-ranking government officials, and leaders of international organisations were frequent targets, with Ukrainian President Volodymyr Zelenskyy being the most targeted individual.[29]

During these campaigns, European voters were intimidated with narratives designed to undermine support for Ukraine. Simultaneous smear campaigns attempted to stain political leaders with corruption allegations to foster

---

[24] Bugayova and Stepanenko, 2025.
[25] https://www.disinfo.eu/doppelganger-hub/
[26] Pamment and Tsurtsumia, 2025.
[27] 1st EEAS Report on Foreign Information Manipulation and Interference, 2023.
[28] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.
[29] 2nd EEAS Report on Foreign Information Manipulation and Interference, 2024.

distrust in European institutions. These campaigns are rarely generic; they often exploit specific local vulnerabilities through carefully tailored and targeted content.[30]

The Kremlin's FIMI apparatus combines covert and overt means and relies on tailoring their operations to specific audiences. The main approach remains to create new or deepen existing divisions. Russian FIMI actors also strive to push anti-establishment sentiments by undermining trust in the EU by frequently targeting its institutions and leaders. The EU is portrayed as either undemocratic and aggressive, or too weak.[31]

FIMI incidents were reported in 100 different countries in 2025, underscoring the global nature of the threat. In Eastern Europe, Ukraine remains the primary victim, while Moldova appeared as one of the key targets in 2025, due to the parliamentary elections. Armenia was also increasingly targeted in the context of its upcoming elections in 2026. Many EU Member States, such as France, Germany, Poland, Belgium, Italy, and Spain, faced frequent attacks, too, as did the United Kingdom. Financial support, major electoral events, and transatlantic relationships were all topics exploited by the threat actors.[32]

2.1.1 Concept of Reflexive Control

Russia views information as both a weapon and an environment—a concept formally known as information confrontation. Russia's approach to the weaponisation of information is complex and long-term, employing a mix of state and non-state structures to advance geopolitical objectives. By prioritising long-term influence over isolated incidents, Russia continues to exploit structural weaknesses in the global information landscape, establishing its FIMI tactics as a serious security concern for the European Union.[33]

Russia's cognitive warfare is deeply rooted in the Soviet concept of reflexive control. Developed by Soviet mathematician and psychologist Vladimir Lefebvre in 1967, reflexive control is defined as the process of transferring the bases for decision-making from one opponent to another. Essentially, the Kremlin seeks to compel its adversaries to voluntarily choose a course of action that favours Russia by manipulating their perception of reality. Under this doctrine, the goal is to make the opponent accept Russian premises as their own, leading them to reason their way toward a predetermined, Kremlin-favourable

[30] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.
[31] 4th EAS Report on Foreign Information Manipulation and Interference, 2026.
[32] 4th EAS Report on Foreign Information Manipulation and Interference, 2026.
[33] The 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.

conclusion. A prominent modern example occurred in the lead-up to the 2022 invasion: Putin leveraged the false assertion that discussions of Ukraine's NATO accession posed an imminent existential danger to Russia. Although this claim has been thoroughly debunked, the Kremlin used it as a "foundational premise" to justify the full-scale invasion of Ukraine to both domestic and international audiences.[34]

While tactical disinformation focusses on shaping the public's understanding of specific events, Russian strategic information operations strive for systemic, long-term impact. These operations target the fundamental reasoning of individuals, conditioning them to act in Russia's favour while believing they are pursuing their own interests. To change a society's existing premises, the Kremlin substitutes objective facts with a favourable set of "alternative facts." Ultimately, these strategic operations seek to condition the West toward inaction regarding Russian aggression.[35]

For example, the Kremlin consistently asserts that a Russian victory in Ukraine is inevitable, that Russia is entitled to Ukrainian territories it does not even control, and that it deserves a predefined sphere of influence. By using information operations to construct a world order that accepts these premises without resistance, Russia aims to achieve strategic objectives that would otherwise be beyond its conventional military or economic means.[36]

In 2026, Russian funding for FIMI is set to rise as part of the budget increase for state-controlled media. Kremlin's FIMI activity is likely to intensify further, and elections are expected to remain key targets for Russian FIMI, both in the EU and in neighbouring countries, including Armenia. It is also anticipated that the Baltic Sea and the Arctic regions will be among the targets in the information space.[37]

2.2 The Chinese Dimension

China is also a proven FIMI actor, though its focus differs slightly from Russia. It seeks not only to push its own message but also to aggressively suppress any content challenging its official narrative.[38] China utilises a diverse array of methods to advance its global interests, ranging from classic information operations to the suppressing of critical voices. Its primary targets include domestic

---

[34] Bugayova and Stepanenko, 2025.
[35] Bugayova and Stepanenko, 2025.
[36] Bugayova and Stepanenko, 2025.
[37] 4th EAS Report on Foreign Information Manipulation and Interference, 2026.
[38] 1st EEAS Report on Foreign Information Manipulation and Interference, 2023.

audiences, Taiwan, and the Chinese diaspora, with the United States remaining a central focus for its influence networks. A key element of Chinese FIMI is its attempt to control all discourse related to China worldwide by suppressing unwanted information.[39] Particularly in developing countries, Chinese diplomats and state media consistently portray the United States and its European allies as malicious forces whose influence must be eradicated.[40]

During Russia's war of aggression against Ukraine, Chinese state-controlled media and official social media channels have frequently amplified pro-Kremlin narratives. The EEAS has identified several instances where disinformation has migrated between the Chinese and Russian FIMI ecosystems, with content created by one actor being amplified by the other.[41]

China continues to expand its global media footprint, utilising state-controlled outlets and social media to spread both general and localised content, most notably in Africa. This content is meticulously tailored to align with China's official narratives. EEAS analysis indicates that China's efforts are heavily focussed on bolstering the country's international image, particularly regarding human rights, the South China Sea, and issues it deems strictly domestic.[42]

Chinese efforts present China as a force for peace and a reliable and consistent diplomatic and trading partner, especially for the Global South. While promoting Chinese concepts and diplomatic efforts, these narratives were often coupled with offensive elements, such as criticism of "the West" as cynical and aggressive.[43]

[39] Nichols, Svetoka, Lucas et.al., 2022.
[40] Soula and Avgoustidis, 2024.
[41] 1st EEAS Report on Foreign Information Manipulation and Interference, 2023.
[42] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.
[43] 4th EAS Report on Foreign Information Manipulation and Interference, 2026.

Analytical Frameworks: The 4D and 5D Models

According to Mārtiņš Hiršs, the Russian information influence strategy is built on four core principles: **Dismiss, Distort, Distract, and Dismay**. These techniques are designed to confuse the public, erode the understanding of unfolding events, and sow discord within a target society's political and social elite. [44]

- **Dismiss:** To reject accusations and attack the critic.
  - *Methods:* Personal attacks, mockery, and setting unrealistic demands for evidence.
- **Distort:** To manipulate information by omitting crucial details or context.
  - *Methods:* Forgery, information distortion, and the use of fake experts.
- **Distract:** To divert attention by spreading conspiracy theories or levelling counter accusations.
  - *Methods:* Whataboutism, straw man arguments, conspiracy theories, and flooding the information space with noise.
- **Dismay:** To discourage opponents from taking meaningful action.
  - *Methods:* Presenting false dilemmas and slippery slope arguments.[45]

The European External Action Service (EEAS) utilises a nearly identical classification in its analysis but includes a fifth element: **Divide**. While Hiršs views societal division as the result of these actions, the EEAS classifies it as a specific ***method*** of operation:

- **Dismiss:** Pushing back against criticism, denying allegations, and denigrating the source.
- **Distort:** Reframing, twisting, or fundamentally changing the narrative.
- **Distract:** Shifting attention toward a different actor or narrative to deflect blame.
- **Dismay:** Using threats and intimidation to scare off opponents.
- **Divide:** Deliberately creating conflict and widening existing fractures within or between communities.[46]

---

[44] Hiršs, 2025.
[45] Hiršs, 2025.
[46] 1st EEAS Report on Foreign Information Manipulation and Interference, 2023.

2.3 Threats to Electoral Integrity

Elections are the cornerstone of democratic societies; the legitimacy of these regimes depends on the integrity of the vote. FIMI campaigns may pose a critical threat to this stability, as hostile actors seek to manipulate public opinion, influence voter behaviour, and erode trust in electoral processes.[47] Consequently, democratic institutions and cycles have become the primary targets of these operations.

The recent global electoral landscape has seen a record number of recorded incidents, most notably during the 2024 European elections, the Taiwanese and U.S. presidential elections, the French legislative elections, and the critical votes in Moldova and Georgia. Techniques identified during the 2016 U.S. elections, such as social media manipulation and hack-and-leak operations, have since evolved. Today, Russia funds foreign media, hires influencers via intermediaries, deploys highly targeted advertising, and maintains vast bot networks to spread fabricated news and foment polarisation.[48]

Regarding the European Elections, the EEAS detected 42 specific cases of Russian FIMI activity. These efforts escalated sharply in the weeks leading up to the vote and persisted well after the polls closed. The operations followed a calculated, strategic pattern:

- **Infrastructure Preparation:** Establishing FIMI networks well in advance.
- **Initial Assault:** Launching early attacks on the democratic process.
- **Cyber-Enabled Interference:** Deploying digital tools to compromise information or infrastructure.
- **The Surge:** Maximising activity immediately prior to the vote.
- **Post-Election Undermining:** Implementing efforts to cast doubt on the legitimacy of the results.[49]

In 2024, Russia targeted Moldova's presidential elections and its EU accession referendum. Similarly, the parliamentary elections and subsequent civic unrest in Georgia were fuelled by pro-Kremlin actors striving to dismantle societal cohesion and exacerbate political divisions. Beyond covert operations, Russia leveraged diplomatic channels and state officials to lend legitimacy to its disinformation. Russian diplomatic social media accounts act as amplifiers, extending the reach of these campaigns across Africa, the Middle East, and Latin America.[50]

---

[47] FIMI-ISAC Collective, 2024.
[48] Havula, and Pörsti, 2026.
[49] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.
[50] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.

2.4 The Challenge of Attribution and Timely Response

Identifying the operators behind FIMI remains a sensitive and technically complex challenge. Malicious actors utilise a set of tools to hide their identity or create intentional misdirection. However, it is possible to track foreign bot activity by analysing linguistic features, comment metadata, and posting timestamps, and then cross-referencing them with content published by official Russian administration channels.

After foreign interference campaign was uncovered, a significant intervention occurred ahead of the Czech parliamentary elections in October 2025, when TikTok removed 178,000 accounts linked to coordinated FIMI operations.

In the defence of electoral processes, a timely response is vital. This requires constant monitoring and the capacity for rapid intervention. If this is not achieved, coordinated information operations are able to influence the feeds provided by platform algorithms and even drown out legitimate information.[51] FIMI is therefore one element that organisations engaged in electoral observation, such as EU and the OSCE, should give more attention.

3 FIMI and CSDP Missions: Risks to Personnel and Mandates

FIMI has become an urgent issue to address in the field of the EU's Common Security and Defence Policy, as FIMI campaigns frequently target public opinion regarding EU civilian missions and military operations abroad. These campaigns seek to diminish a mission's popularity, erode diplomatic relations, and, in extreme cases, may lead to physical hostility against personnel and assets on the ground. Any deterioration of relations with a host country, or the cultivation of a negative image among the local population, can cause significant damage to the European Union's strategic interests.[52]

By misleading partner countries and local populations about a mission's role and mandate, FIMI actors can directly jeopardise the successful implementation of the mandate and even the security of mission members. In unstable

---

[51] Trnka, 2025.

[52] European External Action Service, 2026. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

regions, particularly those characterised by armed insurgencies or transnational threats, FIMI can trigger violence by swaying public sentiment against an EU presence.[53]

The following section briefly describes foreign interference in specific countries and regions hosting CSDP missions. While Ukraine faces the greatest volume and complexity of disinformation and interference, it is excluded from this specific analysis due to the sheer scale of the conflict.

3.1 Armenia: A New Front in the Hybrid War

Much like Moldova and Georgia before it, Armenia is now viewed by Moscow as a new front in a hybrid war. Russia appears increasingly unwilling to cede ground to what it perceives as Western enemies in the South Caucasus.[54] Consequently, foreign influence operations in Armenia have evolved from episodic disinformation into complex, multilayered efforts. Beyond mere information manipulation, these operations now encompass electoral engineering, illicit political financing, institutional co-optation, and cyber-disruption. The primary source of these efforts is Russia and its Armenia-based proxy networks, whose shared objective is to preserve long-term Russian control over Armenia's geopolitical orientation as Yerevan seeks deeper cooperation with the West.[55]

Unsurprisingly, the EU Mission in Armenia (EUMA) has been a target of controversial allegations since its inception. Russian narratives paradoxically portray the mission as powerless and ineffective, yet simultaneously claim it is secretly armed and represents an obstacle to peace. The mission is further accused of conducting espionage against Armenian actors, Russia, and Iran, and acting as a front for "creeping NATO expansion." Notably, Russian and Azerbaijani media outlets frequently cite one another to amplify these narratives, creating a closed loop of misinformation that reinforces these claims across the region.[56]

A central disinformation narrative alleges that the EU is conducting a geopolitical offensive in the South Caucasus region, depicting Russia as being under an existential threat of encirclement and destabilisation. In this framework, the EU is characterised as a hostile actor waging a hybrid war through covert tactics. Furthermore, the EU is accused of orchestrating destabilisation in Armenia

---

[53] European External Action Service, 2026. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
[54] Carnegie Endowment for International Peace, 2026.
[55] Helsinki Citizens' Assembly Vanadzor, International Partnership for Human Rights, 2026.
[56] media.am, 2025.

by supporting revolutionary elites and the "puppet regime" of Nikol Pashinyan in an effort to expel the Russian presence from the country.[57] During 2025 and the first quarter of 2026, Armenia was targeted by FIMI incidents in the context of the upcoming elections in June 2026.[58]

3.2 Georgia: Domestic Narratives and the "Second Front"

Many Russian tactics follow patterns observed from the Black Sea to the Arctic. As in Armenia, adversarial narratives portray the EU as a destabilising force in Georgia. However, this is localised through the narrative of a shady global "party of war," which allegedly seeks to drag Georgia into a direct confrontation with Russia to open a "second front."

In Georgia, many of these narratives are domestically generated and reflect the interests of the ruling elite. This homegrown disinformation has reduced the need for direct Russian FIMI efforts, as the Kremlin can simply amplify existing local themes. For example, by claiming that the EU funds protests against the ruling Georgian Dream party, the government seeks to implicate the EU in domestic political struggles. Interestingly, the EU Monitoring Mission (EUMM) is largely exempted from such claims, as the current regime perceives the mission's presence as serving its own interest in stability.[59]

3.3 Moldova: A Laboratory for Interference

Prior to the 2024 presidential election and the EU accession referendum, Russia launched a campaign to undermine Moldova's European trajectory and weaken support for President Maia Sandu. Unlike in previous cycles, the Kremlin made little effort to conceal its involvement, and it combined covert and overt messaging channels. Numerous FIMI resources previously used against Ukraine were redirected to establish a sprawling network of local channels within Moldova. Russian official channels became directly involved in targeting Moldova, adopting a more aggressive posture. The Russian Ministry of Foreign Affairs and state-controlled media outlets acted as primary content creators, directly targeting Moldova.

---

[57] EUISS, 2025.
[58] 4th EAS Report on Foreign Information Manipulation and Interference, 2026.
[59] EUISS, 2025.

This disinformation ecosystem relied on a "trickle-down" amplification strategy:

- **Initial Amplification:** Telegram channels affiliated with Russian state media served as the primary nodes.
- **Repurposed Narratives:** Outlets previously focussed on Ukraine and the South Caucasus shifted their focus to Moldova, even repurposing baseless allegations, such as organ trafficking, to target the Moldovan leadership.
- **Full-Scale Media Infrastructure:** A network of websites, complete with professional TV studios for live broadcasts, was established. Technical analysis linked the IP addresses of these networks directly to multiple RT-affiliated (Russia Today) domains.[60]

The core messaging sought to portray the EU as an existential threat to Moldova's economic and political sovereignty while characterising EU integration as a direct provocation of Russia or a threat to Russian-speaking communities. These efforts were also used to fuel domestic tensions within the Transnistrian region.[61]

The Russian FIMI infrastructure tested in 2024 was fully operationalised during the critical September 2025 Parliamentary Elections.[62] In response, the Moldovan authorities introduced a series of targeted legal adjustments designed to restrict foreign interference. Amendments to the Audiovisual Code and media legislation created tightened windows for sanctioning disinformation during campaign periods, allowing the Audiovisual Council to act within accelerated deadlines. Furthermore, these tools strengthened national capacity through partnerships with trusted notifiers and specialised fact-checking mechanisms.[63]

The 2025 elections served as a definitive stress test for Moldova's resilience architecture. The operationalisation of the Centre for Strategic Communication and Combating Disinformation (CSCCD) and its inter-agency task force enabled a structured national response. Moldovan institutions conducted joint simulations, real-time monitoring, and proactive narrative correction. By the end of the 2025 cycle, Moldova had developed an integrated and functioning operating model comparable to the defence systems within the EU.[64]

---

[60] https://euvsdisinfo.eu/in-russias-fimi-laboratory-test-case-moldova/
[61] https://euvsdisinfo.eu/in-russias-fimi-laboratory-test-case-moldova/
[62] https://euvsdisinfo.eu/in-russias-fimi-laboratory-test-case-moldova/
[63] The European Platform for Democratic Elections (EPDE), 2025.
[64] FIMI-ISAC Collective, 2025.

3.4 Sub-Saharan Africa: Geopolitical Battleground

In November 2024, the First Ministerial Conference of the Russia–Africa Partnership Forum convened foreign ministers from across the continent alongside representatives from the African Union and various regional organisations.[65] During the summit, Russian President Vladimir Putin pledged "total support" for the continent, specifically targeting cooperation in combating terrorism and extremism. Russian Foreign Ministry spokeswoman Maria Zakharova framed the conference as a strategic victory that dashed Western "dirty hopes" for Russia's isolation, underscoring Moscow's intent to deepen its influence and bolster its regional presence.[66]

Russia has significantly expanded its FIMI operations across Africa as the continent increasingly becomes a key geopolitical battleground. Moscow has adapted its tactics to capitalise on regional political shifts, positioning itself as a sovereign counterforce to the West. This strategy relies on an integrated network of state-run media, covert outlets, diplomatic channels, and local amplifiers. While global agencies such as TASS and RIA Novosti provide baseline narratives, local branches such as RT Africa and Sputnik Afrique localise content to resonate with regional audiences. Russian embassies, particularly in countries such as South Africa and Kenya, frequently serve as amplifiers. By consolidating state assets, covert operations, and local networks, Russia aims to reshape public perception and undermine Western influence, to advance its long-term geopolitical objectives.[67]

3.5 The Sahel: A Pattern of Information-Kinetic Convergence

A distinct pattern has emerged in Russia's engagement with the Sahel states. A massive surge in pro-Russian media typically precedes the deployment of military forces, now reorganised under the Africa Corps (formerly the Wagner Group). For instance, in the two months prior to Wagner's arrival in Mali in 2021, local pro-Russian messaging surged by an astonishing 1,576%. Between 2020 and 2023, Mali, Burkina Faso, and Niger saw similar dramatic increases

---

[65] Joint Statement of the First Ministerial Conference of the Russia-Africa Partnership Forum, 10 November 2024. https://mid.ru/en/foreign_policy/russia_africa/1980876/

[66] Terren, L., Van Aelst, P. & Van Damme, T., 2025.

[67] EU vs Disinfo. 2025 https://euvsdisinfo.eu/echoes-of-influence-inside-russias-fimi-activities-in-africa/

in pro-Russian output. This flood of media correlates directly with a measurable rise in public support for Russia. Narratives often weaponise anti-colonial sentiment, particularly toward France, while promoting Russian leadership as a catalyst for pan-Africanist causes and regional stability.[68]

These campaigns also frame Western policies on social issues, such as LGBTQI+ or women's rights, as neo-colonial attempts to undermine local traditions and values. Simultaneously, independent and Western media outlets are systematically discredited as mere "propaganda outlets."[69]

Russia's influence has intensified rapidly in Mali and Burkina Faso, directly impacting CSDP missions by destabilising long-term cooperation efforts and eroding trust in EU partnerships. Survey data from 2019 to 2023 illustrates this shift:

- **Mali:** Pro-Russian sentiment rose from 64% to 89%.
- **Burkina Faso:** Pro-Russian sentiment rose from 55% to 81%.
- **French Leadership:** Approval collapsed from approximately 50% to less than 20% in both countries.

Following the junta-ordered closure of the mission in Niger in 2023, EUCAP Sahel Mali remains the only civilian CSDP mission active in the region.[70]

Monitoring FIMI in Sub-Saharan Africa is rather challenging for CSDP missions because the media landscape operates in a non-traditional manner. Information flows often merge conventional media with social media, radio, and word of mouth. In environments marked by insurgencies and the presence of non-state armed groups, FIMI poses a severe threat to both national stability and the safety of international actors.[71]

4 European Response

While this paper cannot introduce every entity currently monitoring and countering FIMI, several European and international partners have established national and private organisations to combat disinformation and broader FIMI activities.

---

[68] Terren, L., Van Aelst, P. & Van Damme, T., 2025.
[69] EU vs Disinfo. 2025 https://euvsdisinfo.eu/echoes-of-influence-inside-russias-fimi-activities-in-africa/
[70] Terren, L., Van Aelst, P. & Van Damme, T., 2025.
[71] Council of the European Union, 2026.

The current U.S. administration has withdrawn from efforts to counter foreign influence operations, and closed a State Department division for monitoring disinformation by Russia, China, and Iran. Also, the units within the FBI and cybersecurity authorities tasked with intervening in foreign interference have been disbanded. Demands on the deregulation of American social media platforms has led them to cut down on moderation and fact-checking, which also has an impact on the European information environment.[72]

To protect the integrity of the information environment and strengthen democratic resilience, in the last few years the European External Action Service (EEAS) defined the concept of FIMI and developed a toolbox to respond to this security threat.[73] The East StratCom Task Force was founded in 2015 to address Russia's disinformation campaigns, and was followed by the creation of the Western Balkans Task Force, the Task Force South, and the Sub-Saharan Africa Stratcom Task Force.[74]

The EEAS presented an analytical framework and methodology in its first EEAS Report on Foreign Information Manipulation and Interference Threats in 2023. Its aim was to bring experts closer together to systematically detect, analyse, document, and ultimately understand FIMI activities. The second report on FIMI threats outlines how to connect analysis to effective action. It proposes an evidence-informed and risk-based framework of responses, the FIMI Response Framework, which enables the activation of adaptive instruments.[75]

The EUvsDisinfo website and social media accounts, published in several languages, are another element of EEAS aimed at countering disinformation. EUvsDisinfo analyses and debunks cases where the Kremlin is utilising disinformation for information manipulation.[76]

4.1 FIMI Toolbox for Domestic and Overseas Use

Threat actors use FIMI as a strategic instrument of their foreign policy and to foster their ambitions. For good reason, FIMI is considered a security threat, as well as a threat to society and democracy. Because the risks are complex,

---

[72] E.g., Havula, and Pörsti, 2026.
[73] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.
[74] https://www.eeas.europa.eu/eeas/2022-report-eeas-activities-counter-fimi_en#:~:text=STRAT.,Ukraine%20on%2024th%20February%202022.
[75] 2nd EEAS Report on Foreign Information Manipulation and Interference, 2024.
[76] EUvsDisinfo https://euvsdisinfo.eu/

there is not one single solution for all of them. Therefore, the EU has developed the FIMI Toolbox to tackle multi-faceted and multi-level setup of threats and risks.[77]

After the first EEAS Report on Foreign Information Manipulation and Interference Threats, threat reports on the FIMI threat landscape have been published annually. Each has introduced new instruments to the analysis and responses to FIMI. The first report introduced a methodology for investigating FIMI activities, and the second report put forward a response framework for responding it.[78] The third report presented a matrix to expose networks behind influence operations and the fourth focussed on deterring FIMI operations.[79]

Malicious actors seek to blur their origin by using tools and techniques that confer anonymity or create misdirection. The EEAS analysed 540 FIMI cases from 2025, 29% of which were attributed to Russia and 6% to China. While 65% of the incidents remain unattributed, there are indicators of coordination with Russian- or Chinese-attributed FIMI infrastructures.[80] To support attribution and develop existing methodologies, the EEAS STRAT has produced the FIMI Exposure Matrix,[81] a framework to classify and link channels to FIMI threat actors. The European Union has created a set of instruments to address FIMI, while fully respecting fundamental rights and freedoms. The instruments can be grouped into four dimensions:

1. **Situational Awareness:** A thorough understanding of the threat is vital, to decide the most suitable responses.
2. **Resilience Building:** Continuous and permanent developing of working methods and processes on, e.g., strategic communications, cooperation with the EU's Rapid Alert System, and raising awareness.
3. **Disruption and Regulation:** Efforts to enhance trust, transparency, and safety in the information environment, such as the Digital Services Act.
4. **Measures related to EEAS and diplomatic responses:** Instruments in the area of foreign and security policy, such as international cooperation, the G7 Rapid Response Mechanism, or the sanctions on Kremlin-controlled outlets such as RT and Sputnik.[82]

---

[77] 2nd EEAS Report on Foreign Information Manipulation and Interference, 2024.
[78] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.
[79] EUvsDisinfo
[80] 4th EAS Report on Foreign Information Manipulation and Interference, 2026.
[81] 3rd EEAS Report on Foreign Information Manipulation and Interference, 2025.
[82] 2nd EEAS Report on Foreign Information Manipulation and Interference, 2024.

The EEAS supports CSDP missions in their capability to address and counter FIMI by equipping missions with the relevant instruments, such as situational awareness, capacity building, and providing advice when necessary.[83]

As described earlier, CSDP missions are by no means exempt from disinformation and other foreign interference. On the contrary, they are often on the frontline of information warfare, and may face operations launched by local or foreign actors to diminish the European presence in the region. In tense circumstances, absurd rumours can spread and lead to unpredictable consequences.

Missions are likely the local actors with the most targeted capacity to monitor FIMI incidents and assess their severity. In civilian CSDP missions, Mission Analytical Capability Analysts (MAC) and Press and Public Information Officers (PPIO) are usually the primary focal points for monitoring FIMI. Among other tasks, PPIO is monitoring local media, and has local staff members with the language and cultural knowledge to assist them. MACs are collecting their data from various open and other sources.

In the field, attribution of FIMI campaigns is outside of the mandate of civilian CSDP missions. However, if instructed to do so and within their available capacity, the missions can make valuable contributions to EEAS's efforts to detect and analyse FIMI campaigns through their understanding of the local context.

Head of Mission (HoM) is used publicly to correct disinformation regarding the mission when necessary. When a diplomatic or political response is considered appropriate, EU delegations play a crucial role. The delegations should also provide political guidance in the field, including in responding to FIMI incidents, and lead the actions. Nonetheless, the division between missions' and delegations' responsibilities and tasks may not always be clear, which may lead to diffidence in tense situations.

Follow-up and reporting on FIMI should be included among the main deliverables of MACs and/or PPIOs in every mission, and they should receive proper training for the tasks prior to deployment. Consequently, monitoring and reporting FIMI activities should be considered a duty for all mission members.

Since situations can escalate very quickly, the actions and responsibilities for countering FIMI operations should be clear and operatives should preferably be trained like all other mission security procedures. EEAS should also provide clear instructions on the division of responsibilities between CSDP missions and delegations to monitor, assess, and, when necessary, respond to FIMI in the field.

---

[83] EEAS: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

Sources

Bugayova, Nataliya and Stepanenko, Kateryna, *A Primer on Russian Cognitive Warfare*, 2025.

Carnegie Endowment for International Peace, *Russia Won't Give Up Its Influence in Armenia without a Fight*, 2026. https://carnegieendowment.org/russia-eurasia/politika/2026/01/armenia-russia-drifting-apart.

Helsinki Citizens' Assembly Vanadzor, International Partnership for Human Rights, *Countering Foreign Influence Operations in Armenia: Building Democratic Resilience ahead of the June 2026 Elections and Beyond*. A policy brief.

CyberRisk Gesellschaft mit beschränkter Haftung (GmbH), 2026. https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html

ENISA (European Union Agency for Cybersecurity), *Threat Landscape for Foreign Information Manipulation*, 2024.

EU DisinfoLab, *Operation Doppelgänger: The Evolution of Russian Impersonation Campaigns*, 2024. https://www.disinfo.eu/doppelganger-hub/

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), *The Hybrid Threat Landscape*, 2024 (a).

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), *Local Vulnerabilities and Foreign Interference*, 2024 (b).

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), *The South Caucasus as a Hybrid Front*, 2024 (c).

European External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats – Towards a framework for networked defence*, 2023.

European External Action Service (EEAS), *2nd EEAS Report on Foreign Information Manipulation and Interference Threats – A Framework for Networked Defence*, 2024.

European External Action Service (EEAS), *3rd EEAS Report on Foreign Information Manipulation and Interference – Exposing the architecture of FIMI operations*, 2025.

European External Action Service (EEAS), *4th EEAS Report on Foreign Information Manipulation and Interference Threats – Dismantling the FIMI House of Cards*, 2026.

European External Action Service (EEAS), *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI),* 2026. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

European Institute for Gender Equality, *Glossary and Thesaurus*, 2026. https://eige.europa.eu/publications-resources/thesaurus/terms/1460?language_content_entity=en#:~:text=Description.%20Doxing%20refers%20to%20the%20online%20researching,publicly%20expose%20and%20shame%20the%20person%20targeted

The European Platform for Democratic Elections (EPDE), *Moldovan Parliamentary Elections: Post-electoral Analysis*, 2025. https://epde.org/reports/moldovan-parliamentary-elections-post-electoral-analysis/

European Union Institute for Security Studies (EUISS), *Digital Echoes: Countering adversarial narratives in Georgia and Armenia*, 2025.

EUvsDisinfo. https://euvsdisinfo.eu/

FIMI-ISAC Collective, *Findings I: Elections*, October 2024. https://www.disinformationindex.org/files/fimi-isac-collective-findings-i-elections.pdf

FIMI-ISAC Collective, *Assessment of Foreign Information Manipulation and Interference in the 2025 Moldovan Parliamentary Election*, 2025. https://www.fimi-isac.org/reports

Havula, Pipsa and Pörsti, Joonas, *Venäjän ja Kiinan mediaan kohdistama informaatiovaikuttaminen ja häirintä - Kartoitus Suomen ja naapurimaiden tilanteesta*, 2026.

Hiršs, M., in *Handbook on Countering Disinformation: Recognise and Resist. State Chancellery*, Riga 2025.

Joint Statement of the First Ministerial Conference of the Russia-Africa Partnership Forum, 10 November 2024. https://mid.ru/en/foreign_policy/russia_africa/1980876/

media.am, *Coinciding Agendas: Russian and Azerbaijani Media Narratives Target EU Mission*, 2025. https://media.am/en/verified/2025/06/02/42959/

NATO StratCom Center of Excellence (COE), *Allied Joint Doctrine for Information Operations*, 2023 (a).

NATO StratCom Center of Excellence (COE), *Psychological Operations (PSYOPS) Policy*, 2023 (b).

Nichols, Katherine; Svetoka, Sanda; Lucas, Edward et al. *China's influence in the Nordic-Baltic information environment: Latvia and Sweden*, Nato Strategic Communications Center of Excellence, 2022.

OSCE/ODIHR, *Election Observation Mission Final Report: Moldova Parliamentary Elections*, 2025.

Oxford Internet Institute, *The Global Inventory of Organized Social Media Manipulation*, 2024.

Oxford Bibliographies, 2026. https://www.oxfordbibliographies.com/display/document/obo-9780199756841/obo-9780199756841-0007.xml

Pamment, James Tsurtsumia, Darejan. *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency, Psychological Defence Agency*, 2025. https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency

Soula, Etienne and Avgoustidis, Alexandros. *Bribes and Lies: Foreign Interference in Europe in 2024*, Alliance for Securing Democracy, 2024. https://securingdemocracy.gmfus.org/bribes-and-lies-foreign-interference-in-europe-in-2024/

Terren, L., Van Aelst, P. & Van Damme, T. *Shifting Alliances in West Africa – Measuring Russian engagement to support counter-FIMI strategies*, European Union Institution for Security Studies, 2025.

Trnka, Michal, Presentation at the Disinfo 2025 conference, Ljubljana, 15.09.2025.

van der Klaauw, Cornelis. *Cognitive Warfare: The Future of Conflict*, NATO Strategic Communications Centre of Excellence (StratCom COE), 2024.

VIGINUM, *Foreign information manipulation and interference (FIMI) threat awareness. Guide for media and fact-checkers during the Olympic and Paralympic Games*, 2024.

Photo on the front cover: EUMM Georgia

CMC Finland

CMC Finland