2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI)

European External Action Service (EEAS)

August 2025

European Union
EXTERNAL ACTION

FOR MORE INFORMATION:

EUvsDisinfo
https://euvsdisinfo.eu/

1st EEAS Report on FIMI Threats
https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

Report on FIMI targeting LGBTIQ+ people
https://www.eeas.europa.eu/eeas/fimi-targeting-lgbtiq-people_en

2nd EEAS Report on FIMI Threats
https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

Report on Doppelganger during the 2024 European Parliament elections
https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf

Report on Operation False Façade
https://euvsdisinfo.eu/uploads/2024/05/EEAS-TechnicalReport-False-Facade.pdf

3rd EEAS Report on FIMI Threats
https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

Disclaimer: This paper aims to illustrate, in a non-exhaustive manner, actions that the EEAS has pursued in order to tackle the threat of foreign information manipulation and interference (FIMI), including disinformation. It is not the purpose of this paper to provide a complete list of all events and activities taken by the EEAS in 2024, but rather to provide key highlights and best practices in the response to FIMI. It is important to underline that, in its daily operations, the EEAS often conducts its activities in cooperation with partners within the EEAS structure, other EU Institutions, EU Member States, international partners, civil society and private sector. This report serves for informative purposes only.

This report discusses research in progress and feedback on its methodology and empirics is much appreciated. However, we would kindly ask you to contact the Data Team before sharing with third parties.

TABLE OF CONTENTS

Executive summary

In 2024, foreign information manipulation and interference (FIMI) remained **a critical and evolving threat to democratic processes** worldwide. Malign actors continued to exploit **technological advances**—particularly AI-driven tools and platforms—to distort the information environment, undermine trust, and target the EU and its Member States as well as countries in the immediate EU Neighbourhood and beyond. These tactics are increasingly part of **broader hybrid strategies** that combine cyber operations, censorship, and disinformation to weaken democratic institutions and societal cohesion. This is why the *Strategic Compass for Security and Defence* identifies FIMI as a key **foreign policy and security challenge** for the EU, with close ties to cybersecurity and hybrid threats.[1]

Over the years, the European Union—through the work done at the EEAS in close cooperation with EU Institutions and EU Member States—has emerged as a **global leader** in developing tools, partnerships, and strategies to address the FIMI threat. Crucially, all EEAS actions are anchored in the **respect for fundamental rights and freedoms**, and contribute to broader multilateral efforts to counter authoritarian influence.

Building on the Strategic Compass and the European Democracy Action Plan,[2] in 2024 the EEAS continued to expand the **EU FIMI Toolbox**, which was endorsed by the European Council in December 2023.[3] The toolbox focuses on four interdependent pillars:

▸ **Situational awareness**: Monitoring, analysis, and information sharing mechanisms such as the EU Rapid Alert System (RAS) and the FIMI Information Sharing and Analysis Centre (FIMI-ISAC);

▸ **Resilience**: Support for civil society, media literacy, capacity building, and partnerships in vulnerable regions, including EEAS's flagship counter-FIMI project *EUvsDisinfo*;

▸ **Regulation**: Alignment with EU initiatives such as the Digital Services Act or the Code of Practice – now Code of Conduct – on Disinformation and ongoing discussions on platform accountability;

▸ **External action**: Strategic communication campaigns and diplomatic engagement to expose and counter FIMI globally.

EU Member States, civil society, international partners, and private sector actors all play vital roles in reinforcing this toolbox and in building a more secure and trustworthy global information environment.

Throughout 2024, particular attention was given to **protecting the integrity of elections** within the EU and abroad. The EEAS worked closely with EU Institutions, EU Member States, and like-minded partners to detect and analyse FIMI attempts. In the run-up and during the **2024 European Parliament elections**, the **EU Rapid Alert System (RAS)** continued to serve as a key mechanism for information exchange on FIMI, enabling early warning and coordinated responses across EU Member States, EU Institutions and international partners. The EEAS also intensified collaboration in other formats, including in the context of the already existing **tripartite coordination mechanism**, composed by the EEAS, the European Parliament and the European Commission. Coordination with like-minded international partners, tech platforms, and the private sector was also step up, in anticipation of a year marked by high electoral activity globally.

As FIMI grows in sophistication and scale, the EEAS remains resolute in its mission to defend the integrity of the EU's information space. A **whole-of-society approach**—grounded in transparency, fundamental rights, and democratic values—is essential to counter this challenge. In 2024, the **FIMI Information Sharing and Analysis Centre (FIMI-ISAC)** became fully operational and provided an innovative platform to enhance the EU's collaboration with civil society organisations specialised in countering FIMI, fostering shared situational awareness and building a trusted community of FIMI responders.[4] The *EUvsDisinfo* platform remained a key awareness-raising tool, reaching a global audience of over 38 million in 2024 with evidence-based analysis of information manipulation campaigns—especially those originating from Russia, China, and other foreign FIMI actors. As of the end of 2024, the *EUvsDisinfo* database featured **more than 18,000 examples** of uncovered and debunked pro-Kremlin disinformation cases.

In parallel, the EEAS continued to **reinforce its regional engagement** to counter FIMI beyond the EU's borders. Support for Ukraine, Georgia, Moldova, and countries in the Western Balkans, Middle East and North Africa, and Central Asia region was strengthened through tailored strategic communication and capacity-building initiatives, while the Sub-Saharan Africa StratCom Task Force deepened cooperation with partners across the continent. These efforts helped build local resilience, support independent media, and empower civil society and fact-checking communities.

The EU also intensified its external action to address FIMI at a global level. The **G7 Rapid Response Mechanism (RRM)** delivered a **Collective Response Framework** by the end of 2024, developed and negotiated under the leadership of the EEAS, providing a basis for collective responses against the FIMI threat in full alignment with and protection of fundamental values. The EU and **NATO** continued to develop their strategic partnership in the field, while **Joint Security Commitments**—including on FIMI—were concluded with Ukraine and **Security and Defence Partnerships** featuring a FIMI component were signed with **Moldova** (21 May), **Norway** (28 May), **Japan** (1 November), **Republic of Korea** (4 November), **North Macedonia** (19 November) and **Albania** (18 December). The EEAS also continued to support the **EU sanctions policy** and provide evidence for additional sanctioning of Russian individuals and outlets, which serve as instruments of FIMI and war propaganda. Since the start of Russia's full-scale invasion of Ukraine, the EU has listed over 100 individuals involved in Russia's propaganda and FIMI activities, and suspended the broadcasting of over 30 Russian state-controlled FIMI outlets within the EU. **A new sanctions framework** against Russia's destabilising activities, including FIMI, against the EU and its Member States was adopted in October 2024. In 2024, the EU adopted the **first listings** in response to Russia's hybrid threats abroad, including entities and individuals engaged in FIMI activities.
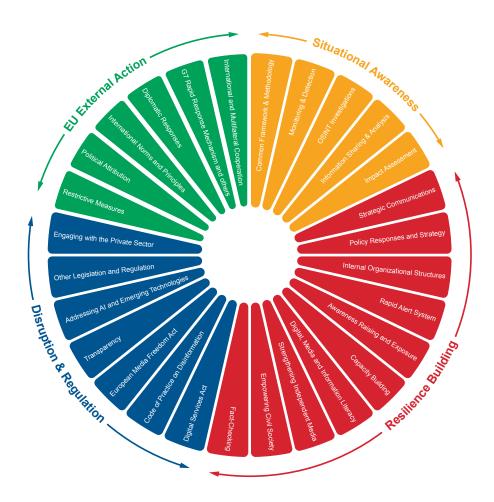
1.STRENGTHENING SITUATIONAL AWARENESS

A thorough understanding of the FIMI threat is paramount for informing EU decision-making in countering this increasing challenge to democracy and security. Thanks to **significant commitment** by the EEAS in developing tools and methodology to track, analyse, and expose FIMI, the overall EU situational awareness has steadily grown in both geographic scope and technical depth.

In January 2024, the EEAS convened its annual flagship conference, *Beyond Disinformation: Strengthening our societies against Foreign Information Manipulation and Interference* (FIMI), that brought together stakeholders from EU institutions, international partner governments and organisations, as well as civil society and private sector partners. On this occasion, HR/VP Borrell launched the **2nd EEAS Report on FIMI Threats**, building on the first report published in 2023.[5] Drawing on 750 investigated FIMI incidents between 1 December 2022 and 30 November 2023, the report provides concrete insights into evolving tactics and

vulnerabilities and proposes a **framework for coordinated responses** against FIMI building on a strong evidence-based approach. It concludes with a case-study applying the framework to previous election-related FIMI incidents in the EU and beyond, offering practical guidance to protect integrity in the information space ahead of the multiple elections taking place in 2024. In April 2024, together with the Spanish authorities, the EEAS also published a technical report on **Operation False Façade**, presenting Russia's FIMI information laundering scheme.[6]

The **FIMI-ISAC** was set up in 2024 to unite the civil society defender community to strengthen collaboration against information manipulation. Its goal is to implement a standardised and interoperable approach for collecting and sharing data on FIMI incidents, in line with the common framework and methodology developed by the EEAS. The FIMI-ISAC represents a major advance towards a more coordinated, effective, and scalable response to FIMI threats.

THE 2024 EUROPEAN PARLIAMENT ELECTIONS

On 6-9 June 2024, the **European Parliament elections** took place and millions of citizens headed to the polls. Election interference does not only take place right before elections – it is a comprehensive and long-term process, which occurs before, during and after the elections. This is why the EEAS preparation for the 2024 European Parliament elections **started already in 2019**, in close coordination with the European Parliament, the European Commission and EU Member States as well as civil society organisations, building on lessons learned from the previous European Parliament elections. The EEAS work rested on the **pillars** laid down in the **FIMI Toolbox**, which the 2024 Council Conclusions on democratic resilience acknowledged as contributing significantly to a comprehensive approach by ensuring coordinated responses and strengthening the overall resilience.[7] In detail:

‣ As part of its efforts to reinforce **situational awareness**, in addition to the above-mentioned 2nd annual Report on FIMI threats, the EEAS published in June a dedicated **report on the Doppelgänger FIMI operations** in the context of the European Parliament elections.[8] The latter was the first report outlining an operation that was then widely reported by other FIMI defenders and media. The EEAS also contributed to the EU's overall situational awareness on FIMI.

‣ Regarding **raising awareness and building resilience**, EUvsDisinfo continued to regularly publicly report about elections interference by Russia and its proxies. In a series of articles on the website, the EEAS showed examples of **key TTPs** employed by the pro-Kremlin actors targeting the European Parliament elections. Analytical articles were published on the Kremlin's attempts to go after leaders with smear campaigns,[9] sow distrust and discontent,[10] flood the information space,[11] drag everyone down into the mud with them,[12] and dismiss the results and drive new wedges after the elections;[13]

‣ On increasing **capacity and resilience building**, the EEAS developed trainings and workshops for diverse audiences. These included the table-top exercise "**Elections in Euphoria**", a dynamic and scenario-based simulation designed for youth, in which participants take on a role of the activists from an NGO promoting election integrity and run a pro-turnout campaign. This workshop was facilitated in collaboration with the European Parliament at the European Youth Event in Vilnius and also with the European Commission during the European Youth Week. The EEAS also delivered trainings in a European Youth Event in Italy and in workshops organised by the College of Europe.

‣ A **reinforced cooperation and joint preparedness with the European Parliament and the Commission** on FIMI was put in place ahead of the elections, working on a **tripartite cooperation format**. This enabled close coordination between teams who worked on tracking and analysing FIMI incidents, strategic communications and awareness raising about FIMI and disinformation, including during election days. The EEAS also strengthened **cooperation** with other networks, including with **EU Member States** via the **Rapid Alert System** and, when relevant, with other networks such as the European Cooperation Network for Elections (ECNE), CERT-EU and relevant Council working parties. A dedicated working group focusing on the elections was set up in the RAS, to enhance informal and quick information sharing, in addition to regular calls.

Throughout 2024, efforts to build capabilities to counter **China's FIMI** progressed in response to calls from EU Member States and the European Parliament. These efforts included deepening understanding of China's activities by monitoring key information environments and analysing its tactics, techniques, and procedures (TTPs). The objective was to develop targeted responses to Chinese FIMI, with initiatives to boost resilience and capacity rolled out over the course of the year.

In November 2024, the EEAS published the toolkit "**How to Detect and Analyse Identity-Based Disinformation/FIMI. A Practical Guide to Conduct Open Source Investigations**" that highlighted the many ways that FIMI actors carry out attacks using the weaponisation of identity-based disinformation (IBD). The publication was followed by an event uniting civil society, EU and international partners in a discussion on how to analyse and respond to identity-based FIMI attacks.

The EEAS continued to systematically provide situational awareness on FIMI attacks and strengthen the counter-FIMI capabilities of **Common Security and Defence Policy (CSDP) missions and operations** in the Eastern Partnership (EaP) region, Sub-Saharan Africa and the maritime dimension. In 2024, the EEAS fulfilled the Strategic Compass mandate and successfully **equipped all CSDP missions and operations with analytical tools to detect, analyse, and respond to FIMI** in their areas of operation. In addition to analytical support and dedicated trainings, the EEAS strengthened strategic communications capabilities of CSDP missions and operations and started to provide dedicated support during crisis.

2. BUILDING RESILIENCE WITHIN THE EU, THE NEIGHBOURHOOD AND BEYOND

Efforts to **foster resilience** in the EU were stepped up, notably in relation to the European Parliament elections (see related box on p. 6). The Political and Security Committee (PSC), the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and regional working parties (e.g. COEST, COWEB, COAFR, COASI, etc.) were briefed on a regular basis on the latest developments concerning FIMI activities.

The EEAS also conducted several **election interference-related workshops** targeting the EU Institutions and CSDP missions and operations. A table-top exercise was co-organised with the Hybrid Working Party under the Belgium Presidency of the Council. In collaboration with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the EEAS also organised a simulation exercise for the RAS contact points in April, and participated in the inter-institutional table top exercise and training organised by DG CNECT. Furthermore, the EEAS provided **trainings on election integrity** for the EU staff during the Interinstitutional Safety and Security Days in May, online training for the CSDP missions and operations, and organised two "Lunch and Learn" initiatives with the EU Member States highlighting best practices in countering FIMI.

EUvsDisinfo, the EEAS flagship project for raising awareness about pro-Kremlin information manipulation and disinformation, experienced **significantly increased reach**: *EUvsDisinfo* content reached at least **38.8 million people in 2024**, a substantial increase from ~20.3 million in 2023. This growth is largely attributable to a higher volume of content produced and posted across multiple social media platforms – Facebook,[14] X,[15] LinkedIn,[16] YouTube,[17] Instagram,[18] and Threads.[19]

The visitors of the EUvsDisinfo website continued to show deep engagement. An exceptionally high **average session duration of more than 14 minutes** suggests thorough use of resources like the "Database" or "Learn" sections. The **Disinformation Review newsletter** continued its weekly cadence (49 issues sent). **Subscriber** numbers grew by **15%**. The website continues to offer content in 13 languages and select content in Bulgarian and Kazakh.

With more than **18,000 examples** of pro-Kremlin exposed and debunked disinformation cases by the end of 2024, the database remains the **world's largest open and structured source of its kind** and provides a practical tool for journalists, researchers, scholars and others tracking and debunking pro-Kremlin information manipulation and interference.[20] Guest content continued to feature, including topics related to soft power FIMI operations, energy, and Africa. Several special topics were covered in connection with key developments in the FIMI landscape. These included Russia's targeting of Ukraine's infrastructure and the Black Sea, the 1,000-day mark since the full-scale invasion of Ukraine on 24 February 2022, the Kremlin's staged efforts to appear interested in peace, systemic brainwashing in Belarus, the European Parliament elections in June 2024, the Paris Olympics, the 79th session of the UN General Assembly, elections and a referendum in Moldova, and Germany's Federal Assembly elections — among others.

CAPACITY BUILDING SUPPORT TO UKRAINE AND MOLDOVA

In 2024, the EEAS devoted considerable effort to support Ukraine and Moldova in countering FIMI. The East StratCom Task Force (ESTF), the Sub-Saharan Africa Task Force and DG NEAR jointly organised a **TAIEX workshop on information resilience** for peer-to-peer exchange between Ukraine, EU Member States and African countries (Ghana, Ivory Coast, Kenya, Nigeria) on securing the information landscape, building institutional and societal resilience, as well as identifying and implementing countermeasures in order to promote EU-Ukraine-Africa cooperation against FIMI.

The ESTF contributed to building response to FIMI capacities of **Moldovan partners**, implementing the "whole-of-society" approach, when civil society, media, and government works together in building societies resilience to FIMI. The EU integration referendum in Moldova and presidential election campaign (2024) was an important test case for Moldovan society resilience to FIMI and lessons learnt for EU communication improvement.

The EEAS Western Balkans Task Force (WBTF) and DG NEAR jointly organised another **TAIEX workshop on FIMI** in October 2024 for a peer-to-peer exchange between **Albanian** civil servants and EU experts in the framework of the ad-hoc parliamentary committee looking into all forms of interference in democratic processes, followed by a second and potentially third round in 2025. The aim of the workshop was to look into ways the Albanian parliament could approach possible scenarios in the future, which will most probably result in a comprehensive national strategy on FIMI, including disinformation.

The EEAS **Sub-Saharan Africa StratCom Task Force**, launched in 2023, monitored **information environments in Sub-Saharan Africa** in order to keep track of FIMI threats and incidents targeting the EU and analyse trends over time, across several contexts (Sahel region, Gulf of Guinea countries, CAR, DRC, Senegal, South Africa). Specific analytical capacity was devoted to the post-electoral crisis in Mozambique, MPOX outbreak in Central Africa, Russian engagement in the media sector in Africa and narratives and behaviours accusing Ukrainian support to terrorist groups in the Sahel. The Sub-Saharan Africa StratCom Task Force also undertook baseline analyses and actor mappings of new countries of engagement such as South Africa and Ghana to enhance understanding of local information manipulation dynamics and inform responses. **Regular exchanges with EU Delegations** took place to strengthen shared awareness and preparedness, including in the context of electoral processes (Ghana) or in the context of attacks against the EU (DRC).

Three events took place in Brussels, with participation of journalists from various African countries: in June (African Union Media Fellows), November (West Africa) and December (Central Africa), in order to increase awareness of media professionals on EU policy making, notably topics of interest to African audiences (migration, peace & security, etc.) and on FIMI dynamics in Europe and Africa. The Task Force also **supported EU Delegations' initiative to counter FIMI** such as an awareness raising campaign during the Presidential elections in Ghana, workshops on FIMI in South Africa and Uganda. The **EEAS Task Force South** has continued to bring journalists and key opinion shapers from across the MENA geography to conduct capacity buildings regarding the EU and its action to counter FIMI.

The EEAS continued engaging with the **civil society**, media professionals, journalists, fact-checkers, data analysts, and media literacy experts in different formats. The year 2024 marked the first time that the EEAS participated and supported the **Global Fact Conference**, the biggest and the most prestigious gathering of fact-checkers organised by the International Fact-Checking Network. The EEAS was represented in a panel on FIMI targeting elections and identity-based disinformation.

Furthermore, the EEAS collaborated with the European Fact-checking Standards Network and invited **fact-checkers** from Georgia, North Macedonia, Türkiye and Ukraine to join the **EU Open Days**. The fact-checkers engaged in live fact-checking with the visitors and taught them verification tools. The EEAS hosted as well one panel discussion with the fact-checkers and one workshop on verification tools.

The second **Media Forum**, organised jointly by the East StratCom Task Force and EU Delegation in Kazakhstan, took place in Astana, Kazakhstan. It brought together a diverse group of journalists, fact-checkers, researchers, and media professionals to discuss the transformative role of artificial intelligence (AI) in journalism and the challenges of fighting FIMI.

The EEAS also continued the **Connecting Media Communities project**, a gathering for media professionals from the EU Neighbourhood and other regions, from Africa to Asia. The event took place in Pristina, Kosovo, on 3-4 October. Participants engaged in several workshops, spanning from constructive journalism, usage of AI in newsrooms to addressing disinformation in gaming. A pivotal outcome of the event was the **Charta for Journalists**, co-authored by all participants. This document outlines the principles and commitments needed to counter disinformation in the years to come. It emphasizes building societal trust in media, ensuring journalist safety and security, securing sustainable financial resources for independent media, and strengthening fact-checking and verification capabilities.

3. EXTERNAL ACTION AND DIPLOMACY

In light of the transnational nature of the threat, the fight against FIMI requires fully leveraging **the EU external action and diplomacy** to work with like-minded and international partners on information sharing, policy approaches and specific projects.

In 2024, the EU signed **Joint Security Commitments** with **Ukraine** and **Security and Defence Partnerships** with **Moldova**, **Norway**, **Japan**, **South Korea**, **North Macedonia**, and **Albania**—marking a significant expansion of its strategic cooperation and global footprint. These agreements include concrete deliverables on foreign information manipulation and interference (FIMI) agenda, reinforcing joint efforts to detect, counter, and build resilience against disinformation and hybrid threats.

The EEAS continued to engage in established dialogues with like-minded international partners throughout the year. Cooperation with the **United Kingdom** and **Canada** on FIMI-related issues remained strong, as both continue to be key international partners in this field, with a shared interest in evolving from joint analysis toward coordinated responses—wherever feasible and appropriate. During the **EU-US Trade and Technology Council (TTC)** Ministerial in April 2024, the EU and the US released a **Joint Statement** that made explicit reference to the risks posed by FIMI, they also agreed on using the same methodology to detect and analyse the threat. To advance more effective responses to FIMI, the EEAS actively participated in expert dialogues and integrated FIMI discussions into established cooperation frameworks with other partners. For example, in line with the EU's **Indo-Pacific strategy**, FIMI-focused discussions were also held with partners across the region.

At the multilateral level, key efforts were channelled through the **G7 Rapid Response Mechanism (G7 RRM)**. The EEAS led a dedicated **Working Group on Collective Response**, working to enhance the G7's response capabilities and develop operational principles to align member states' approaches in countering foreign threats to democracy. Through the **G7 Leaders' Apulia Communiqué**, G7 Leaders reaffirmed their commitment to safeguard democratic values and human rights from FIMI and transnational repression (TNR) threats, and tasked the G7 RRM with developing a **collective response framework** to counter FIMI by the end of 2024. Under the leadership of the EEAS, the framework was developed and delivered, providing the G7 RRM with collective response options to FIMI incidents and facilitating their operationalisation.

In June 2024, the EEAS became one of the founding members of **Ukraine Communications Group** (**UCG**) – a multilateral initiative to synchronise Ukraine-related strategic communications towards priority countries in South America and Africa.

Regular exchanges of in-depth analysis and real-time insights with **NATO** staff ensured continuous collaboration, helping to sustain a shared situational awareness of hostile activity in the information environment.

"Sanctions have not impacted Russia's reputation or attractiveness to investors."

Sanctions have contributed to a deterioration in the investment climate, and the lack of foreign investment will dent Russia's future development prospects. In 2022-2023 over EUR 230 billion of investments were pulled out from Russia. Chinese companies prefer to increase their exports to the Russian market rather than investing in it, and Russia is becoming increasingly dependent on trade with China.

The EEAS also continued to support the **EU sanctions policy** and provide evidence for additional sanctioning of Russian individuals and outlets, which serve as instruments of FIMI and war propaganda. Since the start of Russia's full-scale invasion of Ukraine, the EU has listed over 100 individuals involved in Russia's propaganda and FIMI activities, and suspended the broadcasting of over 30 Russian state-controlled FIMI outlets within the EU. A **new sanctions framework** against Russia's destabilising activities, including FIMI, against the EU and its Member States was adopted in October 2024. In 2024, the EU adopted the **first listings** in response to Russia's hybrid threats abroad, including entities and individuals engaged in FIMI activities.

4. ANALYSIS OF THE THREAT LANDSCAPE IN 2024

In 2024, the prime target for **Russia's** FIMI operations continued to be **Ukraine** with attempts to undermine its legitimacy, jeopardize the international support for the government and people. Almost all disinformation narratives and FIMI activities related to Ukraine in one way or another. This includes attempts to swing international opinion to legitimising Russia's war of aggression, derail and distract focus from Russia's attacks on civilian targets, infrastructure, Russian forces' war crimes and wanton destruction. Historical revisionism and attempts to grossly distort facts became even more mainstream. **AI-generated** content was used more intensely by pro-Kremlin actors as a tool to flood the information space with manipulative content and false claims. Towards domestic audiences inside Russia, the narratives presenting Ukraine, EU, Western countries included a high degree of **hate speech**, making 'Nazi' a common reference and incitement to genocide, continued as a regular occurrence in Russian outlets. **Narratives supporting the war** flooded the education sector, culture, entertainment and most news flows. Attempt to **undermine the EU**, sow divisions around immigration, cost of living, etc. as well as smearing European leaders were general features, but peaked around the European Parliament elections and in connection with Moldova's EU referendum.

Throughout 2024, **China** proved to be a multifaceted FIMI actor with a broad range of tactics. Its activities range from the spreading of **conspiracy narratives** to clearly illegitimate operations such as **intimidation** and **harassment of critical voices** with the aim of **suppressing information** even outside of its borders. Different tactics are often used in combination and can be connected to **other forms of interference**, such as economic coercion, lawfare, and cyber-attacks.

While content creation related TTPs remained most common, they were bolstered by various **amplification TTPs**, including information laundering, posting across platforms, and using hashtags - often hijacking them to better serve Chinese interests. Content was often created in **cooperation with various foreign entities** (e.g. media co-production) to increase credibility. The growing network of China's FIMI assets and proxies extended beyond the state media enterprise. Our analysis confirmed an increase in soliciting both private public relations companies and influencers to create, amplify, and launder content aligned with China's political interests worldwide, often through covert online FIMI networks (e.g. the "Paperwall" campaign). Chinese FIMI activities have also increased the **use of AI** for operational purposes, spanning from overt content sharing to more covert and manipulative operations.

Information suppression continued to be one of the most concerning elements of Chinese FIMI, targeting larger entities such as businesses, civil society, universities and even governments, but also (diaspora) individuals and their families.

In terms of **narratives**, we observed China's persistent efforts to **defend its international image** continue, especially regarding human rights and South China Sea, and areas it deems exclusively domestic, such as Xinjiang, Tibet, Hong Kong, and Taiwan. At the same time, Chinese actors regularly leveraged international conflicts (e.g. Russia's war of aggression against Ukraine, Gaza) as vectors for projecting China's positive role in the global arena, often pairing it with offensive narratives targeting "the West" as hypocritical and inefficient vis-à-vis the Chinese model of international engagement. Taiwanese and, to a lesser extent, the US elections were targeted by China's FIMI networks, and the evolving situation in the South China Sea continued to serve as another high profile front for sustained FIMI activities.

China's FIMI activities operated alongside other threat actors, including Russia. While there have been several reports about the extent of **convergence and mutual learning between the Russian and Chinese ecosystems**, the cross-pollination between the two seems to remain largely opportunistic.

In the **Eastern Partnership region**, **Ukraine** remains the main target of FIMI operations, aiming to support and justify Russia's war efforts as well as undermine Ukraine's fight for its sovereignty and independence. Deceitful claims that Ukraine is "a EU/UK puppet", which is destined to lose are thrown into the information space in addition to messages that "Ukraine does not want peace" and "Support to Ukraine is not in the interest of Europe". Due to EU aspirations for **Moldova** and Ukraine, FIMI operations intensified into amplifying disinformation messages, claiming that "EU accessions leads to loss of sovereignty", "EU membership leads to hardship" and that "EU is corrupt and morally decadent". **Diminishing EU reputation** in the region is a long standing "modus operandi" of Russian information manipulation operations.

In the **Western Balkans**, FIMI operations have sought to **undermine the EU's credibility and hinder the region's EU accession prospects**. Narratives promoting a so-called 'multipolar', 'traditional', and illiberal world order are actively disseminated, often by local actors echoing foreign influence campaigns. These messages are tailored to align with longstanding local grievances and deeply entrenched beliefs. As a result, a generalized anti-Western—implicitly anti-EU—sentiment has gained traction, with varying intensity depending on the actor involved. These narratives were particularly prevalent in Serbia's information environment and spilled over into neighbouring countries where mutual intelligibility of language enables their broader reach.

In the **MENA** region, the information space remained largely antagonistic toward the West, including the EU. This sentiment increased significantly following the **7 October 2023 Hamas attacks on Israel** and the subsequent Israeli military operations in Gaza, the West Bank, Lebanon, Syria, Yemen and Iran. The ongoing crisis polarised regional audiences, many of whom are emotionally invested in the conflict. A broad spectrum of local, regional, and transnational actors have taken advantage of the volatile context to further destabilise the information environment and expand their influence, as well as advance their agendas. Investigations continued to reveal a **surge in manipulated and inauthentic content**, along with a notable rise in hate speech, some of which has crossed into the European information environments inciting violence against certain collectives and religious communities. Tactics observed include the use of **AI-generated visuals**, misleading translations, staged footage, impersonation, and other disinformation techniques aimed at distorting public perception and eroding trust.

In **Sub-Saharan Africa**, information manipulation by foreign and domestic actors intensified throughout 2024, taking advantage of **security crises** (Sahel, Great Lakes, Central African Republic), **electoral processes and contested governance** (Senegal, South Africa, Mozambique, Ghana, Chad), as well as **EU partnerships and programmes** (European Peace Facility deliveries, European Election Observation missions, Migration agreements, Fishery agreements, Just Energy Transition, etc.) or **global developments** (FOCAC meeting in China, BRICS Summit in Russia, World Festival of Youth in Russia, etc.). While most anti-EU, and more broadly anti-Western, narratives draw on local resentment and are peddled by domestic or regional actors, **foreign actors** are increasingly engaged throughout the continent. Besides online activity and information operations by networks of diplomatic accounts, state-controlled media (notably African Initiative) and local/regional media and influencers, **offline engagement** with African media actors is expanding, in the form of trainings (RT Academy, Sputnik pro), study visits to Russia (or Russia controlled parts of Ukraine), content sharing agreements, etc. Attacks against the EU and Western actors are opportunistic but become more systematic in their recurrence and narrative, also promoting strategic competitors like Russia and China as alternative, "reliable and genuine" partners.

In 2024, EU's **Common Security and Defence Policy (CSDP)** areas of deployment continued to face **hostile and coordinated FIMI campaigns**. Over the past year, missions and operations in **Sub-Saharan Africa** witnessed an increase in Russian FIMI targeting the EU and its Member States. This persistent threat has had an impact not only on the image of CSDP and EU deployments in the region, but also on the implementation of CFSP objectives within their mandates. In other areas of operations, particularly in the **EaP**, misleading narratives revolved around the Russian invasion of Ukraine, elections and referendum in Moldova and renewal of the EU mission's mandate in Armenia continuing to sew anti-Western sentiment.

ENDNOTES

1   https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

2   https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en

3   https://www.consilium.europa.eu/en/meetings/european-council/2023/12/14-15/

4   The FIMI-ISAC gathers all parts of the defender community (governments, civil society, private industry) to work towards a standardised and interoperable way of collecting and sharing data on FIMI activities.

5   https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

6   https://euvsdisinfo.eu/uploads/2024/05/EEAS-TechnicalReport-False-Facade.pdf

7   https://data.consilium.europa.eu/doc/document/ST-10119-2024-INIT/en/pdf

8   https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf

9   https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-go-after-the-leaders/

10 https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-sow-distrust-and-discontent/

11 https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-flooding-the-information-space/

12 https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-drag-everyone-down-into-the-mud/

13 https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-dismiss-and-drive-wedges/

14 https://www.facebook.com/EUvsDisinfo

15 https://twitter.com/EUvsDisinfo

16 https://be.linkedin.com/company/euvsdisinfo

17 https://www.youtube.com/channel/UCAiQd5dj168VcYa6Nly_jIw

18 https://www.instagram.com/EUvsDisinfo/

19 https://www.threads.net/@euvsdisinfo

20 https://euvsdisinfo.eu/disinformation-cases/