News Item

4th EEAS Report on Foreign Information Manipulation and Interference Threats

By European External Action Service (EEAS)
April 15, 2026

Executive Summary

The 4th EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats provides a comprehensive assessment of FIMI activities worldwide, based on cases documented and investigated by the EEAS throughout 2025.

A key contribution of this report is the shift from diagnosis to impact through the FIMI Deterrence Playbook. By identifying critical nodes across infrastructures, intermediaries and supply chains, it operationalises deterrence by setting out an approach which targets the threat actor's vulnerabilities. **By striking at the key enablers of FIMI operations such as intermediaries, proxies and service providers the structure that sustains them can become progressively fragile and difficult to sustain.** Existing instruments within the FIMI Toolbox — including sanctions, law enforcement, digital regulation and resilience-building — can be strategically mobilised to raise costs, limiting operational space and reduce the likelihood of future attacks.

The FIMI Deterrence Playbook contributes to bring the EU's and its partners effort to counter FIMI, onto the front foot, marking a shift from a largely reactive to a proactive and anticipatory approach. **In a context of continued escalation, deterrence becomes essential to generate tangible impact.**

During the year, **the EEAS detected 540 incidents globally**. As in previous years, **Ukraine remained the primary target, followed by France, Moldova and Germany.** Attacks not only increased in frequency and intensity but also became more sophisticated. FIMI continues to adapt to technological advances, particularly in Artificial Intelligence (AI). **AI-generated text, synthetic audio and manipulated video have shifted from experimental use to routine**

deployment, becoming cost-effective and scalable tools for threat actors.

In total, **10,500 social media channels and websites were mobilised to produce or amplify FIMI.** Of all documented incidents, 35% were attributed to Russia (29%) and China (6%). Beyond the attributed figures, **Russian and China rely on extensive covert and fabricated networks** aligned with their strategic objectives. By outsourcing capabilities through these opaque networks, they expand their reach while preserving plausible deniability and complicating attribution.

Through systematic mapping of channels and their interconnections, the **report updates the "Galaxy of FIMI operations"** presented in the 3rd EEAS Report on FIMI Threats on in 2025 and deepens understanding of the structural architecture behind FIMI. The network analysis reveals a central group of digital channels functioning as the operational backbone, linked to regional hubs targeting specific geographies, including Sub-Saharan Africa, the Middle East and North Africa, Moldova and Armenia.

Electoral processes once again constituted a primary focus of Russian FIMI activity. In 2025, Russia targeted elections in Germany, Poland, Romania, Moldova, the Czech Republic and Côte d'Ivoire, replicating patterns observed in previous electoral cycles.

This data also enables forward-looking assessment, allowing the anticipation of new vectors of attack. Upcoming electoral processes in Member States (including Slovenia, Hungary, Bulgaria, Cyprus, Estonia, Sweden, Latvia and Denmark) may face similar interference patterns. Beyond the EU, Armenia is expected to remain a key target in the run-up to the June 2026 parliamentary elections. The attack patterns observed during the Presidential elections in Moldova reveal striking similarities with networks and tactics now emerging in Armenia.

Read the full report on the EEAS website here.