Policy Planning and
Strategic Communication
GII.GLOBAL.STRAT.DMD

REPORT ON FIMI THREATS

4th EEAS Report on **Foreign Information Manipulation and Interference Threats**

Dismantling the FIMI House of Cards

European Union
EXTERNAL ACTION

March 2026

FOREWORD BY HIGH REPRESENTATIVE/ VICE PRESIDENT KAJA KALLAS

Today's wars are not only fought with tanks and drones but with lies and algorithms too. The information space is a frontline in the fight for democracy. The greatest threats are state-sponsored operations that seek to confuse and manipulate citizens in order to shape our views, political choices and ultimately the way we vote. Member States of the European Union are top targets for Foreign Interference and Information Manipulation (FIMI), but as we saw this year during elections in Moldova, the closer a candidate country comes to EU membership, the more likely it is to be attacked in this way. Throughout 2025, Ukraine remained a primary goal for Russia-driven content seeking to decrease international support for Ukraine and its people.

Methods of attack are evolving as rapidly as technology develops. Compared to last year, the use of Artificial Intelligence tools in FIMI incidents has increased exponentially. Artificial Intelligence is now fully embedded in Russian and Chinese FIMI operations. AI allows for the mass production of manipulative content at speed, scale and low cost. AI-generated videos and images have become the new norm. Large Language Models (LLMs) are even being 'groomed' by operators who flood the internet with false information in an effort to manipulate results when we use these tools.

We cannot stop others from using FIMI as a weapon of hybrid warfare, but we can make it as hard as possible and ultimately push FIMI actors to reconsider whether pouring so much time and money into it is still worth it. Thanks to the work of the European External Action Service, we know who our enemies are and, in many instances, we know how they are operating. For example, we see the same FIMI playbook that was deployed in Moldova during 2025 being redeployed in Armenia around their elections in 2026.

Europe is far from exhausting our armoury to fight back. Sanctioning operators and their enablers, engaging law enforcement where necessary and regulating our digital space, are all vital steps that Europe must take.

But FIMI is a truly global problem. Last year, more than a hundred countries were attacked, as well as over a hundred individuals including Heads of State and close to 200 organisations such as NATO but also traditional media, NGOs, and academia. Information integrity is a global public good and protecting it demands a global response. That is why countering FIMI is now part of the EU's Security and Defence Partnerships with several countries. And with the experience Europeans have developed in this field, we will keep sharing our knowledge and expertise to support all our partners across the globe.

Kaja Kallas,
EU High Representative
for Foreign Affairs and Security Policy
Vice-President of the European Commission

TABLE OF CONTENTS

GLOSSARY

Term	Explanation
FIMI	Foreign Information Manipulation and Interference (FIMI) describes 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 and is conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.
TTP(s)	In the context of FIMI, “Tactics, Techniques, and Procedures” are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. “Tactics” are the operational goals that threat actors are trying to accomplish. “Techniques” are actions through which they try to accomplish them. “Procedures” are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.
STIX	The Structured Threat Information Expression (STIX™) language is a data format used to encode and exchange cyber threat intelligence (CTI). It can also be used to share information on FIMI incidents, by breaking them down into their different constitutive elements.
Kill Chain	The term “kill chain” describes an end-to-end process, or the entire chain of events, that is required to perform a successful attack. Once an attack is understood and deconstructed into discrete phases, it allows defenders to map potential countermeasures against each one of these phases.
Response Framework to FIMI Threats	This framework is a systematic way of organising and conceptualising the analysis and response processes to FIMI. It merges two workflows: an analytical one providing information on the threat and a response one facilitating the decision-making process on countermeasures. The Response Framework relies on the assessment of potential risks and vulnerabilities extracted from the aggregated knowledge of past investigations. This enables preventive and reactive activities before, while and after an incident occurs.
Threat Actor	An organisation, a government, an individual or a group that poses a security risk by engaging in malicious activities, such as FIMI campaigns, cyberattacks or other harmful actions. Threat actors can have different motives, including financial gain, political influence, espionage or disruption.
Incident	A FIMI incident is an action perpetrated by one or more threat actor(s) pursuing specific objectives and carried out with the intent to deceive. It is composed of a combination of observables and TTPs. Multiple related incidents can be part of a campaign.
Coordinated Inauthentic Behaviour (CIB)	This involves organised, deliberate and manipulative efforts to mislead audiences by using multiple fake or inauthentic accounts. Generally, it includes networks of accounts and pages working together to spread certain messages or carry out specific actions while concealing their nature. CIB operations rely on the extensive use of manipulative tactics and techniques.
Campaign	A coherent set of FIMI incidents launched, over a certain period of time, against one or more targets with a unified objective and a potential narrative arc. One or more campaigns can be attributed to an IMS.
IMS	The term Information Manipulation Set (IMS) refers to the digital footprint of a persistent FIMI activity. An IMS can be defined as a collection of adversarial behaviours, tools, TTPs, and resources that is presumed to originate from the same threat actor, which may be unknown. An IMS should not be confused with the threat actor itself, which may consist of a state, organisation or individual. One or more IMSs can be technically attributed to a specific threat actor and one or more information campaigns (ICs) can be attributed to an IMS.
Infrastructure	A set of underlying technologies and services that make digital activity possible, for example a set of interlinked website domains operated by the same entities and designed to share traffic. An infrastructure can be part of an IMS.
Transnational Information Suppression (TIS)	The intentional action by threat actors and their proxies to suppress unwanted information with the aim to shape global narratives and norms in their favour. For this purpose, states apply a combination of technological, psychological, legal, and economic tactics. These tactics include active censorship measures and inducing self-censorship through systemic surveillance.

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.

Disclaimer_ The data used in this report are provided for informational purposes and are based on the EEAS' strategic monitoring activities and open-source research. The data presented reflect a selective, time-bound sample of observed activity associated, through public reporting or independent analytical attribution, with Foreign Information Manipulation and Interference (FIMI). The findings presented do not claim to be exhaustive or representative of overall FIMI activity and trends by the mentioned actors. The analysis is reflective of the authors' judgments at the time of publication and are subject to revision.

INTRODUCTION

In 2025, Foreign Information Manipulation and Interference (FIMI) reached a new level of operational complexity and global reach, with attacks increasing in frequency, intensity and coordination.

The weaponisation of the information space has become a persistent feature of today's international conflicts, reflecting increasing confrontation among major geopolitical powers. At the same time, the broader security context has deteriorated. Armed conflicts close to the borders of the European Union (EU) have not only persisted but escalated. Incidents involving drones and other incursions into EU territory have contributed to a climate of intimidation and uncertainty. **FIMI does not operate in isolation; it forms part of a broader hybrid arsenal combining digital interference with physical signalling and coercive actions.** It is, therefore, not merely a communication challenge but part of a broader strategy with tangible political and security consequences.

The EU faces FIMI attacks from more fronts, including in the technological domain. On the one hand, challenges related to the governance of global digital platforms and their role in shaping information flows continue to create structural vulnerabilities. On the other hand, **Artificial Intelligence (AI) is increasingly supercharging FIMI operations**, making them cheaper and easier to scale. In 2025, one in four detected incidents by the EEAS involved the use of AI tools to produce or distribute content.

In this context of escalation, the EU must also scale up its response work. Since 2015, **the EEAS has played a pivotal role in countering FIMI.** Building on successive EEAS Reports on FIMI Threats, the EEAS has developed a standardised analytical methodology to understand the threat, established a comprehensive FIMI Toolbox to respond to FIMI activities, and defined systems to link and attribute FIMI activities to threat actors.

On the basis of this experience, and in complementarity with the Democracy Shield, **the next step for the EEAS is to act as the operational "sword", translating analysis and coordination into responses with more tangible impact**.

The EEAS operational strategy sits on three mutually reinforcing pillars:

- **Faster responses**, enabled by improved data and operational coordination.
- **Scaled-up cooperation with partners**, strengthening joint capabilities to act across regions and domains.
- **Greater impact**, by shifting from reaction to anticipation and disrupting the infrastructures and incentives that sustain FIMI.

Under this third pillar (impact), this report presents the **FIMI Deterrence Playbook as a framework to generate tangible operational impact by making FIMI activity more costly and less sustainable for perpetrators**. This approach translates deterrence theory into operational practice for countering-FIMI and provides a structured pathway from analysis to impact. By linking FIMI operations to their financial, technical and organisational enablers, **the Playbook demonstrates how existing instruments in the FIMI Toolbox can be used as a deterrence measure** to constrain the long-term viability of information operations. It provides practical guidance on how sanctions, law enforcement, platform regulation and building resilience can be activated in a cumulative and targeted way to maximise impact.

This report is structured in three parts:

- **FIMI trends and findings in 2025:** The first chapter presents key data from the year, analysing the activities of 10,500 channels involved in 540 incidents. It provides a focused assessment of Russia's and China's activities and examines key developments, including the growing use of AI and patterns observed during electoral processes.
- **FIMI Deterrence Playbook:** The second chapter outlines how deterrence can be operationalised across different critical levels of the FIMI ecosystem. It identifies the structural vulnerabilities and enabling mechanisms that sustain FIMI operations and explains how these pressure points can be leveraged to increase costs, constrain capabilities and reduce the long-term viability of such activities, thereby generating greater operational impact.
- **The Galaxy of FIMI Operations in 2025:** The final chapter maps the interconnected layers of digital infrastructure that threat actors exploit to conduct FIMI operations. Through selected case studies — including on Ukraine and Armenia, as well as on the use of AI by Chinese networks — it illustrates how different operational components interact within a broader FIMI architecture.

This report **constitutes the most comprehensive mapping of FIMI activities in 2025**. It consolidates analytical findings, identifies systemic trends and provides an integrated assessment of the evolving threat landscape.

Beyond analysis, its added value lies in **demonstrating how existing instruments can be better coordinated, sequenced and operationalised to maximise impact.** The FIMI Deterrence Playbook provides a structured framework for increasing costs, constraining capabilities and reducing the long-term sustainability of FIMI activities.

An innovative element of this approach is the integration of additional operational avenues, including stronger links with law enforcement. **This expands the scope of action beyond defensive reaction and situates counter-FIMI efforts within a broader security framework.**

Finally, the report delivers an operational call to action. **Its full implementation requires sustained engagement and coordination with Member States and allies**, whose instruments and authorities are essential to ensuring credible deterrence and tangible impact.

1_FIMI TRENDS AND FINDINGS IN 2025

BLURRED LINES, GLOBAL EXPANSION

In 2025, continuous monitoring and data analysis efforts refined the EEAS' assessment of the global FIMI threat landscape.

Following a proven methodology – focusing on patterns and behaviours and infrastructures mapping – the EEAS is able to identify a number of overarching trends[i] .

First, **FIMI continues to evolve alongside technological progress, particularly in the field of Artificial Intelligence (AI).** This evolution is visible in content itself: synthetic audio and video, as well as AI-generated text, have become a daily and cost-effective tool in threat actors' arsenal. AI also enables mass distribution of content and translation across multiple languages, significantly expanding reach and potential impact.

Second, **FIMI operations are becoming increasingly covert and combining different fields** (information space, physical space, cyber space)[ii]. State threat actors and their proxies are scaling up and expanding existing networks of deceptive assets designed to conceal their real origin. This is reflected in the near-continuous creation of inauthentic "news" outlets, fabricated social media profiles, and online personas.

Finally, while this arena is often framed as mainly virtual, **FIMI remains deeply anchored to a physical dimension** - through concrete events, such as elections, and shaped by the targeting of specific socio-demographic groups and individuals. Besides the information environment itself, FIMI aims at shaping perceptions and influencing behaviour towards very concrete events, actions or individuals.

Overall, **FIMI is deliberate and pursues clear strategic objectives on a broader scale.** The recurring patterns, the Tactics, Techniques and Procedures (TTPs) observed reveal how threat actors keep weaponising information as a key component of their wider hybrid arsenal. The choice of targets - whether countries, key events or specific individuals - is a sign of deliberate and structural planning.

It demonstrates a **high level of adaptability, with campaigns tailored to specific regional contexts while serving global strategic objectives.** One illustrative case of 2025 is the pivot of the Russian FIMI infrastructure focus on the Moldova parliamentary elections towards the Armenia parliamentary elections scheduled in June 2026, which will be analysed further in this report.

The following section provides a global overview of the main trends the EEAS observed in FIMI threats over the last year, focusing on certain key topics, such as AI or election interference, through the lens of Russia and China as threat actors.

i. Identified trends should not be interpreted as exhaustive, as the analysis remains shaped by the focus and scope of monitoring efforts. The empirical data in this report is derived from the EEAS strategic FIMI monitoring efforts. As the EEAS does not cover all regions or languages, this report reflects only a limited portion of threat actors' activities. The scope of FIMI operations could extend far beyond what is represented here. All the incidents included in this report have been encoded in the Structured Threat Information Expression (STIX) format, a standardised language to express and share threat intelligence information in a readable and consistent way.

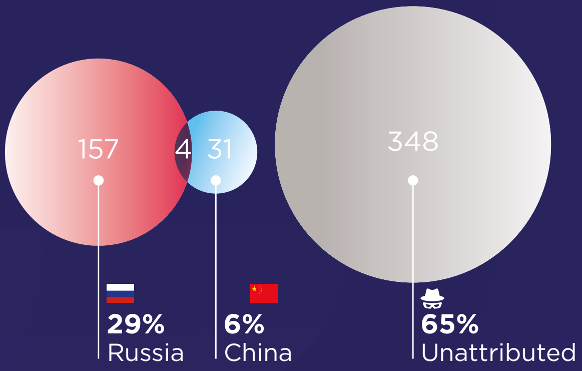
ii. FIMI incidents that would imply for example actions of sabotage, or military/security incidents (such as drones' incursions) supported by information campaigns, based on fabricated content and assets, to alter perceptions of said actions and reality.

2025 FIMI IN NUMBERS

540 incidents

The EEAS detected and analysed 540 FIMI incidents between January 1st and December 31st, 2025. Within this sample, 29% of incidents were attributed to Russia, while 6% were connected to China. On rare occasions, both Russia's and China's FIMI infrastructures worked in unison, mostly in the form of opportunistic amplification of each other's content.

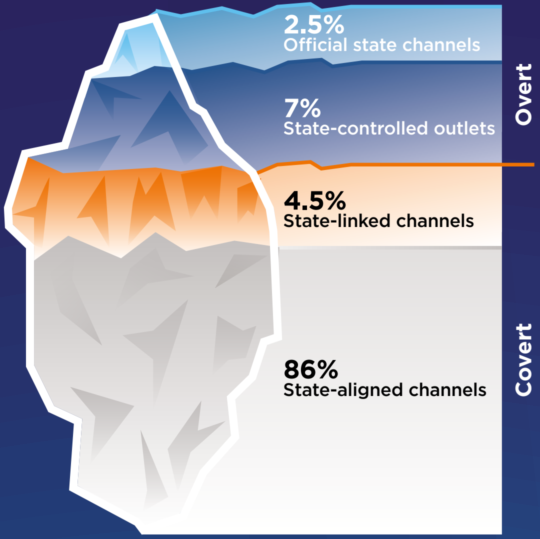
65% of all incidents recorded remain unattributed, but present indicators of coordination with FIMI assets linked to Russian or Chinese attributed infrastructures. The assets involved are deceptive by nature, hiding their operators and funding. As a result, identifying and investigating the behaviours and infrastructure behind unattributed FIMI assets is key to exposing the underlying threat.



10 500 channels

10 500 unique channels were involved in detected FIMI incidents over the last year, ranging from fabricated news websites to social media accounts or blogs, resulting in cross-platform activity and coordination between multiple assets of the FIMI ecosystem.

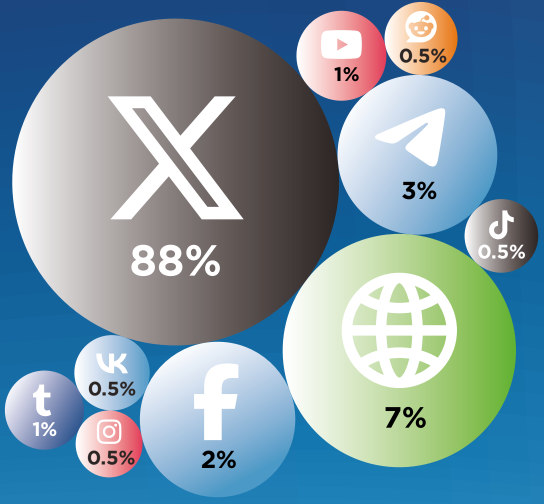
A sample of approximately 3000 of the most recurrent assets was mapped and characterized to be shown in the network graphs at pages 26 and 27**.** As illustrated in the iceberg infographic, 9,5% of these channels are directly related to a state actor (official or state-controlled sources).The vast majority (90,5%) consists of covert assets that are linked to or aligned with a threat actor, with the latter category remaining unattributed. In other words, the biggest part of FIMI infrastructures is hidden or inauthentic (including CIB networks, for instance). Therefore, exposing the connections behind covert FIMI sources remains crucial to mitigating their potential impact.



** Percentages based on the 3000 most recurrent channels*

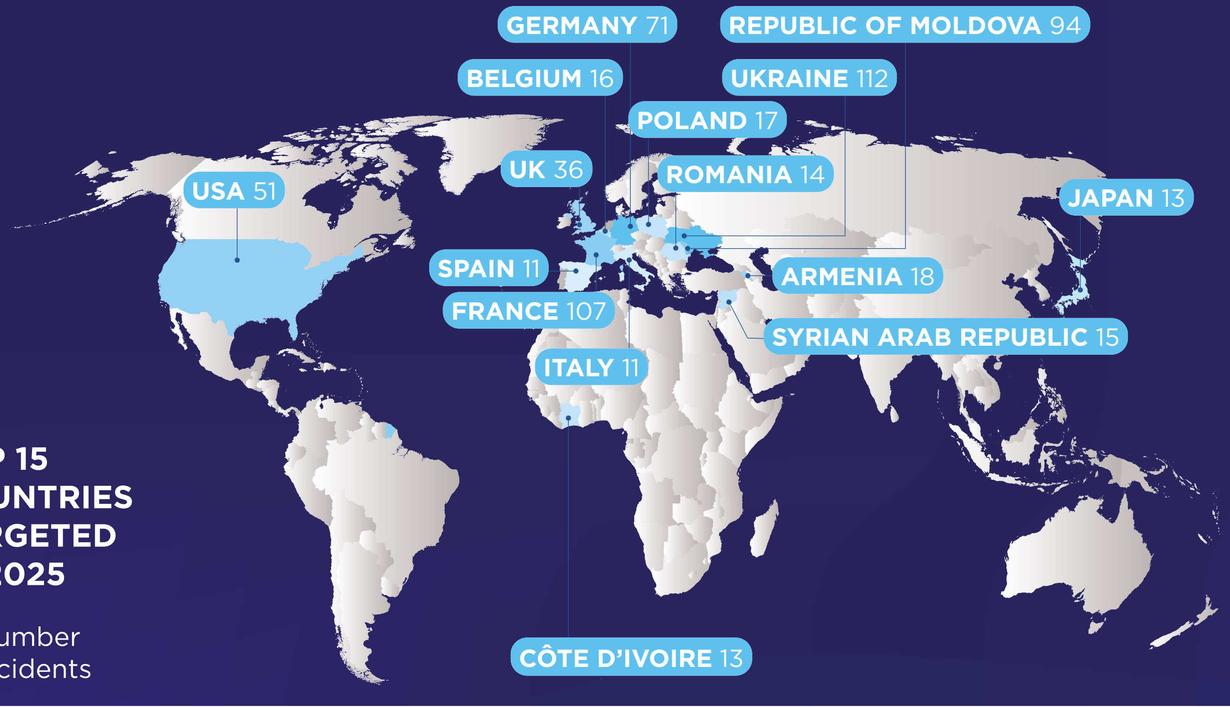
43 000 observables

In 2025, a total of about 43 000 observables (pieces of content such as texts, audios, videos) were recorded on 19 different unique platforms. Social media and messaging platforms remain the most cost-effective means to reach large audiences worldwide. Most of FIMI incidents involve cross-posted content by multiple accounts on various platforms. The objective is to permeate the information space to expand visibility and perceived credibility of the content, while targeting specific audiences on the basis of socio-demographic and geographic factors. For example, many incidents targeting Ukraine and Eastern Europe are found on Telegram, one of the most popular messaging platforms in this area. Facebook groups and pages are often used in incidents targeting specific African countries and audiences. Similarly to previous trends, 88% of instances were concentrated on the platform X. The presence of CIB networks, the ease of creation of fabricated accounts, but also more straightforward access to data explains this concentration. Most of the major social media platforms restrain the access to data that would allow to assess the magnitude of information manipulation activities.



Top 10 platforms by volume of observables

TARGETS OF FIMI
THE THREAT LANDSCAPE



TOP 15 COUNTRIES TARGETED IN 2025

by number of incidents

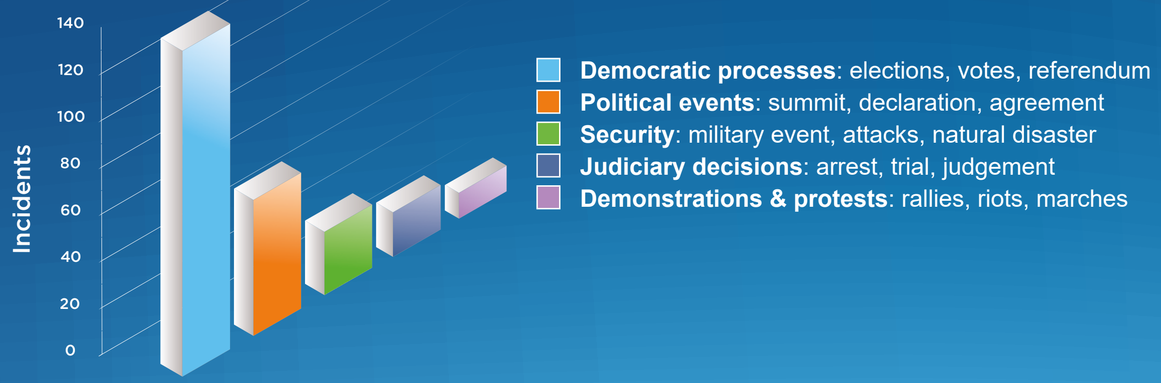
Countries

In 2025, FIMI remained a global threat, impacting and destabilising all regions the world with more than 100 countries targeted. Nontheless, within the EEAS monitoring perimeter, some countries were especially attacked. In Eastern Europe, while Ukraine remains at the heart of Russian hybrid war efforts, Moldova appeared as one of the key priorities of the Kremlin in 2025, considering the parliamentary elections held in October 2025. Following a similar pattern, Armenia is increasingly targeted by FIMI incidents in the context of the upcoming elections in 2026.

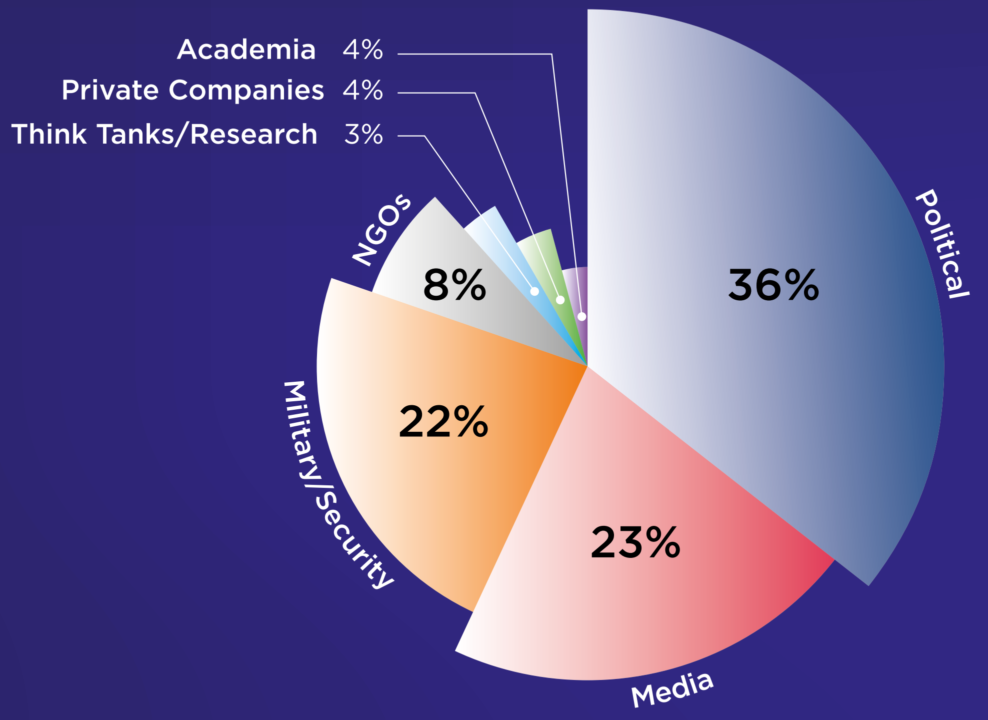
Many EU Member States, such as France, Germany, Poland, Belgium, Italy and Spain, and key partners such as the United Kingdom, were frequently attacked too. The support to Ukraine against the Russian full-scale invasion since 2022, major electoral events such as the German legislative elections, and even the transatlantic relationships were all topics strategically exploited by the threat actors.

Events

Nearly half the recorded incidents were triggered by specific events, especially breaking-news events or electoral processes that provide fertile ground for information manipulation. Major democratic processes such as the Moldovan parliamentary elections were highly anticipated events by the attackers. Likewise, popular demonstrations and riots were exploited throughout the year to amplify perceptions of chaos, fear and disorder, usually against local administrations. High stakes, emotionally charged moments, are seen by threat actors as vulnerabilities that help them reach their target audiences, and help them influence these audiences' reasoning or amplify existing cognitive biases.



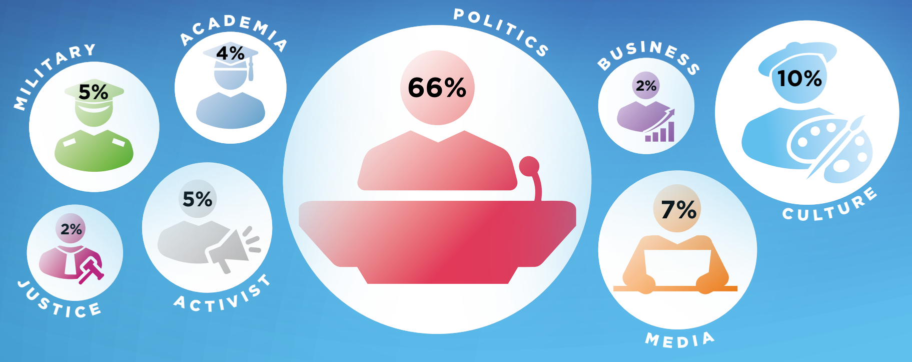
- 🟦 **Democratic processes**: elections, votes, referendum
- 🟧 **Political events**: summit, declaration, agreement
- 🟩 **Security**: military event, attacks, natural disaster
- 🟦 **Judiciary decisions**: arrest, trial, judgement
- 🟪 **Demonstrations & protests**: rallies, riots, marches



Organizations

Around 200 different organizations were targeted in FIMI incidents last year. Their diverse types reflect the multi-level targeting strategy of perpetrators: national governments and political figures, international institutions, traditional media and newspapers, non-governmental organisations, including humanitarian organisations, or even academia.

The political and security sectors - European military forces, intelligence agencies, and police services - were especially targeted, in order to undermine confidence in defence capabilities among target audiences. Similarly, threat actors identified the media sector as critical for democracies, and therefore targeted it with degrading narratives, impersonation attempts, or direct smearing campaigns. Attacks against media play on existing and enduring distrust, so as to exacerbate the increasing disorder in information accessed by target audiences.



Individuals

Near 140 different individuals have been targeted by FIMI incidents in 2025. Most of them are political figures: head of states and public institutions - such as Maia Sandu, Volodymyr Zelensky, Emmanuel Macron, Friedrich Merz, Ursula Von Der Leyen, or Kaja Kallas. Attackers also focused their efforts on diplomatics corps and national representatives to international institutions, such as NATO, aiming to weaken their reputation.

In most cases, personal attacks are an attack on what an individual represents (such as democratic values, principles, or as a perceived adversary), as well as a way to instrumentalise their platform to reach specific audiences.

RUSSIA AS A THREAT ACTOR IN 2025

Russia continues to use FIMI as one of its core instruments of state power, fully integrated into its broader strategic and hybrid toolkit. In 2025, Russia's central priorities continued to be its war of aggression against Ukraine and targeting Ukraine's international partners. Significant FIMI activities were accompanied by escalatory hybrid actions including drone incursions, acts of sabotage, and attacks on critical infrastructure in EU countries such as Poland, Romania, Lithuania and Estonia. These incidents were accompanied by FIMI designed to manage public perception and test responses.

Over the past year, Russian FIMI campaigns underwent a strategic recalibration, shifting from a parallel focus on the EU and the United States to a more concentrated emphasis on Europe, while keeping some room for manoeuvre.

Russian FIMI actors focussed on the EU as an adversary, showed inconsistency regarding the US, and portrayed itself as an alternative to a supposedly morally decadent West and a guarantor of a "multipolar world order".

The Kremlin's FIMI apparatus combines overt and covert means that heavily rely on tailoring their operations to specific audiences. The main approach remains consistent – to sow new or deepen existing divisions (figure 8). Russian FIMI actors also try to mobilise anti-establishment sentiments, by undermining trust in the EU, portraying it as either undemocratic and aggressive, or too weak. EU leaders and institutions are frequently targeted, while initiatives such as the EU Democracy Shield are portrayed as authoritarian.

Elections remained a primary target, utilising country-specific FIMI narratives. For instance, in Czechia, hundreds of anonymous TikTok accounts spread pro-Kremlin narratives ahead of the parliamentary elections, while the Moldovan parliamentary elections faced an unprecedented wave of hybrid threats and FIMI[1].

To counter Russian FIMI, the EU expanded its hybrid sanctions regime to target the networks, assets, and enablers behind such activities. This shift reflects a more coordinated effort to disrupt operational capacity[2], while EUvsDisinfo continued to expose and debunk Russian FIMI narratives.

Domestically, the Kremlin continues its efforts to reinforce regime legitimacy and military support for Russia's war of aggression against Ukraine. Expanded foreign agent, extremist, treason and terrorism legislation is systematically used to suppress independent journalism and dissent. More than 1,000 individuals and organisations have been targeted under this legislation, facing asset freezes and lengthy prison sentences, while opposition to the war against Ukraine is being increasingly prosecuted as 'justification of terrorism'.[3] Authorities have also introduced fines for searching for so-called 'extremist' content online.[4] The Kremlin continued to consolidate control over the domestic information environment through the promotion of state-sponsored platforms such as Max and RuTube, while the latest slew of domestic restrictions on WhatsApp, YouTube and Telegram have further isolated Russian audiences.

Russian state institutions continue to play a key part in FIMI activities. The Foreign Intelligence Service (SVR) has taken on a more visible role, issuing official statements containing false or unsubstantiated claims that are later amplified across FIMI networks. In 2025, this included false allegations of EU and NATO-backed plots to destabilise Moldova, Serbia, and Georgia.

In 2026, Russian FIMI activity is likely to intensify further. Funding for FIMI is set to rise as part of the budget increase for state-controlled media, which is set to reach 146.3 billion roubles (approximately 1.56 billion EUR) in 2026[5], 7% higher than in 2025. It is anticipated that the Baltic Sea[6] and the Arctic[7] regions will be among the targets in the information space. Additionally, it is highly likely that Russia will continue with its efforts to strengthen its role in different regions in the world. Namely, the third Russia-Africa Summit is likely to be used to reiterate arguments about the multipolar world, and degradation of the EU and the West. The Kremlin's previous funding for covert FIMI operations in Africa and Latin America[8] show that these regions will remain among their priorities.

Elections are expected to remain key targets for Russian FIMI, both in the EU and its neighbourhood, including Armenia. The objective will continue to be sowing and deepening societal divisions and undermining political processes deemed to be a threat to Russian interests, in particular EU accession, support for Ukraine and efforts to strengthen EU defence capabilities and readiness.

Other observed trends, such as the reliance on AI-enabled content, continuous use of FIMI alongside other hybrid tactics, and even further tightening of domestic censorship are expected to continue.

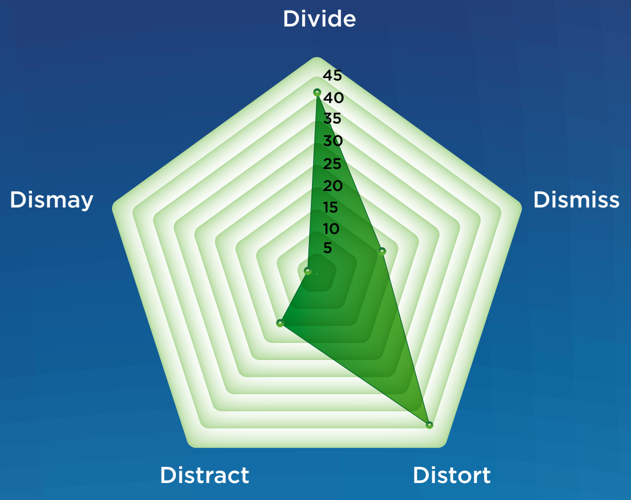


Figure 8_5Ds radar of Russia's strategic objectives. Russia's strategic objectives throughout the attributed incidents in 2025 show a clear tendency towards the use of the techniques of distorting[9] and dividing[10]. Distorting TTPs reframe how existing information or artefacts are presented, while Dividing TTPs focus on widening divisions within society.

CHINA AS A THREAT ACTOR IN 2025

In the current geopolitical and geo-economic context, **China aims to present itself as a reliable global power, while simultaneously reducing Western global influence** (e.g. in international relations, global governance norms, and technology standards).

Throughout 2025, **China** continued its multifaceted FIMI activities, deploying a broad range of tactics. This comprised of **not only the spreading of conspiracy narratives and the expansion of its global FIMI infrastructure, but also more aggressive measures such as intimidation and harassment of critical voices** to suppress information even outside of its borders. Different tactics are often used in combination and can be **connected** to **wider hybrid campaigns**.

China's FIMI infrastructure continued to strengthen the use of tools such as AI to obfuscate content's origin, amplify its reach, distance content from its state-linked origins while increasing its distribution credibility and visibility.

Transnational Information Suppression (TIS)[iii] remains a key concern in detecting and responding to Chinese FIMI. Often overlooked and difficult to track, as both threats and incentives aim to induce wide-spread self-censorship, information suppression manipulates the information environment by silencing authentic critical voices. Instead, China fills that space with content considered favourable and in alignment with its strategic objectives. By targeting media, businesses, civil society, academia and even governments, but also (diaspora) individuals and their families, information suppression straddles the policy areas of FIMI, human rights, and broader non-traditional security. A broad network of agents, proxies, and assets can be deployed to exert economic, legal, psychological, and/or tech-enabled pressure. **Due to its cross-domain and often clandestine nature, identifying TIS' main TTPs, understanding their scope and impact remains a challenge.** Shaping deterrence, disruption, and mitigation mechanisms against TIS will require a whole-of-society approach and a strong international partnership.

The most common narratives in 2025 remained largely similar to those observed in 2024. **Chinese efforts to project a positive image abroad intensified, aiming to position China as a force for peace, 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" e.g. as cynical and or aggressive.

The narrative portraying the EU as subservient to the US in terms of foreign policy (e.g. on Gaza, Ukraine) remained, but this year also included criticism of the EU leadership as hawkish on China, as well as on Russia, Iran, and the DPRK. The change of US trade policy was used to **deploy narratives calling for closer cooperation between the EU and China in setting up a new multilateral order**. This narrative was particularly prominent around the EU-China Leaders' Summit in July. **The so-called big four topics (Taiwan, Hong Kong, Xinjiang, and Tibet) featured heavily**, primarily through defensive posture on human rights abuses in Xinjiang and Tibet. Hong Kong, Taiwan, and the situation in the South China Sea were used in conjunction with promoting China's concepts and views on sovereignty and territorial claims. The ecosystem continued presenting Russia's war against Ukraine and Ukraine's accession to the EU as a source of division.

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-posting between the two seems to remain largely opportunistic.** For instance, a number of Chinese outlets provided a platform for Russian voices in particular in the context of the Shanghai Cooperation Organisation summit and the Victory Day commemorations.

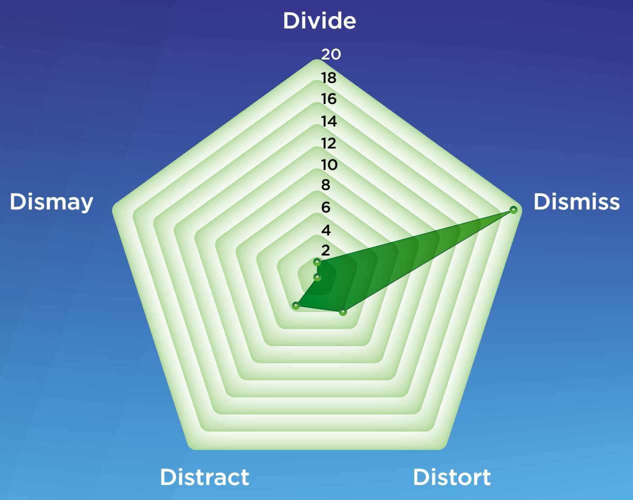
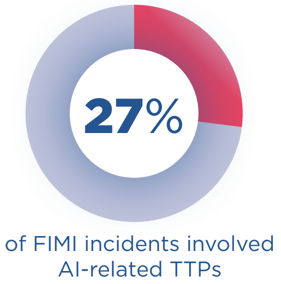


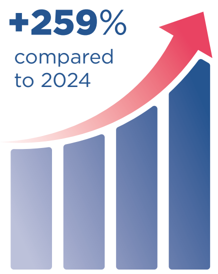
Figure 9_5Ds radar of China's strategic objective. China's strategic objectives throughout the attributed incidents in 2025 show a clear tendency towards the use of the technique of dismissing[11], which consists in arguing that criticisms of China are biased, and promoting its propaganda narratives.

[iii] Transnational Information Suppression: the intentional action by threat actors and their proxies to suppress unwanted information with the aim to shape global narratives and norms in their favour. For this purpose, states apply a combination of technological, psychological, legal, and economic tactics. These tactics include active censorship measures and inducing self-censorship through systemic surveillance.

AI-ENHANCED FIMI ACTIVITIES

In 2025, **27% of the incidents detected by the EEAS involved AI-related TTPs**. **This marks a significant rise compared to 2024**, increasing from 41 to 147 cases — **a growth of approximately 259%**. Russian and Chinese FIMI actors have fully embedded AI tools into their FIMI operations, to **accelerate their content production and scale up influence activities with fewer resources**. These dynamics are examined more closely in chapter 3, which looks at concrete examples linked to Chinese and Russian networks.





AI POWERED CONTENT CREATION & DISTRIBUTION

Threat actors rely on AI tools in different ways to create written content at scale and make it easy to spread the same message across many languages at once. The texts use near-identical templates, reflecting a uniform style across languages. AI-generated original posts and comments are frequently disseminated by Coordinated Inauthentic Behaviour (CIB) accounts on social media, while AI articles are promoted by fabricated news sites (such as the Russian RRN network). AI tools are also used to **rephrase, translate, and adapt existing text from other sources**. In 2025, many FIMI incidents involved the impersonation of Western news outlets, whose content was reshaped into partisan narratives and distributed through inauthentic networks, such as Storm-1516[12]. In other cases, messages from state-controlled outlets were laundered through intermediary sites to hide their original source (for example, content linked to Chinese CGTN).

The use of synthetic audio is no longer experimental. It has become a standard technique used in the production of videos. In 2025, **threat actors moved beyond generic AI voiceovers to advanced voice cloning**, such as in the case of videos produced by Operation Overload and Storm-1516.

AI powered videos, ranging from AI-assisted to fully generated content, **to impersonate specific individuals are becoming increasingly sophisticated and credible**. For example, this technique was particularly used during the Moldovan elections. Similarly, **threat actors relied extensively on synthetic imagery to create emotional content and strengthen the visual credibility of inauthentic assets.** AI-generated photography, cartoons or logos improved the aesthetic quality and perceived authenticity of websites and fake social media accounts. For example, during the German legislative elections, Russian CIB accounts widely shared AI-generated images portraying apocalyptic versions of German landscapes engulfed in chaos and crime, aiming to discredit a specific party while promoting its opponents.

Instead of carefully targeting a single audience, AI tools are deployed at scale to keep a steady stream of content flowing. **The objective is not precision but presence,** ensuring that narratives are constantly circulating, even without clearly defined targets.

KEY CHALLENGES AND TRENDS

The growing quality, scale and apparent credibility of **AI-powered information manipulation challenge audiences' ability to distinguish reliable information from fabricated content**. By repeatedly exposing users to emotionally charged AI visuals, threat actors amplify cognitive chaos and erode the very principle of trust in the information environment.

Some widely used AI tools are themselves becoming targets. For example, one of the most prolific Russian FIMI infrastructure, Portal Kombat is suspected of conducting Large Language Model (LLM) grooming[13], flooding the information space with low-quality multilingual content in an effort to influence AI training data and inject false or manipulative claims disguised as sources of reliable information.

Despite this expansion, much of the AI-generated material in 2025 remains low-quality. Threat actors prioritise quantity over quality, resulting in limited overall impact as organic engagement remains low. For example, Storm-1516 and Overload use AI-generated videos easily identifiable as inauthentic by average viewers, resulting in low overall impact and limited engagement metrics.

AUTOMATED CONTENT CREATION	LARGE SCALE DISTRIBUTION	KEY CHALLENGES
Generative text Articles, social posts, comments	**CIB network** Bot accounts, fake personas	**Algorithm Influence** High volume of content and engagement may artificially push fabricated content in feeds
Synthetic audio & video Impersonation, voice cloning	**Mass production** High volume of content, adapted and replicated or simply copy/pasted to reach higher visibility	**LLM grooming** Influence generative AI sources of information
Synthetic imagery Photos, infographic, cartoons	**Translation, adaptation, replication** Reaching different audiences in various languages anywhere in the world	**Cognitive chaos** Erodes trust in sources of information, pollutes the information environment

Figure 11_Artificial Intelligence in FIMI

THE RUSSIAN FIMI PLAYBOOK TO TARGET ELECTIONS

Based on EEAS monitoring during the reporting period, **elections once again emerged as primary targets of Russian FIMI activity**. Within the scope of the analysis, Russia targeted electoral processes in Germany, Poland, Romania, Moldova, the Czech Republic, and Côte d'Ivoire. The threat actor mobilised its full media infrastructure (including official channels, state-controlled media, Information Manipulation Sets[14], and local proxies) to target elections in line with its geopolitical objectives.

The cases analysed in 2025 **confirm patterns documented over the years in previous elections** and consolidate the phased logic described in the 2nd EEAS Report on FIMI Threats[15]. These **patterns have become the playbook for Russian FIMI used in elections, a repetitive and predictable playbook that can be anticipated and addressed in advance.**

Despite contextual differences and varying levels of sophistication, Russia repeatedly followed a three-stage operational logic:

Phase 1_Control of the information space and delegitimisation of political leadership months before the elections:

After attempting to consolidate its presence in the information space through its own communication channels, Russia launches campaigns months before election day to discredit pro-EU candidates or incumbents and erode trust in their leadership. They rely on recurring allegations of corruption, political repression, health-related issues or often portraying local leaders as subordinated to EU interests. This pattern was evident in Moldova targeting President Maia Sandu and Prime Minister Dorin Recean. The same also emerged ahead of the German elections, targeting Olaf Scholz, Robert Habeck and Friedrich Merz, and was similarly replicated in Poland and Romania. These offensive campaigns often ran alongside the selective promotion of alternative political options.

Phase 2_Weaponising domestic divisions during electoral campaigns:

As elections approach, the Russian FIMI apparatus exploits domestic issues, expanding its targets to state institutions to deepen existing divisions and polarisation. In Germany, this centred on immigration; in Poland, on anti-refugee sentiment; and in Moldova, on allegations of censorship, protests and strikes, and fabricated claims of imminent war with Russia. In both Germany and Moldova, economic and energy issues were also used to blame incumbent governments for perceived failures.

Phase 3_Late-stage undermining of electoral integrity:

It unfolds in the weeks before election day and intensifies during the vote, seeking to discredit electoral integrity and encouraging abstention. In Germany and Poland, fearmongering content amplified warnings of security threats and alleged terrorist attacks on election day.

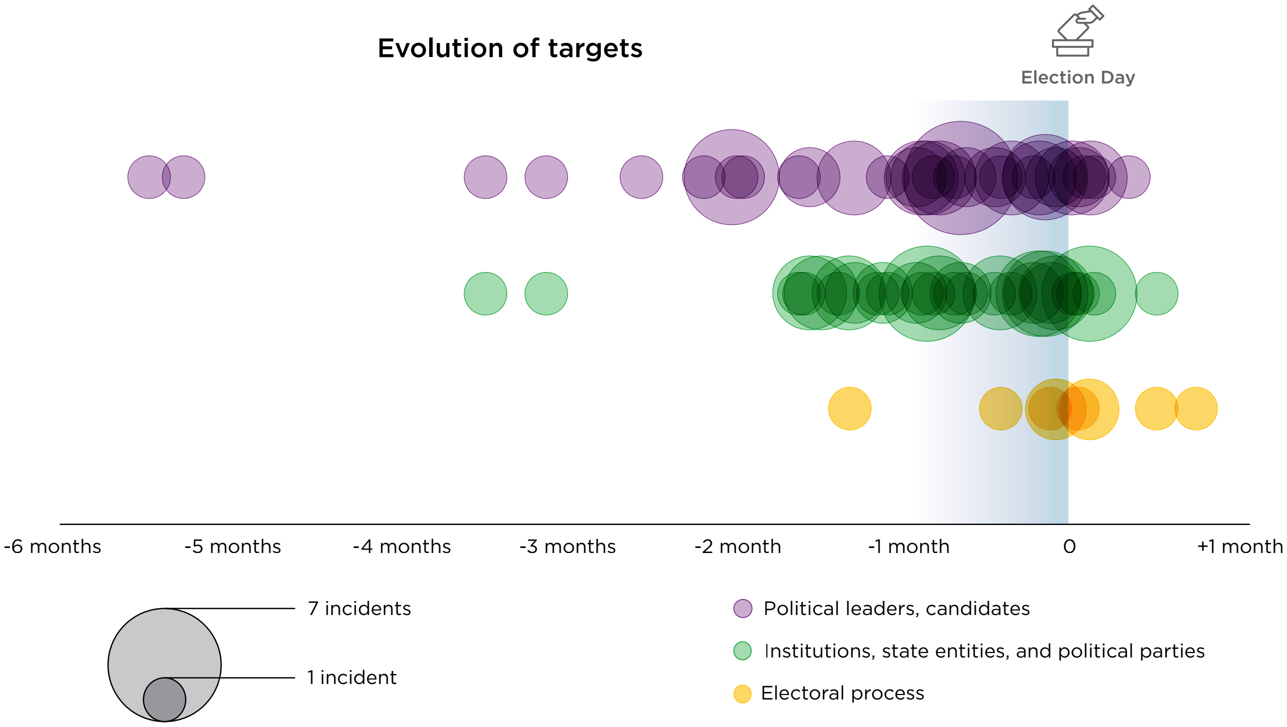


***Figure 12**_Phases and progression of FIMI threats targeting elections in 2025*

2_FROM THREAT ASSESSMENT TO DETERRENCE: RAISING THE COSTS AND REVERSING THE IMPACT

The first chapter of this report offers a comprehensive threat assessment, identifying some overarching FIMI trends, actors and potential evolutions. However, this is only the **first step leading to a concrete counter-measure methodology making the best use of existing tools**, and underlining the efforts remaining, to build proactive defence and systemic resilience.

The next chapter will focus on consolidating existing elements of response into **a deterrence playbook**, which is a matrix to rationalise, coordinate and complement different actions designed to hit the vulnerabilities of the FIMI supply-chain.

FIMI actors have contributed to the emergence of “FIMI-as-a-service”: a **multi-layered business ecosystem in which activities are planned, financed, and subcontracted**, supporting the entire threat actor strategy. After numerous reports on this issue by the FIMI defender community, it is clear that FIMI operates as an industry. Effective deterrence requires prioritising and operationalising measures that lead to a negative cost–benefit ratio for the perpetrators. The following sections present a **scalable deterrence playbook to raise costs for the attackers and tackle the foundations of FIMI operations.**

Democratic institutions across the EU and other like-minded partners already have several sets of instruments to address FIMI. Legal, diplomatic, economic and technical tools provide a strong foundation to address the threat. Yet the threat landscape continues to evolve, requiring not only **improved use of existing mechanisms but also their adaptation and**, where necessary, **the development of new ones**.

When hostile actions do not trigger consequences, they risk becoming normalised[16]. **A stronger deterrence posture is therefore required not to escalate, but to ensure accountability.** Those who attempt to manipulate the information environment should face constraints, exposure and an increase in costs. **Making such activities more difficult, less effective and riskier for perpetrators is central to protecting democratic systems.**

INTEGRATING DETERRENCE INTO THE FIMI TOOLBOX

Deterrence "*is the ability to alter an actor's cost-benefit calculus so they decide against taking an undesired action*"[17]. The concept is equally applied in different domains, including criminology, security, law enforcement, cyber, and regulatory policy.

Deterrence represents a shift in the operational model for countering FIMI. Instead of remaining predominantly reactive to incidents and responding on the terms set by threat actors, it redirects our actions earlier in the chain of activity. **The focus moves from reaction to anticipation**, thereby proactively constraining threat actors' capabilities, exploiting their vulnerabilities and guiding the trajectory of hostile activity before it can happen at scale.

Adding a deterrence dimension does not replace existing efforts. The full range of instruments within the FIMI Toolbox, including situational awareness, legal preparedness and societal resilience, remains essential. Countering FIMI continues to require a whole-of-society approach. However, these existing efforts must now be complemented by a more assertive layer of action. **Deterrence requires prioritising and operationalising those elements within the FIMI Toolbox that can directly affect perpetrators' cost–benefit calculations.**

Deterrence applied to countering FIMI:
Proactive, agile, multidomain, tailored and cumulative

Building on the FIMI analytical methodology[18] and FIMI response Toolbox[19] (detailed in previous EEAS reports on FIMI Threats) and lessons learnt from the Hybrid and the Cyber Diplomacy toolboxes, the **EEAS proposes the FIMI Deterrence Playbook as the new instrument to increase the impact of our actions**. The Playbook guides the coordinated activation of tools capable of disrupting — and ultimately preventing — the strategic, financial and logistical flows that sustain FIMI activities.

It seeks not only to stop individual operations, but also to shape future behaviour by forcing threat actors to reassess and modify their tactics — making it more difficult to operate, discouraging repetition and signalling to other potential actors that such activities will no longer remain low-risk. Deterrence, in this sense, **is not a one-off response but a structured sequence of actions with cumulative impact**[20]: that applies consistent pressure over time and **can be reinforced through alliances and partnerships**.

In practical terms, the FIMI Deterrence Playbook is designed to:

- **Raise costs and risks[21] for threat actors**, ensuring that manipulation no longer represents a favourable cost–benefit calculation.
- **Isolate and constrain operational space**, narrowing the room for manoeuvre.
- **Target critical capabilities**, striking at the "nerves" of the FIMI architecture, including organisational networks, financial flows, operators and technical infrastructure.
- **Push perpetrators to reshape their strategy[22]**, compelling adaptation, increasing uncertainty and forcing them to waste time and resources trying to rebuild infrastructure.
- **Delegitimise threat actors**, reducing their credibility and influence.

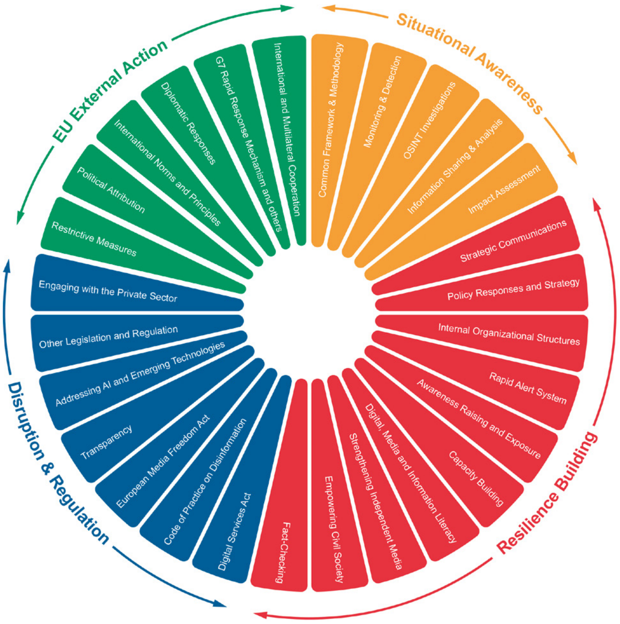

EU External Action
International and Multilateral Cooperation
G7 Rapid Response Mechanism and others
Diplomatic Responses
International Norms and Principles
Political Attribution
Restrictive Measures
Situational Awareness
Common Framework & Methodology
Monitoring & Detection
OSINT Investigations
Information Sharing & Analysis
Impact Assessment
Resilience Building
Strategic Communications
Policy Responses and Strategy
Internal Organizational Structures
Rapid Alert System
Awareness Raising and Exposure
Capacity Building
Digital, Media and Information Literacy
Strengthening Independent Media
Empowering Civil Society
Fact-Checking
Disruption & Regulation
Digital Services Act
Code of Practice on Disinformation
European Media Freedom Act
Transparency
Addressing AI and Emerging Technologies
Other Legislation and Regulation
Engaging with the Private Sector

***Figure 13**_FIMI Toolbox*

DISMANTLING THE FIMI HOUSE OF CARDS

FIMI must be understood not as a communication problem, but as a security issue with structured supply-chain system. As reflected in the FIMI Exposure Matrix[23], threat actors operate through a multi-layered digital ecosystem — a visible surface composed of websites, channels and amplification networks. Yet this digital layer is only the outer shell. Beneath it lies a broader physical and decentralised architecture within which state-actors are the orchestrators[24].

The FIMI architecture functions as a vertical system. At its foundation are the threat actors who plan and finance operations. Above them, intermediaries and proxies turn strategy into concrete actions, using digital and technical infrastructure to produce and amplify content. Each layer is interconnected, and what we see at the surface depends on what is organised underneath. Understanding this layered structure is essential for analysis and attribution[25], as it allows to tailor deterrence measures to specific levels within the FIMI architecture. **By using the FIMI Toolbox to strike at keystones of the configuration, the rest of the structure collapses.**

FIMI operations cut across financial systems, legal frameworks, technical infrastructure and business networks. **Our actions must therefore also be multidomain**. If information is exchanged only within the same analytical circles, there is a risk of repeating the same findings without expanding the response options. But when FIMI analysis is connected , for example, with law enforcement, regulatory authorities and financial investigations, new pieces of the puzzle emerge, thereby enabling stronger attribution, disruption of money flows and action against the supporting infrastructure.

This **multidomain approach must be data-driven.** Situational awareness, particularly the early identification of emerging threats, **enables decision-makers to determine where deterrence measures are required**[26].

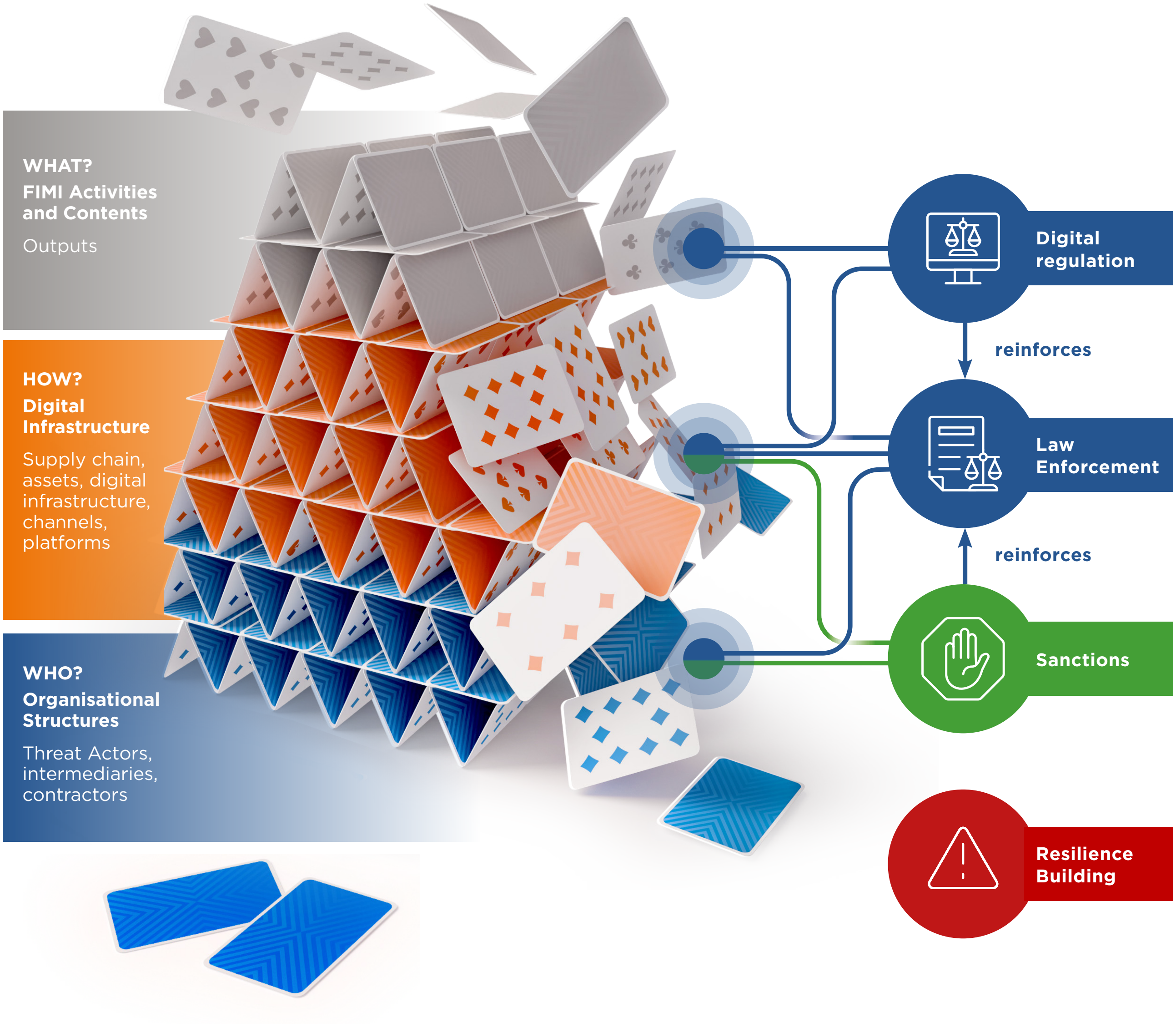

WHAT?
FIMI Activities and Contents
Outputs
HOW?
Digital Infrastructure
Supply chain, assets, digital infrastructure, channels, platforms
WHO?
Organisational Structures
Threat Actors, intermediaries, contractors
Digital regulation
reinforces
Law Enforcement
reinforces
Sanctions
Resilience Building

Figure 14_*Layers of the architecture of FIMI threats and deterrence mechanisms included in the FIMI Toolbox*

Within the FIMI Toolbox, four instruments offer clear deterrence potential:

SANCTIONS

SANCTIONS: Sanctions are restrictive measures that prohibit, for example, the provision of resources and services to individuals or entities involved in FIMI activities. They do not regulate content creation or criminalise speech, instead they **target the actors and economic and technological structures that sustain operations**, with any impact on dissemination resulting indirectly from upstream restrictions. They can be applied when **FIMI-related activities fall within an existing EU sanctions regime** — such as foreign interference, destabilising activities or human rights violations — and when responsible actors can be identified. **Sanctions are imposed at EU level through a political and administrative process,** not a criminal justice one. When listing criteria are met, and political consensus between Member States is achieved, the Council of the European Union adopts designations unanimously based on attribution, intelligence and diplomatic assessment. The Council adopts the measures that become binding across Member States and require compliance by public authorities and private actors. Depending on the measure, this can result in **asset freezes, travel bans and denial of financial, technical and other services** — constraining the resources and reach of the targeted actors *(See Annex 1)*.

LAW ENFORCEMENT

Including law enforcement and judicial measures in the FIMI Toolbox makes it possible to **connect FIMI-related conduct to criminal or administrative offences under EU and/or Member States' law**. This may include fraud, illegal financing, cybercrime or other criminal activity, depending on national legislation. These measures do not target narratives as such, but unlawful conduct linked to influence operations. **Regulatory frameworks such as the Digital Services Act (DSA) and EU sanctions regimes can help to provide the legal basis** for law enforcement.

Law enforcement is activated when information or intelligence indicates a potential offence. Triggers may come from investigations, intelligence reporting, victim complaints, regulatory referrals, or cooperation with platforms and financial institutions. Police and specialised units collect evidence, and judicial authorities enable measures. The results may include **asset seizure, dismantling of organisational structures and direct disruption of operations, arrests, and prosecution for criminal proceedings.** *(See Annex 2)***.**

DIGITAL REGULATION

Digital regulation deters FIMI operations by **reducing their visibility, scalability and sustainability within platform environments**. It operates through the **enforcement of platforms' Terms of Service, as well as through regulatory oversight such as the DSA**.

Digital regulation is activated through platform data, user reports, research findings or regulatory monitoring. By flagging violations — including coordinated manipulation, inauthentic behaviour or illegal content — platforms enforce their Terms of Service through account removal, limits on amplification or demonetisation. Under the DSA, the focus is not on regulating narratives, but on addressing structural platform-level failures that allow illegal content or systemic risks. Digital Services Coordinators and the European Commission supervise compliance, and platforms that fail to meet their obligations may face significant fines. Together, these mechanisms make **FIMI infrastructure unstable, costly, short-lived and harder to scale, reducing reach and disrupting operations without requiring criminal proceedings.** *(See Annex 3).*

BUILDING RESILIENCE

Building resilience **scales up society's ability to recognise, assess and respond to manipulation**. It combines public exposure, strategic communication, media literacy and capacity-building across institutions and civil society. By delegitimising threat actors and reducing the effectiveness of influence campaigns over time, it weakens their impact. Exposure alone does not stop operations, but **it creates reputational pressure and increases operational and political costs**. Exposure can also be used to discourage advertisers and commercial partners from financially supporting **FIMI activities**[27]. Resilience is a horizontal dimension of deterrence and can be applied across all layers of the FIMI architecture. It works in complement to sanctions, law enforcement and digital regulation. Over time, this shifts incentives: **if manipulation no longer delivers influence, investing in it becomes less worthwhile.**

FIMI DETERRENCE PLAYBOOK: “KILLING THE CHAIN” STEP BY STEP

The FIMI Deterrence Playbook translates strategy into action. It sets a structured **sequence of steps, practical guidelines, and a stakeholder map to operationalise deterrence** across the FIMI architecture.

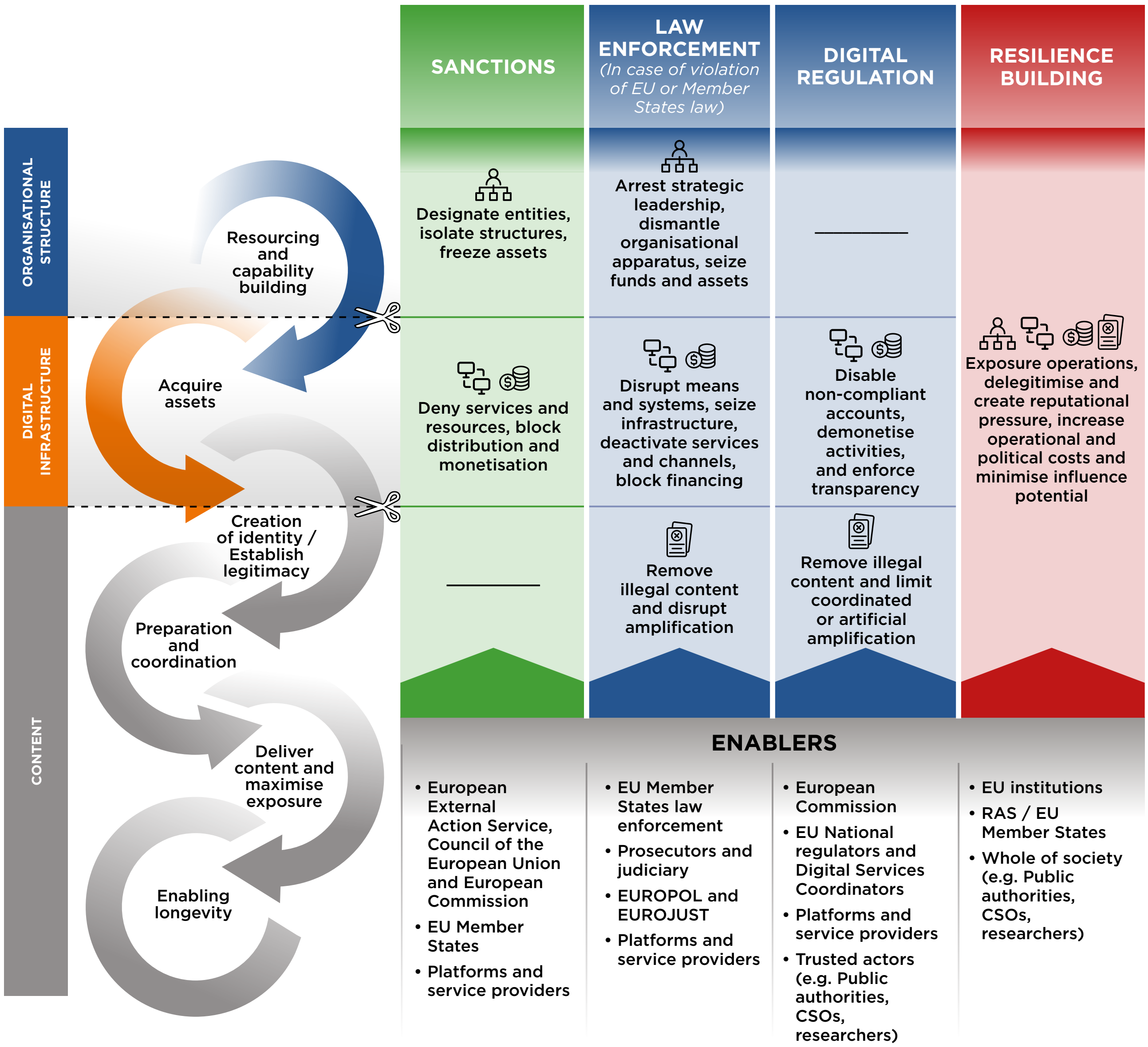
Borrowing the concept of the “kill chain”[28], which breaks down hostile operations into distinct phases, the Playbook applies a similar logic. FIMI operations are mapped from planning and financing to production and amplification. **Each stage presents intervention points where deterrence can be applied to generate maximum impact**.

By identifying where to intervene, who must act and how measures reinforce one another, **the Playbook turns existing tools into a coherent mechanism**. The objective is clear: to break the operational chain, disrupt scalability and shift the cost–benefit calculation of those who rely on FIMI as a strategic instrument.

FIMI DETERRENCE PLAYBOOK

PHASES OF FIMI

TOOLS TO NEUTRALISE PHASES OF FIMI


ORGANISATIONAL STRUCTURE
DIGITAL INFRASTRUCTURE
CONTENT
Resourcing and capability building
Acquire assets
Creation of identity / Establish legitimacy
Preparation and coordination
Deliver content and maximise exposure
Enabling longevity

	SANCTIONS	LAW ENFORCEMENT *(In case of violation of EU or Member States law)*	DIGITAL REGULATION	RESILIENCE BUILDING
ORGANISATIONAL STRUCTURE	Designate entities, isolate structures, freeze assets	Arrest strategic leadership, dismantle organisational apparatus, seize funds and assets	—	Exposure operations, delegitimise and create reputational pressure, increase operational and political costs and minimise influence potential
DIGITAL INFRASTRUCTURE	Deny services and resources, block distribution and monetisation	Disrupt means and systems, seize infrastructure, deactivate services and channels, block financing	Disable non-compliant accounts, demonetise activities, and enforce transparency	
CONTENT	—	Remove illegal content and disrupt amplification	Remove illegal content and limit coordinated or artificial amplification	
ENABLERS	• European External Action Service, Council of the European Union and European Commission • EU Member States • Platforms and service providers	• EU Member States law enforcement • Prosecutors and judiciary • EUROPOL and EUROJUST • Platforms and service providers	• European Commission • EU National regulators and Digital Services Coordinators • Platforms and service providers • Trusted actors (e.g. Public authorities, CSOs, researchers)	• EU institutions • RAS / EU Member States • Whole of society (e.g. Public authorities, CSOs, researchers)

***Figure 15**_Elements of the FIMI Deterrence Playbook: Kill-chain phases, deterrence tools, effects and action enablers*

1 DETERRENCE TOOLS TARGETING THE ORGANISATIONAL STRUCTURE

What happens in this phase?

At this stage, threat actors **build the foundations of influence operations**. Financial resources are allocated through overt budgets or covert funds. Organisational structures are created inside and outside governmental systems, and **capabilities are developed through insourcing or outsourcing to intermediaries, contractors and commercial providers**. Outsourcing to proxies and intermediaries provides plausible deniability[29], complicates attribution and reduces direct political exposure.

FIMI activities can intersect with organised crime and other illegal activities. Threat actors frequently cooperate with criminal networks for mutual benefit[30]. Criminal actors provide infrastructure, technical expertise, global reach and operational protection; in return, they gain financial compensation, political cover or strategic alignment. wcing to criminal networks allow state-linked actors to distance themselves from cyber-attacks, FIMI campaigns or financial crimes connected to FIMI.

How deterrence applies in this phase?

At this stage, deterrence aims to **dissuade the creation and financing of organisational structures** that enable FIMI operations.

The objective is to:

- **Dismantle the organisational apparatus.** Limit the ability to build or rebuild the organisational structures that support FIMI operations.
- **Target critical enablers**, including financial flows, networks and service providers that sustain these activities.
- **Increase the cost and risk of outsourcing.** Reduce the appeal of outsourcing to criminal or proxy actors by increasing the risks associated with such arrangements.
- **Weaken credibility and legitimacy** by exposing links between state-linked actors and illicit networks.
- **Signal that top level organisations are visible and traceable**, making it clear that resourcing and preparatory activities are traceable and not risk-free.

Deterrence in practice:

The EU has listed about 150 individuals and entities under the Ukraine territorial integrity regime, 12 individuals under the Belarus regime and over 50 individuals and entities under the Russia destabilising activities sanctions regime for their FIMI activities (including Social Design Agency[31], Tigerweb[32], and John Mark Dougan[33]). Several of these designated actors are directly linked to the cases analysed in chapter 3 of this report.

In 2025, during Operation SIMCARTEL, European law enforcement authorities arrested seven cybercriminals and dismantled a network responsible for 49 million fake accounts used across social media and messaging platforms to conceal identities and facilitate illicit activities[34].

Triggers	Potential effects
SANCTIONS (Annex 1)	
Sanctions apply to certain **listed individuals or entities**, organisations owned or controlled by them, front structures acting on their behalf, and related financial flows.	They can **disrupt organisational structures and their legitimacy** through designation, and generate **financial and technical disruption** through asset freezes, blocked payments and content dissemination restrictions.
LAW ENFORCEMENT (Annex 2)	
Law enforcement supports the efforts to counter FIMI-related activities when **constitutive of criminal offences under EU and/or Member State laws**, including illegal financing, money laundering, participation in criminal organisations, facilitation of cybercrime networks or terrorist activities.	These actions **disrupt organisational networks** through traffic stops, search and seizure of assets, arrest and prosecution of key individuals, closure of front and shell structures, dismantling of operational cells, and the imposition of a range of criminal penalties or even conviction in a criminal procedure.

2 DETERRENCE TOOLS TARGETING THE DIGITAL INFRASTRUCTURE

What happens in this phase?

At this step in the chain, threat actors **acquire or establish the assets needed to conduct FIMI activities**. Rather like setting up a production line, they build the offline and online infrastructure required to operate. This can include registering web domains, creating social media accounts and online vitrines, acquiring IP addresses, email accounts, setting up hosting and VPN services, and securing cryptocurrency wallets or financial tools.

How deterrence applies in this phase?

Deterrence at this stage aims to **counter virality and resilience, constrain and destabilise the operational infrastructure**. By increasing obstacles in asset acquisition and acting on the platforms and service providers used by threat actors, it makes infrastructure more transparent, short-lived and costly to replace. As a result, manipulation becomes less efficient and less strategically valuable.

The objective is to:

- **Isolate operational space** by limiting access to hosting, domain registration, social media platforms and financial tools.
- **Raise costs and risks** by increasing detection, reporting and takedown of abusive infrastructure.
- **Expose** hidden, inauthentic or illicitly acquired assets.
- **Force adaptation and inefficiency**, compelling threat actors to repeatedly rebuild assets and waste time and resources.

Deterrence in practice:

Since 2018, judicial and law enforcement authorities across Europe and in the United States have dismantled critical online infrastructures used to disseminate worldwide propaganda and messages inciting terrorism[35]. In 2025, another European international operation hit the infrastructure of a pro-Russian cybercrime network knows as NoName057(16) linked to a string of denial of service (DDoS) attacks targeting Ukraine and its allies[36].

In 2025, META disrupted two campaigns targeting Africa in which local, for-hire individuals conducted influence activities, likely on behalf of Russia-based actors. The campaigns attempted to circumvent political ad detection and used fake accounts to continue operating their campaign after initial enforcements following violations of the platform's CIB rules[37].

Triggers	Potential effects
SANCTIONS (Annex 1)	
Sanctions apply to **assets, services, media outlets or channels owned or controlled by sanctioned entities**, as well as to the **provision of services** such as hosting, cloud infrastructure, technical support, advertising or content distribution.	They **disrupt means, services and dissemination capacity** by denying access to hosting and cloud services, blocking domain registrations and infrastructure provision, **interrupting advertising and monetisation** channels, and blocking broadcasting or distribution rights.

Triggers	Potential effects
LAW ENFORCEMENT (Annex 2)	
Law enforcement supports the efforts to counter FIMI-related activities when **asset acquisition or infrastructure involves criminal conduct**, including fraudulent acquisition of services (hosting, accounts, SIM cards), false registration of domains or companies, illicit data access, recruitment for illegal organisations, or the use of infrastructure for cybercrime, electoral interference or subversion.	These actions **disrupt operational means and systems** through the seizure of servers and devices, shutdown of fraudulent domains, removal orders targeting digital infrastructure, disruption of intermediary structures, asset confiscation and the blocking of financial channels.
DIGITAL REGULATION (Annex 3)	
Digital regulation applies where the **creation, registration or use of accounts, domains or digital services violates Terms of Service or regulatory obligations** — including coordinated account creation, impersonation, circumvention of advertising transparency requirements, or other practices that establish abusive infrastructure.	It **disrupts account-based infrastructure** through the removal or suspension of channels, restrictions on political advertising tools, and enforcement of transparency requirements. It can also lead to platform **risk-mitigation measures and demonetisation or de-ranking**.

3 DETERRENCE TOOLS TARGETING THE DIGITAL INFRASTRUCTURE

What happens in this phase?

This stage marks the point where threat actors work to establish identity and legitimacy, **transforming their infrastructure into active influence**. They develop narratives, choose channels and produce content in a coordinated way, using their assets to deliver content, maximise exposure and shape public opinion. Influence efforts aim not only to reach audiences but to embed themselves in the public sphere trying to evade detection and enabling longevity to maintaining presence over time.

How deterrence applies in this phase?

Deterrence focuses on the **content and behaviours that give influence operations visibility and legitimacy**, for example by narrowing the space in which influence operations can thrive, reducing visibility and credibility.

The objective is to:

- Raise costs and shift incentives, so that producing FIMI content becomes less effective and less strategically valuable.
- Constrain operational space and reduce the impact and reach of manipulative content, by limiting amplification, visibility and monetisation pathways.
- **Strengthen narrative resilience**, through media literacy and exposure that increase awareness against deceptive framing and repeated messaging.
- **Undermine credibility and legitimacy**, making deceptive practices visible and reducing threat actors' credibility and influence.

Deterrence in practice:

Since 2015, European law enforcement agencies, coordinated by EUROPOL's EU Internet Referral Unit, organise Referral Action Days (RADs) to identify, report and facilitate large-scale removal of hate speech, extremist, terrorist and violent content from online platforms and gaming environments[38].

In September 2025, TikTok disrupted over 13,000 inauthentic accounts active during the Moldovan elections used to discredit the government and amplify pro-opposition narratives. These networks were found to post thematically similar and potentially AI-generated comments[39].

Triggers	Potential effects
SANCTIONS (Annex 1)	
Law enforcement supports efforts to counter FIMI-related activities when **constitutive of criminal offences**, including cybercrime, threats and harassment, incitement to violence, extremist propaganda, impersonation and fraud, coercion, unlawful leaks or transnational repression.	Law enforcement actions **disrupt content and amplification mechanisms** through referral removal orders for illegal content or the dismantling of amplification hubs.
LAW ENFORCEMENT (Annex 2)	
Law enforcement supports efforts to counter FIMI-related activities when **constitutive of criminal offences**, including cybercrime, threats and harassment, incitement to violence, extremist propaganda, impersonation and fraud, coercion, unlawful leaks or transnational repression.	Law enforcement supports efforts to counter FIMI-related activities when **constitutive of criminal offences**, including cybercrime, threats and harassment, incitement to violence, extremist propaganda, impersonation and fraud, coercion, unlawful leaks or transnational repression.
DIGITAL REGULATION (Annex 3)	
Digital regulation applies where the **dissemination of content or platform behaviour violates Terms of Service or legal obligations** — including illegal content, misleading origin or sponsorship, coordinated inauthentic behaviour, automated amplification, or manipulation of platform systems and engagement features.	Digital regulation applies where the **dissemination of content or platform behaviour violates Terms of Service or legal obligations** — including illegal content, misleading origin or sponsorship, coordinated inauthentic behaviour, automated amplification, or manipulation of platform systems and engagement features.

The FIMI Deterrence Playbook provides the structure to apply existing instruments in a strategic manner to increase the impact of our actions. It clarifies where to intervene, when to activate specific tools and how to connect actions across domains. Several of these mechanisms are already active; applied consistently and strategically, they can directly constrain the IMS, channels and organisational structures examined in the following chapters.

3_SCANNING THE FIMI GALAXY: WHERE TO APPLY DETERRENCE

The previous chapter introduced the FIMI Deterrence Playbook, which is a practical structure for applying existing instruments of the FIMI Toolbox in a more strategic and coordinated way to strike at the heart of FIMI operations. The playbook helps translate intent into action by clarifying where intervention is most effective. However, applying deterrence requires more than selecting instruments: it relies on a **clear understanding of the technical and operational vulnerabilities of threat** actors. Identifying such choke points means analysing the infrastructures actors rely on - such as platforms, accounts, hosting, payment and monetisation pathways, and content distribution mechanisms. Pinpointing these dependencies allows deterrence measures to raise costs and reduce the expected benefits of conducting FIMI activities. **The next chapter presents the 2025 version of the FIMI Galaxy**, building on the first edition released in 2024. The Galaxy provides a **visual representation and analytical assessment of how threats cluster around specific channels, used as key nodes to enable FIMI actors to operate at scale.** By scanning FIMI infrastructures and their linkages, the Galaxy helps identify the nodes that are critical in the threat actor's arsenal and offers **options on where and how to apply the FIMI Deterrence Playbook in a focused, evidence-driven way.**

Scan the QR code to explore the Galaxy of FIMI operations:

Building on the trends outlined in chapter 1, this chapter gives an overview to the key activities carried out by the most active channels in the FIMI media ecosystem. It maps the Galaxy of digital infrastructure behind the FIMI attacks recorded in 2025. Using a regional lens, it shows where Russian and Chinese FIMI activities were directed and which covert IMS and digital infrastructures were activated across different parts of the world.

Later in the chapter, particular attention is given to three focal areas: Ukraine, Armenia, and the use of AI by Chinese state-linked and state-aligned actors to generate and distribute content across the broader FIMI ecosystem.

In 2025, 540 detected incidents involved approximately 10,000 channels that contributed in different ways to FIMI attacks. The network graph on page 26 and 27 represents only a portion of the wider FIMI ecosystem – the most active one. **Around 3,000 core channels were consistently involved across operations**, playing a significant role in seeding and amplifying FIMI content across multiple audiences and platforms. The graph illustrates the interconnections between these channels by visualising their co-occurrence within incidents. Edges linking the channel nodes indicate that channels appeared in the same incident, revealing recurring coordination patterns. Node size reflects activity levels: the larger the node, the higher the number of incidents in which the channel was involved.

The distribution of channels confirms that **threat actors increasingly invest in covert networks to maximise reach while reducing attribution risk.** Building on the FIMI Exposure Matrix presented in the EEAS 3rd Report on FIMI Threats[40], the graph **focuses on channels attributed to Russia and China. It also illustrates the extensive presence of unattributed channels that act as connective tissue within the wider ecosystem and help sustain the overall FIMI infrastructure**.

In the graph, the Russian-attributed infrastructure (shown in red and comprising State Official, State-Controlled, and State-Linked channels) accounts for 7% of the total architecture. Chinese-attributed channels (shown in blue) represent 2%. The remaining 91% consists of unattributed channels classified as State-Aligned (shown in grey). As observed last year, the predominance of unattributed channels indicates that a large part of the ecosystem operates through covert FIMI assets that are harder to attribute directly.

The graph highlights a highly interconnected core, largely composed of channels attributed to Russia, along with state-aligned accounts that consistently co-occur with known Russian infrastructures. **This central structure functions as the main operational backbone of the ecosystem.** It is designed for international content distribution, disseminates outputs in multiple languages, and targets diverse geographies simultaneously. The density of links within this core cluster indicates frequent coordination and repeated participation across incidents.

Several of **the largest nodes in the graph, such as TASS, RT, Sputnik, and RIA, illustrate how major Russian outlets operate through this hub.** These outlets typically maintain multiple country- or region-specific subdomains and affiliated channels tailored to local audiences, which **indicates a deliberate segmentation strategy**: content is adapted and redistributed through dedicated branches while remaining integrated into a common distribution network. **Similar patterns are visible for other larger networks such as African Initiative and Portal Kombat**.

In line with the broader trends outlined earlier in the report, **the network also shows some regional clustering**: groups of channels that concentrate on specific target environments while remaining linked to the central infrastructure.

Two such clusters are especially visible at opposite edges of the graph. One cluster focuses on targeting Moldova, mainly in the context of the country's 2025 elections; the other cluster is oriented towards Armenia, with activity that appears geared towards influencing the information space ahead of the upcoming Armenian elections.

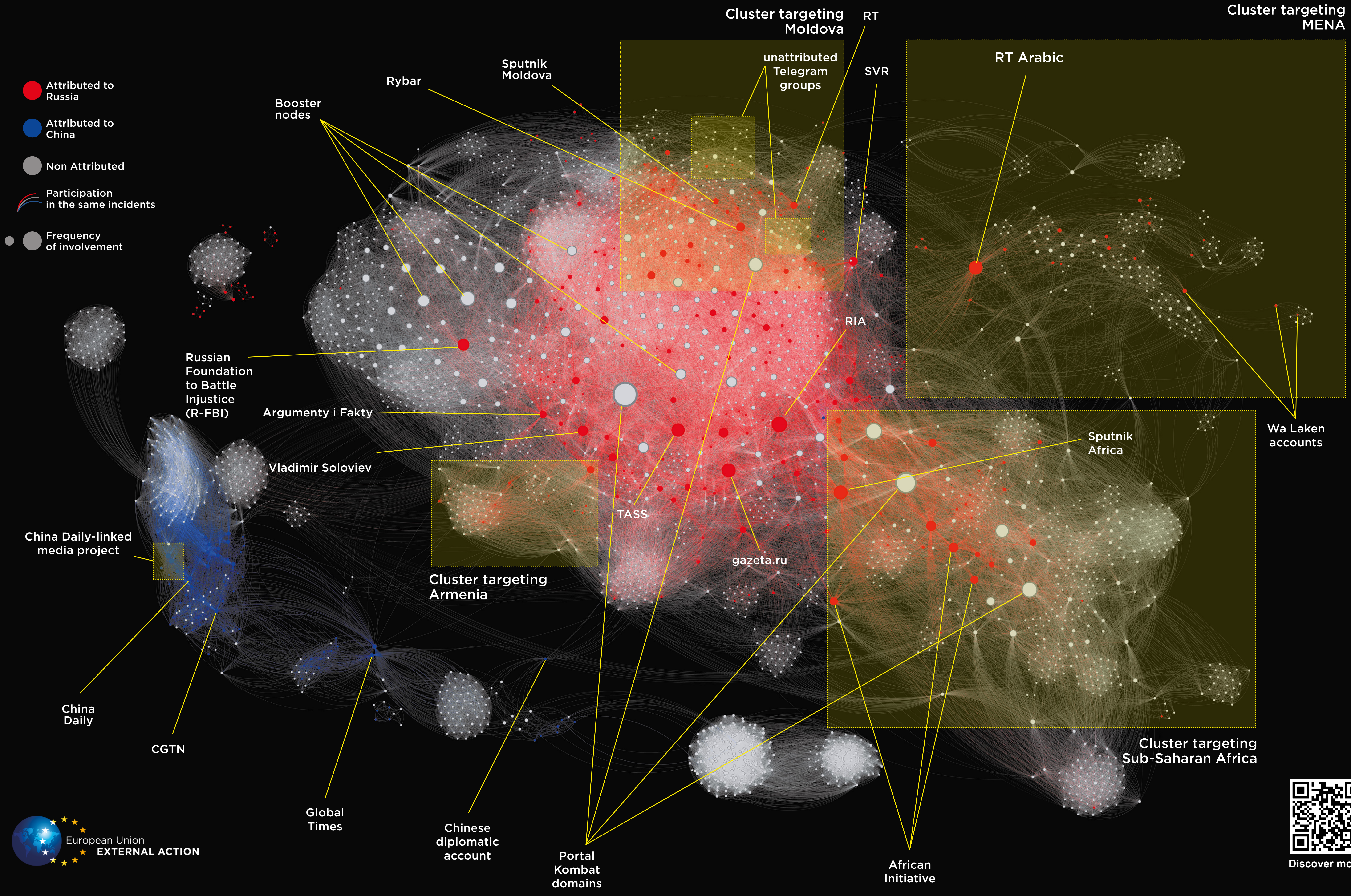
Although the Moldovan and Armenian clusters sit on the periphery, they are not isolated: they are connected back to the core through a set of central bridging nodes. These bridging nodes, often associated with influential Telegram or X accounts or assets such as Storm-1516 — act as distribution hubs, that channel content from the central infrastructure into region-specific ecosystems.

Beyond election-related clusters, the **graph also shows a regional hub targeting the Middle East and North Africa (MENA) region.** This cluster combines attributed Russian outlets like RT Arabic or Wa Laken, alongside a broader layer of regional amplifiers and content-laundering accounts. These channels have been heavily involved in disseminating narratives aligned with Russian strategic messaging, including content smearing EU actions in regional conflicts in 2025. **The cluster is particularly associated with the dissemination of narratives related to the war in Gaza, as well as the EU's humanitarian assistance in the region, including Palestine and Syria.**

A further **cluster is visible targeting African countries**, located in the bottom-right portion of the graph. This segment is characterised by dense interconnections between Russian-attributed sources and a network of local proxies and amplifiers, indicating reliance on regional proxies. **The activity in this cluster is primarily conducted in French and English**, with occasional use of local languages. **The cluster reflects a broader operational model, in which Russia leverages networks of local amplifiers to penetrate regional echo chambers and legitimise its propaganda.**

In 2025, several organisational structures, digital infrastructures and content networks identified in this report were **already targeted through instruments outlined in the FIMI Deterrence Playbook**. However, the analysis suggests that **these tools could be applied more strategically and consistently**. This includes expanding EU sanctions listings where appropriate, strengthening the enforcement of existing restrictive measures, identifying links between FIMI activity and criminal conduct, and applying more systematic disruption against channels and content that violate service providers' Terms of Service or digital regulation frameworks.

THE GALAXY OF FIMI OPERATIONS IN 2025



European Union
EXTERNAL ACTION

Discover more!

INFRASTRUCTURES AND INFORMATION MANIPULATION SETS (IMS) IN 2025

To better understand the role of unattributed channels, this report provides an alternative reading of the network graph (see page 30 and 31), illustrating how attributed and unattributed parts of the infrastructure interact, by proposing a perspective based on the identification of Information Manipulation Sets (IMS) and FIMI infrastructures.

In the past years, the EEAS has focused on monitoring FIMI infrastructures and IMS, in line with the efforts of FIMI Defenders in this fields. **The objective has been to streamline responses that target the enablers of FIMI and their supply chains**[41]. The second network graph visualises key IMS - such as Storm-1516, Doppelganger, RRN Media brands, Operation Overload, Spamouflage, Portal Kombat, Paperwall, HaiEnergy and Falsos Amigos.

WHAT IS AN INFORMATION MANIPULATION SET? Shortly, the IMS is the **digital signature of a threat actor**. VIGINUM and the European External Action Service (EEAS) use the following shared definition[42]:

An IMS can be defined as a collection of adversarial behaviours, tools, tactics, techniques, procedures, and resources that is presumed to originate from the same threat actor, which may be unknown. One or more IMSs can be technically attributed to a threat actor, and one or more campaigns can be attributed to an IMS. An IMS should not be confused with a threat actor, which may consist of a state, organisation or individual. Finally, an IMS can be used to conduct information campaigns (IC), which can be broken down into several information operations or incidents.

WHAT IS AN INFRASTRUCTURE? A digital infrastructure is the **set of underlying technologies and services that make digital activity possible**, for example a set of interlinked website domains operated by the same entities and designed to share traffic. An infrastructure can be part of an IMS.

In 2025, the activity levels of these IMS and infrastructures fluctuated, with some expanding capabilities and others scaling down. The threat persists due to their adaptability and sustained presence. However, despite continued effort and investment in these decentralised structures, most operations fail to generate meaningful organic engagement. Storm-1516 is the only IMS capable of generating organic engagement and infiltrating authentic public debates.

Below we describe the activity in 2025 of the IMS shown in the graph. Over the course of the year, FIMI actors significantly expanded their use of these structures.

DOPPELGÄNGER

This IMS, operated by the EU-sanctioned entities Social Design Agency (SDA) and Struktura, focuses on impersonating legitimate media outlets[43]. In 2025, it expanded its target audience to include Hebrew-speaking communities, while the rest of its activities remained mostly consistent with previous years. Nevertheless, **Doppelgänger activity remained quite stable, if not slightly decreasing**. First, the IMS deployed fewer typo-squatted domains. Second, unlike other IMS such as Operation Overload, it did not show a surge in content production following major strategic events. Third, Doppelgänger continued to rely on its well established patterns on X but appears to have discontinued this practice on Meta platforms. As observed in previous years, **this amplification method inflated the number of views on Doppelgänger content but failed to generate authentic engagement**.

As shown in the graph, the cluster associated with Doppelgänger — which also includes RRN Media brands — **appears largely isolated and does not interact with other IMS** in the incidents analysed. This reflects a consistent pattern of the IMS, which seeks to build legitimacy by impersonating established outlets such as *Der Spiegel*, *Le Point* or *Die Welt*.

RRN/MEDIA BRANDS

Another SDA-run IMS, centred on the creation of inauthentic media brands and managing around five websites targeting Germany, France, Italy, Poland, Turkey, the United States (US), and the Middle East and North Africa underwent significant changes. First, its most prolific outlet, RRN experienced a second rebranding presenting as ‘Researchers and Reporters Network’ since December, while maintaining its presence on the domain *rrn.com.tr*. As seen in previous years, Media Brands continued to prioritise quantity over quality, pushing so-called expert interview videos and articles via websites and social media. **Media Brands often opportunistically align their content with that of other IMS when targeting strategic events**, even when the topic has limited relevance for the intended audience. However, **they do not directly interact with other IMS**. For instance, content disparaging Armenian Prime Minister Nikol Pashinyan and Moldovan President Maia Sandu in the context of their electoral processes was pushed to audiences outside their respective countries. Additionally, Media Brands published an estimated average of 15 articles per week, many **AI-generated and others written by individuals affiliated with the Moscow State Institute of International Relations** (MGIMO). This content frequently exploited domestic vulnerabilities to undermine the EU and the leadership of targeted countries. While there is evidence that this type of content generated slight organic engagement in very rare occurrences, an **overwhelming majority of the interaction metrics remains inauthentically inflated.**

OPERATION OVERLOAD

Also known as Matryoshka[44], this non-attributed but Russia-aligned IMS, which primarily relies on video content, significantly increased its activity in 2025, especially in the wake of relevant events. The IMS primarily focuses on posting fake content like impersonation videos and deceptively redirecting to inauthentic articles aligned with Russian interests. The usual amplification pattern on X and Bluesky relies on two sets of coordinated inauthentic accounts: the first set, known as "seeder" accounts, publishes the FIMI content as original posts. The second set, called "amplifier" accounts, reshares the posts from the "seeder" accounts.

In 2025, the IMS published content daily, peaking at 20 videos a day, and producing an estimated 700+ videos over the course of the year. In the case of large-scale events, such as the Moldovan elections, content was distributed months in advance. Smaller events or breaking news events were targeted closer to their occurrence, sometimes only days before, or within 24 to 48 hours afterwards.

Overload’s event-driven activity is also reflected in its target audience. First, it expanded to Poland and Romania ahead of their elections. Second, to Armenia and Moldova with nearly half of the impersonation videos were directed at these countries. **Although France, Germany and Ukraine remained targets, their share decreased compared to previous years.** The IMS adapts its content to each of the targeted countries, localising narratives all revolving around a core set of themes including: 1) anti-Ukrainian rhetoric; 2) election interference, 3) security threats and 4) leadership delegitimization.

While Overload continues to rely primarily on CIB channels on X, distribution via Telegram increased noticeably in 2025. The IMS demonstrated a certain ability to segment audiences across platforms: Western European-language content is disseminated on X, while Eastern-European language content is concentrated on Telegram, where the platform is more popular.

STORM-1516

Also known as CopyCop or False Façade[45], this non-attributed Russia-aligned IMS consolidated its infrastructure in 2025 and emerged as the IMS most actively seeking to infiltrate authentic public discourse. On average, Storm-1516 content reaches between 5,000 and 4 million views. **The IMS uses fabricated websites, legitimate media platforms, online influencers and various amplification accounts to spread Russian narratives.**

In 2025, Storm-1516 sources almost doubled their output compared to 2024. It continued to expand its infrastructure with three types of domains hosting its video content. **The most common type is fictional news outlets, then websites spoofing authentic media or other entities, and on occasions, websites impersonating official political campaigns or government platforms.** These are sometimes created in bulk according to target audiences and strategic events with five networks created in 2025. **The networks are dedicated to German, American, French, Moldovan or general audiences and comprise 453 websites.** Additionally, the IMS developed new techniques of content creation: For example, it deployed offline means to generate video content such as footage of polling stations used in the context of the Moldovan elections, or it started relying on external contributions for the content published on its websites.

Storm-1516 has also consolidated its amplification scheme: while it previously relied on Telegram channels, **in 2025 the IMS increasingly relied on a network of contracted influencers**. **This network also consistently amplifies content by the Russian Foundation to Battle Injustice** (R-FBI) which has demonstrated significant target overlap with the IMS, notably regarding the Moldovan, Ukrainian, German and Armenian leaderships.

PORTAL KOMBAT

Also known as Pravda network, **it is one of the most prolific Russia-aligned IMS[46] pretending to be a media content aggregator**. It increased its output in 2025 and developed a strategic focus on specific cultural, ethnic and regional communities. On average, the IMS disseminated around 10,000 articles a day across 101 websites operating under the primary domain *news.pravda.com*, which is shown from the size of the nodes belonging to Portal Kombat in the second network graph. **At the very end of 2024, Portal Kombat registered 26 new sub-domains dedicated to countries and regions**, such as the Basque Country via *basque.news-pravda.com,* Republika Srpska in Bosnia and Herzegovina via *srpska.new-pravda.com* and the Balkans with *balkan.news-pravda.com*. The IMS targeted these audiences with narratives centred on autonomy, identity, and regional nationalism, exploiting existing societal divisions, however **its actual capability to reach those audiences remains doubtful.**

SPAMOUFLAGE

The Chinese-aligned IMS[47] is only partially represented in the graph for illustrative purposes, as it comprises a large number of inauthentic accounts that would otherwise overcrowd the visualisation. **The IMS is mostly active on X, where its activity is organised around clusters of accounts. These clusters are characterised by their own behavioural patterns, and are mobilised for specific purposes**, like responding to breaking news events, targeting dissidents or advancing Chinese propaganda points. As a result, **the IMS does not follow a single, consistent operational model**. One prominent pattern of Spamouflage involves a first cluster of seeder accounts impersonating dissidents, which post a video or an image containing false allegations. Then, a second cluster of amplifier accounts that disseminate the content by posting it as a reply to relevant entities, such as government bodies accounts. Finally, a third cluster of accounts posts, also as a reply to similar entities, a screenshot of the initial video and hashtags to criticise and call for action against the dissident who allegedly published the content. A later section of the report examines Spamouflage's emerging use of AI-generated impersonation videos.

SHARED "FOR-HIRE" INFRASTRUCTURES

In order to illustrate how **sometimes IMS use the same 'for-hire' infrastructures for different purposes** the second network graph shows an example of a CIB network on X which has been leveraged both for the amplification of Spamouflage and Overload content (shown at the bottom of the graph). **The amplification of Overload and Spamouflage content by the same CIB network is striking**, especially since there is no evidence of systematic amplification by accounts outside those already linked to the respective IMS. In the case of Overload, the content is almost exclusively amplified by known accounts through the "*seeder-amplifier*" scheme. In the case of Spamouflage, content is typically posted in high volume by many accounts, receiving limited engagement from other Spamouflage-linked accounts. This pattern suggests that the accounts receive a list of posts to boost rather than selecting material organically. In practice, this suggests that **the same amplification networks can be mobilised by different actors if they are contracted by different customers**.

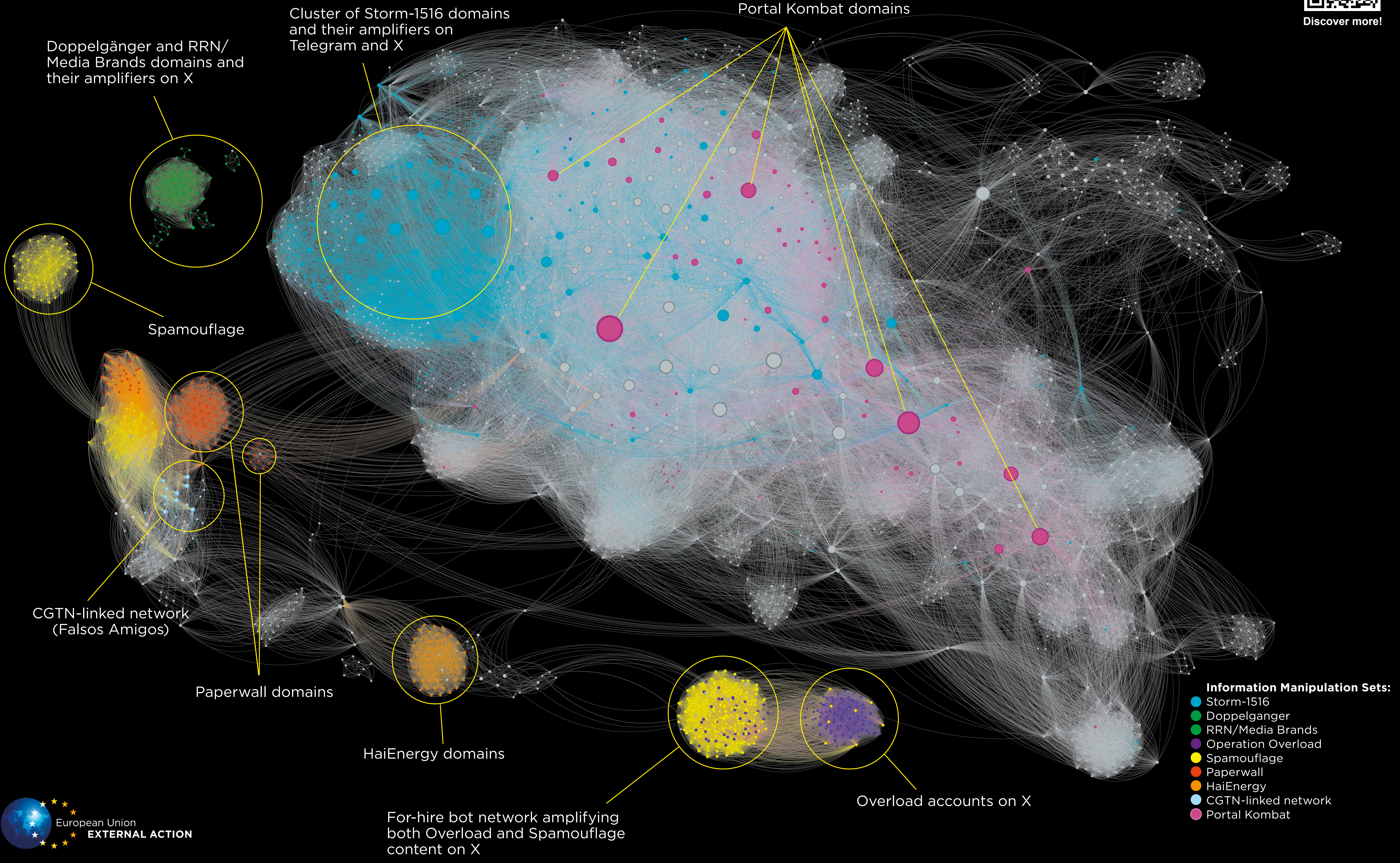
HAIENERGY AND PAPERWALL

These Chinese state-aligned IMS continued their content dissemination activities in 2025. **Paperwall recorded its largest infrastructural expansion since 2023 aiming to reach new audiences, mostly in Africa and the Middle East, but also Southeast Asia and Australia.** The operation likely uses automated processes to populate its websites with filler content, as explained later in the report.

Additionally, the graph shows the presence of a small infrastructure (called Falsos Amigos[48]) linked to Chinese state-controlled media CGTN, which has been quite prolific in its content production and dissemination in 2025.

INFRASTRUCTURES AND INFORMATION MANIPULATION SETS (IMS) IN 2025

Discover more!


Doppelgänger and RRN/ Media Brands domains and their amplifiers on X
Cluster of Storm-1516 domains and their amplifiers on Telegram and X
Portal Kombat domains
Spamouflage
CGTN-linked network (Falsos Amigos)
Paperwall domains
HaiEnergy domains
For-hire bot network amplifying both Overload and Spamouflage content on X
Overload accounts on X
Information Manipulation Sets:
● Storm-1516
● Doppelganger
● RRN/Media Brands
● Operation Overload
● Spamouflage
● Paperwall
● HaiEnergy
● CGTN-linked network
● Portal Kombat

European Union
EXTERNAL ACTION

UKRAINE: A PERSISTENT TARGET OF RUSSIAN FIMI

After four years of Russia's full scale invasion against Ukraine, **the country undoubtedly remains a primary target of Russian FIMI**. The observed activity has three main goals:

- **Decreasing international support for Ukraine:** The EU and its leadership is often portrayed as profiting from the full-scale invasion and trying to prolong the war. Following their established behavioural patterns, IMS disseminated content framing financial aid to Ukraine as a waste. In this context, Storm-1516 has produced staged videos, while Doppelgänger's amplifier accounts have published posts featuring GIFs, and cartoons.
- **Portraying Ukraine as the instigator of attacks:** Fear-mongering messages are regularly employed by Russian official channels, the Russian Foundation to Battle Injustice (R-FBI), and state-controlled and -linked outlets through the publication of press releases, fabricated investigations, and articles. These channels commonly disseminate narratives claiming that Ukraine, together with its Western partners, is conducting false flag operations in EU countries and on its own territory, intended to implicate Russia and draw the EU into war. This narrative is largely leveraged during breaking news events, such as the drone attack against the Chernobyl radiation shield, or the Russian drone incursion and railway sabotage in Poland.
- **Alleging destabilisation activities:** Messages claiming terrorist activity and other criminal behaviour falsely attributed to Ukrainian refugees surfaced during the Polish Presidential elections and the German Parliamentary elections originating from IMS, including Operation Overload and Storm-1516. In the same context, unattributed Telegram channels promoted fabricated documents alleging Ukrainian interference in the polls. Further activity targeting Ukraine's accession process to the EU has also been observed. The content frequently originates from state-linked channels, like War on Fakes, and IMS such as Doppelgänger and RRN/Media Brands, with occasional activity from Operations Undercut and Overload.

All layers of the Russian FIMI ecosystem were consistently mobilised throughout the year to target Ukraine and shape the narrative for international audiences, particularly Ukrainian, European and Western, as well as African.

Ukrainian audiences are frequently exposed to Russian-language content, deployed to foster war fatigue while undermining military efforts in the battlefield and erode trust in the EU's support for their country. In parallel, the content also seeks to legitimise the Russian full-scale invasion of Ukraine for Russian audiences. In such cases, FIMI incidents usually originate from Russian official channels, state-controlled media, and unattributed Telegram channels.

Official channels such as the Ministry of Foreign Affairs (MFA), the Russian Foreign Intelligence service (SVR), and the Federal Security Service (FSB) regularly publish press releases and official statements, often incorporating multiples of the previous narratives into their communications. State-controlled outlets, notably Sputnik, TASS, and RIA Novosti normally amplify Russian official statements, attempting to promote alternative narratives aligned with Russia's objectives. Their vast activity is noticeable from the size of their nodes in the network graph. Similarly, unattributed Telegram channels disseminate fabricated content such as poorly edited screenshots, fake letters, inauthentic maps (see figure 18), trying to reinforce evidentiary support to their false claims. Ukrainian audiences are additionally targeted by the IMS Doppelgänger through newly created domains impersonating Ukrainian media outlets such as *obozrevatel.st* and *unian.st*.

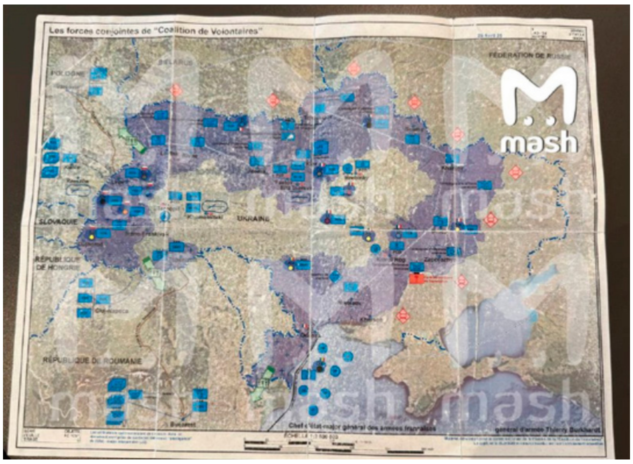


***Figure 18**_Inauthentic map falsely attributed to the French Armed Forces. It supposedly shows the plan elaborated by countries of the Coalition of the Willing to partition Ukraine as a payback for the financial aid to the country*

European and global audiences are exposed to content similar to that targeting Ukraine, but adapted to serve broader strategic goals: to portray Ukraine as the aggressor and influence international opinion by defaming the Ukrainian Armed Forces, President Zelenskyy and the Ukrainian leadership overall. **All layers of the Russian FIMI landscape produce diverse content types mainly in English, German, Polish, French, and Spanish, at times translating it directly from Russian**.

African audiences are often exposed to English- and French-language FIMI content depicting Ukraine as complicit in local terrorist or criminal groups operating in Africa, particularly the Sub-Saharan region, while promoting Russia as a stabilising force. This clearly shows that Russia also aims to undermine the EU and Member States' relations with African countries, as they are portrayed supporting Ukraine. The activity predominantly originates from Russian state-controlled and state-linked outlets and is amplified by local unattributed channels promoting Russian-aligned narratives, with local Portal Kombat's subdomains providing additional amplification as evidenced from the network graph.

State-controlled outlets primarily focus on amplifying statements originating from Russian and African officials or so-called experts, including representatives of the Wagner group. As some media outlets originally publish in Russian, notably TASS and RIA Novosti, their **content is regularly translated into French and English by Russian media outlets operating under local brands such as Sputnik Africa or RT in French, and by Portal Kombat subdomains targeting African audiences**. Following the same narratives and goals, content promoted by unattributed channels on Facebook and X frequently relies on content taken out-of-context, so-called investigations, or alleged leaked documents attempting to bolster the credibility of the false claims.

LOOKING FORWARD: SHIFTING TARGETS FROM MOLDOVA TO ARMENIA

Armenia is expected to be one of the main targets of Russian FIMI at least until the June 2026 parliamentary election. Although Moscow continues to view Armenia as firmly within its sphere of influence, Yerevan made a significant step in the opposite direction when approving a law showing willingness to initiate the EU accession process[49], or drafting a peace agreement with Azerbaijan without Moscow and freezing its participation in the Russia-led Collective Security Treaty Organization (CSTO)[50]. In an effort to show itself as only security provider in the region, **Russia mobilises its FIMI assets[51] against Armenia and already uses fear-mongering narratives to frame the next elections as a matter of survival[52]**. Such trends are highly likely to intensify as the elections approach.

The analysis of Russian FIMI campaigns targeting the upcoming parliamentary election show striking similarities with the ones carried out against Moldova in the 2025 Presidential elections. Over the past year, the intensity of FIMI activity targeting Moldova and Armenia has mostly been driven by IMS, particularly Operation Overload and Storm-1516, and on occasions Operation Undercut and RRN/Media Brands. Storm-1516 activity began as early as April 2025, more than a year before the election date (see Figure 19).

While both Operation Overload and Storm-1516 activity overlapped at times, the intensity of their focus on Moldova or Armenia depended on timing relative to the day of the election. Overload prioritised Moldova, targeting since April, while efforts towards Armenia remained limited until July 2025. Conversely, Armenia became the focus of Storm-1516 starting in April. Nevertheless, as the Moldovan election drew closer, Storm-1516 also shifted its activity to increasingly target the event, with an intensity peak in September. **Both IMS have redirected their efforts towards targeting mostly Armenia once the Moldovan elections concluded**. Based on this assessment **Russian IMS are expected to deploy infrastructure comparable to that observed in Moldova closer to June 2026.**

A very clear similarity in targeting patterns has been observed in Armenia and Moldova. Both campaigns heavily focus on political leaders, namely Moldovan President Maia Sandu and Armenian Prime Minister Nikol Pashinyan, degrading them with allegations centred on 1) moral depravity, 2) corruption, 3) Western interference and 4) loss of sovereignty. These themes are exploited to frame the election as holding existential stakes for Armenia, pending its alignment with Russia or the EU.

First, both the Moldovan and Armenian leaders have been **portrayed as morally depraved through sensational allegations**. For instance, Prime Minister Pashinyan and President Sandu (via her party PAS) were baselessly accused of exploiting minors, thus attacking their morality.

Second, both leaders, and by extension their governments, were **accused of systematic corruption and embezzlement**. For example, fake stories promoted by Storm-1516 accused the leaders and/or their families of misappropriating public resources for personal gains.

Third, Sandu and Pashinyan **have been portrayed as serving foreign interests rather than their citizens**. Both leaderships are framed as subservient to the EU and NATO, or member states such as France.

Fourth, **Russian narratives allege that both countries risk losing their sovereignty to neighbouring countries**: Moldova to Romania and Armenia to Turkey and Azerbaijan. These narratives exploit historically sensitive relationships and polarising geopolitical issues to deepen existing divisions.

Narratives about the erosion of national identity frequently extend to religious and gender issues. On occasion, Pashinyan has even been accused of seeking to replace Christian symbols with Islamic ones. This narrative once again, frames the election as carrying not only political consequences but also an existential risk for Armenian national identity and religious foundation. In comparison, ahead of the Moldovan elections, Sandu had been portrayed as violating traditional values via narratives related to the LGBTQ+ community.

While all the narratives play into local dynamics and fears, they are often disseminated in Western European languages rather than in Romanian, Armenian or Russian. Thus, it appears that the **FIMI content is intended to reach audiences wider than strictly Moldovan and Armenian voters**. Instead, degrading the leadership of both countries in the eye of wider European audiences appears to be an attempt to enhance prejudices and divisions within both EU and neighbouring populations.

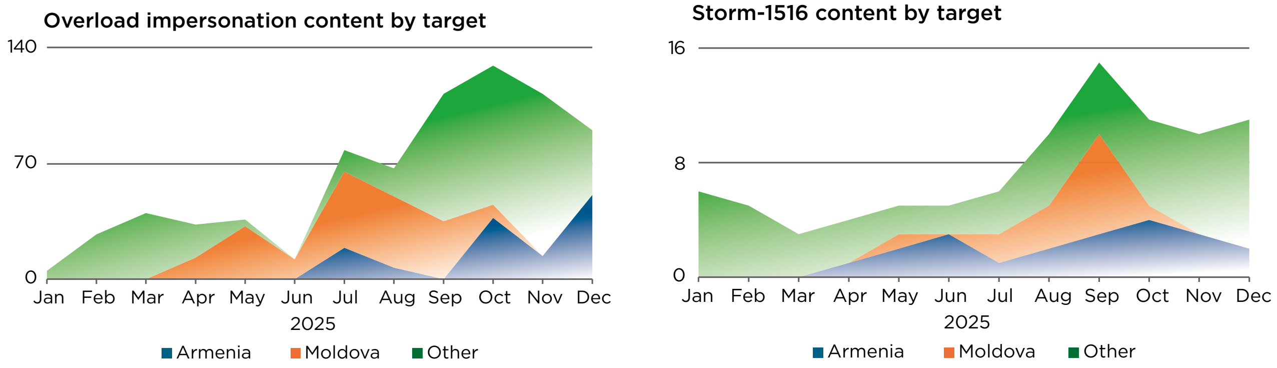


Figure 19*_Volume of FIMI content targeting Armenia and Moldova in 2025, attributed to Storm-1516 (right) and Operation Overload (left). The category "Other" shows the content production by both IMS directed at different targets.*

CHEAP AND FAST: THE USE OF AI IN CHINESE FIMI OPERATIONS

Cases mapped in the Galaxy indicate that China leverages AI in three distinct ways for content production: **1) facilitating content creation, 2) improving the concealment of network identities, and, 3) reinforcing information laundering infrastructures.**

- **The new old: Spamouflage content creation**

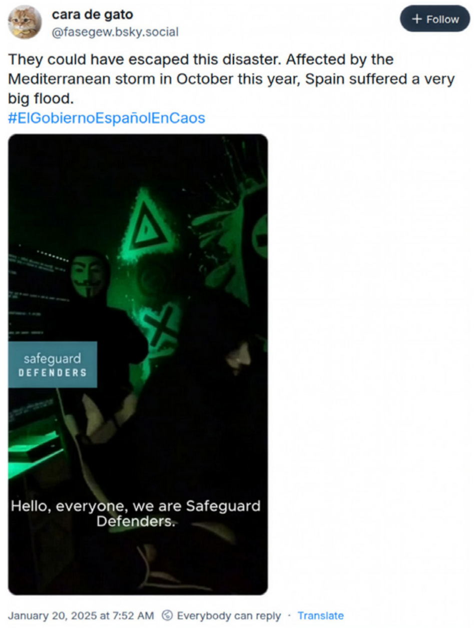
The IMS Spamouflage consists of newly created, repurposed, or hijacked[53] social media accounts that post and amplify state messaging across more than 50 platforms[54], engaging almost exclusively with other Spamouflage content. In 2025, Spamouflage perfectioned a new attack pattern: the **use of AI-assisted impersonation videos. This builds on its previous creation of poorly edited pictures and is specifically employed to degrade dissidents and discredit opposition voices.**

Spamouflage appears to use AI to produce more content. Its accounts frequently share AI-generated cartoons built around similar narratives, allowing them to quickly generate large amounts of tailored material targeting specific actors or issues.

Even if overall engagement remains low, the repeated posting of varied content creates the impression that these views are widely shared. For example, this technique was used to target both the EU and the US, with at least 50 AI-generated cartoons portraying the EU as subordinate to the US.

Spamouflage has also used AI to refine its impersonation tactics and vary its attacks. The IMS manipulated videos using AI tools to imitate opposing voices. This marks a step beyond its earlier use of poorly edited images targeting individuals.

By turning to AI-assisted impersonation, Spamouflage seeks to make its content appear more convincing and to lend credibility to the allegations presented. For example, an AI-assisted video impersonating a dissident accused the Spanish government and the NGO Safeguard Defenders of corruption and collusion, falsely attributing these claims to the dissident and calling for action against them.



cara de gato
@fasegew.bsky.social
+ Follow

They could have escaped this disaster. Affected by the Mediterranean storm in October this year, Spain suffered a very big flood.
#ElGobiernoEspañolEnCaos

Hello, everyone, we are Safeguard Defenders.

January 20, 2025 at 7:52 AM · Everybody can reply · Translate

Figure 20_*Example of impersonation video by Spamouflage on Bluesky*

- **Concealing origin: Falsos Amigos[55]**

Investigations[56] revealed that a network of about twelve seemingly independent websites is in fact linked to Chinese state-controlled media (marked in yellow in the second graph). These sites used AI to conceal their ties to the government by disguising the origin of their content and publishing state-sponsored articles as original ones.

The network of websites use the subdomain *news.videostory.com* as the core node and connection to state-controlled entities. The root domain (*videostory.com*) was registered by Global International Video Communications (GIVC), a state-owned company established by China Central Television (CCTV) and China Global Television Network (CGTN). The connections between GIVC and *videostory.com* are further reflected through the network's infrastructure.

AI is used for two key purposes: first, enhancing its perceived legitimacy through consistent visual identity, and second, seeding state narratives while hiding the content's origin. **Generative tools have been used for the creation of profile pictures, website logos, and favicons using Dall-E.** This has been confirmed by the prompts found in the file name of several favicons. **The network also uses AI to paraphrase and translate CGTN content** to produce new, seemingly authentic articles tailored to the targeted audience of each inauthentic outlet.

Evidence of the use of generative tools is visible in several ways. First, error messages and AI prompts have appeared directly on the website. Second, some sites have been populated with unusually large volumes of content within very short timeframes. In addition, manipulated articles and the original CGTN content are often published almost simultaneously, suggesting the likely use of automated processes. **Despite this level of activity, the network has struggled to generate genuine engagement. Although affiliated social media accounts, particularly on Facebook, show thousands of followers, individual posts receive little to no interaction.**

- **Populating content: Paperwall expansion**

Exposed in 2024, the Paperwall IMS is known to launder content originating from the Chinese state through a network of inauthentic news websites leveraged by the public relations firm Haimai and intermediaries such as Times Newswire[57]. Recent investigation unveiled the network's new expansion and its use of automated processes. **Paperwall expanded its infrastructure to include 108 additional domains, targeting 40 new countries with content in 15 new languages**, which marks the operation's largest expansion so far. A recent trend consists in populating many of these websites with content translated from Russian sources, including state-controlled media. This is visible in the second graph where the Paperwall cluster is also connected to *aif.ru*, which is the source amplified by the network.

The quality and timing of the content suggest signs of automation, despite no clear evidence of translation exploiting LLMs. First, the content is frequently translated and republished by Paperwall websites within hours of the original publication. Second, the quality of translation remains poor. Third, the final products at times have residual source text, such as linked article titles or anchor texts revealing the actual source. This automated process also enables the concealment of the content's origin.

CONCLUSION

The analysis and operational instruments presented in this report demonstrate that **a purely defensive or reactive posture is insufficient in the face of a threat shaped and dictated by threat actors**. While it is neither realistic nor feasible to completely stop threat actors from using FIMI, the impact and sustainability of these activities can be significantly reduced. Through disruption, cost imposition and the limitation of operational space, threat actors can be compelled to adapt, reassess and reconsider the viability of their campaigns. At the same time, strengthening societal resilience diminishes the effectiveness and legitimacy of manipulation efforts.

A proactive and deterrence-oriented approach is therefore essential. By acting not only against individual incidents but against the enabling conditions that sustain them, the EU can reduce the space in which FIMI operates. **Building credible deterrence capacity is key to generating tangible and lasting impact.**

This requires a better use of existing instruments, their adaptation and reinforcement where necessary, and, where appropriate, the development of additional tools. The deterrence dimension should be integrated across all levels of counter-FIMI action. Such measures remain firmly grounded in international law and are designed to safeguard information integrity and the freedom to express and access information without manipulation of the digital environment.

Translating this assessment into practice requires a set of concrete operational follow-ups, outlined below.

- **Strengthening data collection and information sharing at more levels:** The complexity and covert nature of FIMI operations require more structured and agile information-sharing across sectors and jurisdictions. Public authorities, law enforcement, cyber threat intelligence organisations, intelligence services and civil society each hold complementary insights that, when combined, strengthen understanding of operational networks and their vulnerabilities. Developing cross-jurisdictional evidence pipelines — including through open-source investigations — would support systematic documentation of unlawful behaviour and enable coordinated follow-up action.
- **Making better use of existing instruments and expanding the FIMI Toolbox:**
    - **Sanctions**: Increasing the impact of sanctions calls for a three-step approach: improving the precision of listings to better target instigators and enablers; strengthening implementation so that designations result in real disruption; and adapting the framework to prevent and address circumvention.
    - **Actions targeting intermediaries, enablers and service providers:** FIMI has a clear business dimension. Commercial entities provide services and capabilities that enable FIMI, while systemic vulnerabilities in platforms and service providers can be exploited by threat actors. Effective responses therefore need to address the different layers of this supply chain. Strengthening information exchange between public authorities and private actors is central to this effort. Maintaining a robust regulatory framework for the online space remains an important component.
    - **Leveraging legal and law enforcement avenues**: The role of law enforcement and judicial authorities can be further integrated into counter-FIMI efforts. Certain FIMI activities intersect with existing legal and criminal frameworks, offering opportunities to use established mechanisms more systematically. At national level, judicial practice can consolidate jurisdiction and contribute to the development of a broader legal basis for countering FIMI. At EU level, studies on existing legal instruments could help identify gaps and possible avenues for strengthening the legal framework.
- **Integrating a deterrence dimension into counter-FIMI:** Building credible deterrence capacity should become an integral part of counter-FIMI action. This entails a shift towards data-driven forward-looking analysis and impact-oriented measures. By embedding deterrence into the design of counter-FIMI efforts, the EU can raise costs, increase uncertainty and force threat actors to reshape and rethink their operations.
- **Strengthening collective response and Member States engagement**: Many of the instruments required to increase impact lie within the competences of Member States. Their activation and effective implementation, supported by EU coordination and cooperation with partners, are essential to maximising the impact of the FIMI Toolbox. Stronger coordination among law enforcement, cyber and intelligence — at both national and European level — is central to improving attribution and disruption. At the same time, as threat actors continue to expand resources devoted to FIMI, sustained and proportionate investment in counter-FIMI capabilities is necessary to scale up response.

The time has come to translate situational awareness into sustained collective action, ensuring that FIMI becomes a high-risk and increasingly unviable tool for those who seek to exploit it.

ANNEX

Annex 1: Detailed deterrence mechanism - Sanctions

(Applicable where EU restrictive measures regimes apply. Sanctions do not criminalise speech as such, but target the providers and economic base of content production, when it concerns FIMI or war propaganda)

Layer	Trigger (sanctions applicability)	Potential effects
1. **Organisational structure** (threat actors, intermediaries, contractors, front organisations)	• Entities or individuals listed under EU sanctions regimes • Organisations owned or controlled by listed persons • Front organisations acting on behalf of sanctioned actor • State-linked influence operators designated under thematic regimes • Financial flows linked to listed persons or entities	**Disruption of organisational structures and legitimacy** • Disruption of corporate, proxy and front structures • Restrictions on travel into the EU for listed natural persons • Reputational and political isolation of enabling entities • Exposure and isolation of intermediaries **Financial and technical disruption** • Asset freeze and prohibition to make funds available to listed individuals and entities. Blocking of payment and technical channels and intermediaries • Disruption of shell companies and procurement networks
2. **Digital infrastructure** (accounts, platforms and logistics)	• Assets, services, media outlets or channels owned or controlled by sanctioned entities • Provision of services prohibited under sanctions (hosting cloud, technical services, consulting, advertising, content distribution)	**Disruption of means, services and dissemination capacity** **Logistical support and dissemination capacity** • Denial of hosting, cloud, and digital services • Disruption of procurement of hardware and software • Blocking of domain registrations and infrastructure provision • Interruption of advertising and monetisation services • Suspension of broadcasting and distribution rights • Restrictions on content distribution and syndication
3. **Content** (outputs)	*Sanctions do not regulate content, instead they target designated actors and the resources and services that enable their activities. Any effect on content dissemination is an indirect consequence of upstream restrictions.*	

Annex 2: Detailed of deterrence mechanism - Law Enforcement

(Applicable where conduct violates EU or Member States law. For law enforcement to seek judicial investigative measures they must first demonstrate the underlying predicate offence that generated the illicit activity)

Layer	Trigger (law violations depending on the MS)	Potential effects
1. **Organisational structure** (threat actors, intermediaries, contractors, front organisations)	• Participation in or support to criminal organisations • Activities conducted by or on behalf of sanctioned entities/individuals • Illegal financing (fraud, covert donations, straw donors, money laundering, concealed use of legal entities to carry out covert political or financial activities…) • Sanctions evasion (circumvention through intermediaries and provision of funds or services to listed entities) • Terrorist financing • Entities and individuals participating in or facilitating cybercrime networks	**Disruption of identities and organisational networks** • Arrest and prosecution of key individuals • Closure of front organisations, shell companies and intermediary structures • Dismantling of local "cells" • Freezing and seizure of funds and assets • Criminal fines and penalties
2. **Digital infrastructure** (accounts, platforms and logistics)	• Fraudulent acquisition of services (hosting, SIM cards, accounts…) • False registration of domains or companies • Illicit data acquisition (e.g. unlawful access to systems, data theft) • Use of infrastructure for electoral interference, subversion of constitutional order or cybercrime (e.g. Hacking, DDoS attacks, altering or deleting data, algorithmic manipulation)	**Disruption of means and systems** **Logistical disruption** • Seizure of servers, hosting, devices… • Shutdown of domains and websites used for fraud or impersonation • Disruption of botnets, coordinated account networks… • Suspension of anonymisation services • Disruption of intermediary and facilitator networks through judicial requests and removal orders to service providers **Financial disruption** • Blocking donation and crowdfunding channels • Asset confiscation
3. **Content** (outputs)	• Cybercrime related conducts (e.g. Hacking, DDoS attacks, altering or deleting data, sabotaging an algorithm…) • Criminal offences affecting individual rights, threats, doxxing, harassment and criminal hate speech • Incitement to violence • Incitement to heavily disturb public order and critical infrastructures • Terrorist and extremist propaganda • Impersonation and fraud • Document forgery • Leaks used as part of a campaign (where linked to unlawful access or coercion) • Coercion and blackmail • Transnational repression • Recruitment for hostile services • Calls for donations or financing for illegal actors	**Disruption of content and amplification mechanisms** • Removal orders of illegal content to service providers • Dismantling of amplification hubs • Disruption of coordinated distribution networks • Judicial preservation and request for data disclosure linked to assets used for disseminating and amplifying content (in order to prepare judicial proceedings and further investigative leads)

ANNEX 3: Detailed deterrence mechanism – Digital regulation

(Applicable under platform Terms of Service and EU digital regulation, such as the DSA. Focus is on risk mitigation)

Layer	Trigger Activities/content that trigger platform obligations under the DSA)	Potential effects
1. **Organisational structure** (threat actors, intermediaries, contractors, front organisations)	*DSA does not apply to threat actors, sponsors, or organisers unless they are themselves regulated service providers.*	
2. **Digital infrastructure** (accounts, platforms and logistics)	• Inauthentic accounts (e.g. Fake accounts, CIB networks, impersonation, misrepresentation of identity or affiliation, multiple-account use) • Non-transparent political or issue-based influence (e.g. Undisclosed or misleading political or organisational affiliation or advertising, missing sponsor or funding disclosure, circumvention of ad transparency) • Platform use creating systemic risks to electoral or civic processes (Use of platform features or amplification undermining election integrity, participation, or democratic debate)	**Disruption of account-based infrastructure** • Referral to service providers and/or removal order for the suspension of repeated offenders, inauthentic, impersonating, or coordinated accounts • Restrictions on political advertising and issue-based influence tools • Platform risk-mitigation measures addressing electoral and civic integrity **Financial disruption** • Demonetisation of revenue-sharing and advertising systems **Expose operational visibility** • Enforcement of political and issue-based transparency requirements • Data access for researchers
3. **Content** (outputs)	• Illegal content (e.g. Terrorist content, incitement to violence, criminal hate speech, doxxing, harassment, fraud, scams, impersonation) • Misleading origin or sponsorship (e.g. undisclosed state-linked or organisational affiliation, false or misleading claims of independence or grassroots origin, concealment of sponsorship or coordination) • Automated or bulk activity in violation of platform's terms of services (Unauthorised automation of posting, liking, amplification, CIBs or bot use) • Manipulation of platform systems (e.g. Engagement manipulation, gaming of ranking or recommender systems, artificial visibility boosting)	**Reduction of reach, visibility, and impact** • Referral to service providers and/or removal order of illegal content • Labelling and contextualisation • Reduced reach of harmful content • Disruption of coordinated campaign rollouts • Limiting cross-platform amplification • Reduction of artificial amplification and reach • Downranking or reduced recommendation of coordinated content

REFERENCES

1 EUvsDisinfo. (2025, September). *Kremlin disinfo surge targets Moldova ahead of elections*. EUvsDisinfo. https://euvsdisinfo.eu/kremlin-disinfo-surge-targets-moldova-ahead-of-elections/

2 Council of the European Union (2025), *Russian hybrid threats: Council sanctions twelve individuals and two entities over information manipulation and cyber attacks*; https://www.consilium.europa.eu/en/press/press-releases/2025/12/15/russian-hybrid-threats-council-sanctions-twelve-individuals-and-two-entities-over-information-manipulation-and-cyber-attacks/

3 Mariana Katzarova (2025), *Rule of fear: silencing dissent and anti-war expression in the Russian Federation in the name of national security. Report of the Special Rapporteur on the situation of human rights in the Russian Federation*; https://docs.un.org/en/A/80/382

4 Reuters (2025), *Russia passes law punishing searches for 'extremist' content*; https://www.reuters.com/world/russia-passes-law-punishing-searches-extremist-content-2025-07-22/

5 Ministry of Finance of the Russian Federation. (2025, November). *Бюджет для граждан 2026–2028*. Ministry of Finance of the Russian Federation. https://minfin.gov.ru/common/upload/library/2025/11/main/Budzhet.pdf

6 Estonian Foreign Intelligence Service. (2026). *International security and Estonia 2026*. Estonian Foreign Intelligence Service. https://www.valisluureamet.ee/doc/raport/2026-en.pdf

7 Schalin, J., & Arts, S. (2026, January). *Bracing for a cold front: Assessing Russian and Chinese strategic objectives and hybrid threat capabilities in the Arctic*. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). https://www.hybridcoe.fi/publications/bracing-for-a-cold-front-assessing-russian-and-chinese-strategic-objectives-and-hybrid-threat-capabilities-in-the-arctic/

8 Forbidden Stories. (2026, February 14). *Propaganda machine: Secret documents reveal Russia's foreign influence strategy across three continents.* Forbidden Stories. https://forbiddenstories.org/propaganda-machine-secret-documents-reveal-russias-foreign-influence-strategy-across-three-continents/

9 DISARM Foundation. (n.d.). *Technique T0076: Distort . DISARMframeworks* (GitHub repository). Retrieved February 24, 2026, from https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0076.md

10 DISARM Foundation. (n.d.). *Technique T0079: Divide. DISARMframeworks* (GitHub repository). Retrieved February 24, 2026, from https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0079.md

11 DISARM Foundation. (n.d.). *Technique T0075: Dismiss. DISARMframeworks* (GitHub repository). Retrieved February 24, 2026, from https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques/T0075.md

12 VIGINUM, & Secrétariat général de la défense et de la sécurité nationale (SGDSN). (2025, May). *Analysis of the Russian information manipulation set Storm-1516.* https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf

13 CheckFirst. (March 2025). *"Pravda" network: Worldwide expansion and LLM, Wikipedia pollution*. CheckFirst. https://checkfirst.network/pravda-network-worldwide-expansion-and-llm-wikipedia-pollution/i

14 EU DisinfoLab. (January 2026). *Building a common operational picture of FIMI: Using IMS to strengthen technical attribution and disruption.* https://www.disinfo.eu/building-a-common-operational-picture-of-fim

15 European External Action Service. (January 2024). 2nd *EEAS report on foreign information manipulation and interference threats: A Framework for Networked Defence*. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

16 Rusinaitė, V. (2025). *Turning strategy into praxis: Lessons in hybrid threat deterrence* (Hybrid CoE Paper 25). The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/turning-strategy-into-praxis-lessons-in-hybrid-threat-deterrence/

17 – North Atlantic Treaty Organization. *What is Deterrence?*. https://www.act.nato.int/activities/deterrence/
– Mazarr, M. J. (2018). *Understanding deterrence*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf

18 – European External Action Service (EEAS) (February 2023) 1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
– European External Action Service. (March 2025). *3rd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations*. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

19 European External Action Service. (January 2024). 2nd *EEAS report on foreign information manipulation and interference threats: A Framework for Networked Defence*. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

20 Ideml

21 Mazarr, M. J. (2018). *Understanding deterrence* (PE-295). RAND Corporation. https://www.rand.org/pubs/perspectives/PE295.html

22 Keršanskas, V. (2020). *Hybrid CoE Paper 2: Deterrence – Proposing a more strategic approach to countering hybrid threats*. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats/

23 European External Action Service. (March 2025). *3rd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations*. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

24 – EU DisinfoLab. (January 2026). *Building a common operational picture of FIMI: Using IMS to strengthen technical attribution and disruption.* https://www.disinfo.eu/building-a-common-operational-picture-of-fimi
– CheckFirst. (February 2026). *Unveiling GRU's information operations troops with OSINT and medals.* https://checkfirst.network/unveiling-grus-information-operations-troops-with-osint-and-medals/

– Tadaweb and Paul Charon, (October 2025) Baybridge – Anatomy of a Chinese Information Influence Ecosystem, Focus 3, IRSEM. https://www.irsem.fr/storage/file_manager_files/2025/10/focus-3-charon-a4-ok.pdf
- A. Dek et al. ‚Mapping the online manipulation economy.Science390,1112-1114(2025). DOI: 10.1126/science.adw8154. https://www.science.org/doi/10.1126/science.adw8154
– Recorded Future. (2025). *Malicious Infrastructure Finds Stability with aurologic GmbH.* https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-1106.pdf
– Qurium. (n.d.). *Exposing the evil empire of doppelganger disinformation.* https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/i

25 EU DisinfoLab. (January 2026). *Building a common operational picture of FIMI: Using IMS to strengthen technical attribution and disruption.* https://www.disinfo.eu/building-a-common-operational-picture-of-fimi

26 Keršanskas, V. (2020). *Hybrid CoE Paper 2: Deterrence – Proposing a more strategic approach to countering hybrid threats*. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats//

27 Global Disinformation Index https://www.disinformationindex.org/
NewsGuardTech https://www.newsguardtech.com/

28 Nimmo, B. and Hutchins, E. (March 2023) Phase-based Tactical Analysis of Online Operations. Working Paper of the Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations
Miller, C. (2024). *Directing responses against illicit influence operations (D-RAIL).* EU DisinfoLab. https://www.disinfo.eu/publications/directing-responses-against-illicit-influence-operations-d-rail
DISARM Foundation. *DISARM Framework.* https://www.disarm.foundation/framework

29 Europol (2025), European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

30 Idem

31 European Union. Social Design Agency — EU sanctions tracker. https://data.europa.eu/apps/eusanctionstracker/subjects/155817

32 European Union. *Tigerweb* — EU sanctions tracker. https://data.europa.eu/apps/eusanctionstracker/subjects/177847

33 European Union. *John Mark Dougan* — EU sanctions tracker. https://data.europa.eu/apps/eusanctionstracker/subjects/180200

34 Europol. (2025, January 21). *Cybercrime service takedown: 7 arrested*. Europol. https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

35 Europol. (2025, January 22). *Islamic State propaganda machine hit by law enforcement in coordinated takedown action.* Europol. https://www.europol.europa.eu/media-press/newsroom/news/islamic-state-propaganda-machine-hit-law-enforcement-in-coordinated-takedown-action

36 AP News. (2025, January 21). *Europol-coordinated operation disrupts NoName057(16) cybercrime group linked to pro-Russian activity.* AP News. https://apnews.com/article/europol-hackers-cybercrime-russia-ukraine-42d98dabdc0182dac4bd4c80d880cdb4

37 Meta. (2025). Adversarial threat report: Q2–Q3 2025. Meta Transparency Center. https://transparency.meta.com/sr/Q2-Q3-2025-Adversarial-threat-report

38 Europol. (2025, March 12). *Europol spearheads largest referral action against online hate speech*. Europol. https://www.europol.europa.eu/media-press/newsroom/news/europol-spearheads-largest-referral-action-against-online-hate-speech

39 TikTok. (2025). *Covert influence operations: Overview of enforcement actions.* TikTok Transparency. https://www.tiktok.com/transparency/en/covert-influence-operations

40 European External Action Service. (March 2025). *3rd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations*. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_eni

41 EU DisinfoLab. (January 2026). *Building a common operational picture of FIMI: Using IMS to strengthen technical attribution and disruption.* https://www.disinfo.eu/building-a-common-operational-picture-of-fimi

42 Viginium - Secrétariat général de la défense et de la sécurité nationale. (January 2026). *Définitions et objectifs du concept de « mode opératoire informationnel » (MOI)*. https://www.sgdsn.gouv.fr/publications/definitions-et-objectifs-du-concept-de-mode-operatoire-informationnel-moi

43 EU DisinfoLab , Doppelganger Hub (2026) https://www.disinfo.eu/doppelganger-hub

44 VIGINUM. (2024, June 10). *Matriochka : une campagne prorusse ciblant les médias et la communauté des fact-checkers*. Secrétariat général de la défense et de la sécurité nationale (SGDSN). https://www.sgdsn.gouv.fr/publications/matriochka-une-campagne-prorusse-ciblant-les-medias-et-la-communaute-des-fact-checkers
CheckFirst. (2024, June 4). *Operation Overload: How pro-Russian actors flood newsrooms with fake content and seek to divert their efforts*. https://checkfirst.network/operation-overload-how-pro-russian-actors-flood-newsrooms-with-fake-content-and-seek-to-divert-their-efforts/

45 EUvsDisinfo. (2024, May 2). *Building a false façade*. EUvsDisinfo. https://euvsdisinfo.eu/building-a-false-facade/
Insikt Group. (2024, May 9). *Russia-linked CopyCop uses LLMs to weaponize influence content at scale* (Cyber Threat Analysis). Recorded Future. https://www.recordedfuture.com/research/russia-linked-copycop-uses-llms-to-weaponize-influence-content-at-scale

46 Portal Kombat. *Pravda Dashboard*. https://portal-kombat.com/

47 Nimmo, B., Eib, C. S., & Tamora, L. (2019, September 25). *Spamouflage: Cross-platform spam network targeted Hong Kong protests*. Graphika. https://graphika.com/reports/spamouflage/

48 Graphika. (August 2025). *Falsos Amigos*. https://graphika.com/reports/falsos-amigos

49 Armenpress. (March 2025). *Armenian parliament adopts EU bill at second reading,* original at https://armenpress.am/en/article/1215464

50 Ministry of Foreign Affairs of the Republic of Azerbaijan. (March 2025). *News no. 10525*. https://mfa.gov.az/en/news/no10525

51 Peace Dialogue Armenia. (November 2025). *Armenia's Information Frontlines: Trends, Threats, and Narratives to Watch*. https://peacedialogue.am/en/wp-content/uploads/sites/2/2025/11/Narrative_Analysis.pdf

52 Digital Forensic Research Lab. (December 2025). *Kremlin-originated campaigns target Armenia with Ukrainization narrative*. https://dfrlab.org/2025/12/23/kremlin-originated-campaigns-target-armenia-with-ukrainization-narrative/

[53] Institute for Strategic Dialogue. (December 2023). *Pro-CCP network 'Spamouflage' weaponizes Gaza conflict to spread anti-US sentiment*. https://www.isdglobal.org/digital-dispatch/pro-ccp-network-spamouflage-weaponizes-gaza-conflict-to-spread-anti-us-sentiment/

[54] Meta. (2023). Adversarial Threat Report, Second Quarter 2023. https://transparency.meta.com/metasecurity/threat-reporting

[55] Graphika. (August 2025). *Falsos Amigos*. https://graphika.com/reports/falsos-amigos

[56] Idem.

[57] Molter, V. (2024, November 22). *Seeing through a GLASSBRIDGE: Understanding the digital marketing ecosystem spreading pro-PRC influence operations*. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/glassbridge-pro-prc-influence-operations?hl=en

Discover the

FIMI EXPLORER

on EUvsDISINFO

EU VS DISINFO

THE JEWELS FROM THE LOUVRE WERE STOLEN BY A UKRAINIAN OLIGARCH

REALLY?

The Kremlin wants you to believe it.

Here's why.

EU VS DiSiNFO

DON'T BE DECEIVED

European Union
EXTERNAL ACTION