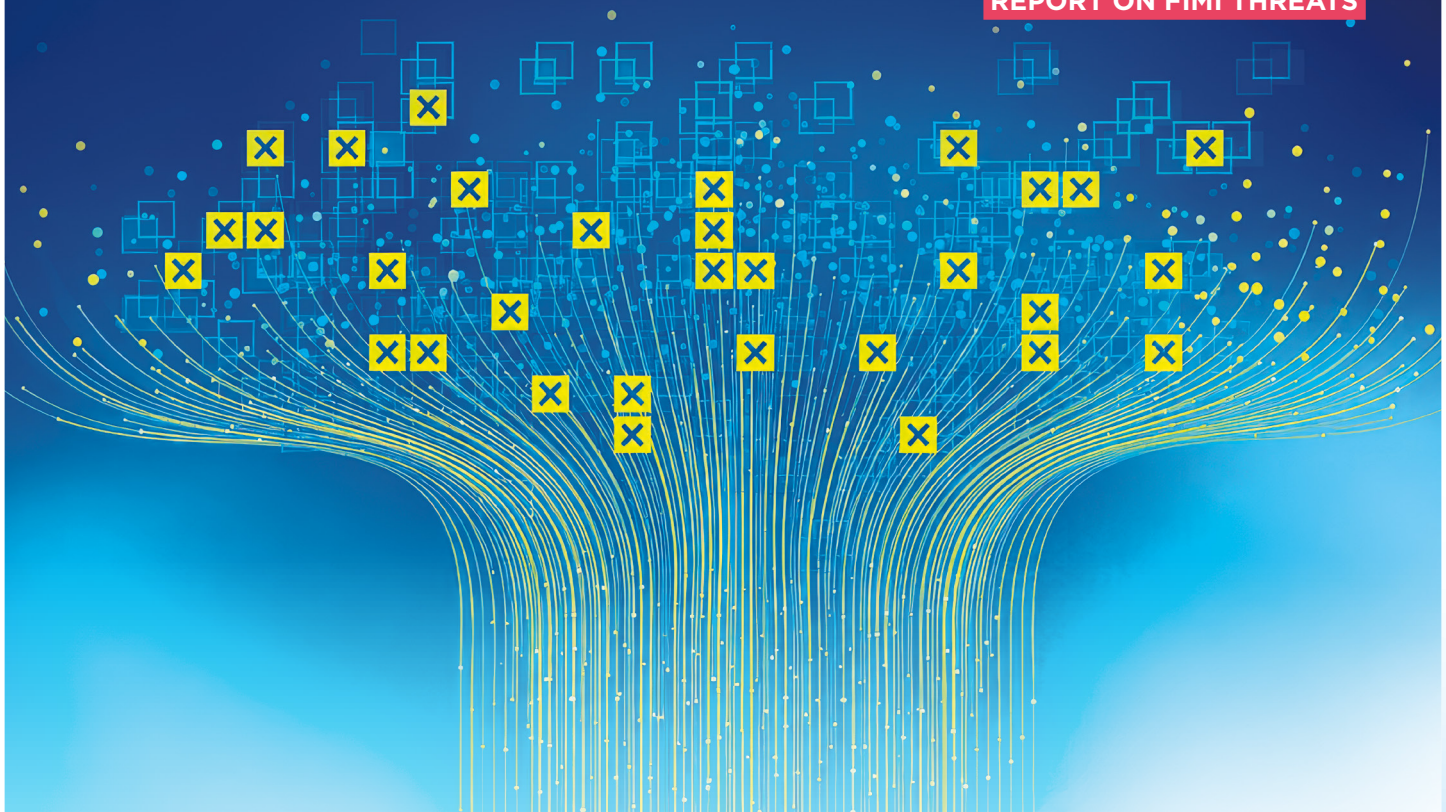
EEAS Policy Planning and Strategic Communication (GII.GLOBAL.STRAT.DMD)
& Center for Countering Disinformation (CCD)

REPORT ON FIMI THREATS



Beyond the Battlefield: **Russia's Information War Against Ukraine's European Future**

A joint analysis by the European External Action Service (EEAS)
and the Center for Countering Disinformation (CCD)
on FIMI targeting Ukraine's accession process to the EU

European Union
EXTERNAL ACTION

CENTER FOR COUNTERING
DISINFORMATION

June 2026

FOREWORD BY HIGH REPRESENTATIVE/ VICE PRESIDENT KAJA KALLAS

Ukraine has made its strategic choice to become a part of the European Union. Since achieving candidate status in 2022 and opening accession negotiations in 2024, Ukraine has consistently demonstrated its determination to advance reforms and firmly anchor its future firmly within our Union. This effort is being undertaken in wartime, as the Ukrainian people defend their country's sovereignty and territory against Russia's invasion with extraordinary courage and at immense human cost.

Russia understands what Ukraine's accession to the EU would mean. A democratic, sovereign and successful Ukraine within the European family, on Russia's border, represents a strategic failure of the Kremlin's imperial ambitions in Europe. This is why Russia systematically seeks to undermine trust in Ukraine's reforms, weaken support for enlargement, and sow divisions within Ukraine, across the EU, and globally.

This report is the product of close cooperation between the European External Action Service and the Center for Countering Disinformation, a working body of Ukraine's National Security and Defense Council. It reflects our shared commitment to identifying, analysing and exposing foreign information manipulation and interference (FIMI) targeting Ukraine's European future. It also demonstrates how far we have come in strengthening our collective resilience against such threats.

Russia's FIMI operations are neither isolated nor accidental. They are deliberate, coordinated, and persistent. They seek to exploit fears related corruption, security, identity and economic costs. They target audiences both in Ukraine and across EU Member States, aiming to undermine Ukraine's accession to the EU. These campaigns evolve continuously, including through the growing use of AI-powered tools and increasingly sophisticated information manipulation techniques. Yet Russia's efforts reveal an important truth: the Kremlin fears Ukraine's success.

We must remain clear-eyed about what is at stake. This is not only about Ukraine. It is about the security, unity and credibility of Europe itself. Enlargement has always been a geopolitical investment in peace, stability and democracy. Today, that is truer than ever.

The European Union will continue to stand with Ukraine. Together with our Ukrainian partners, the EEAS will further strengthen our collective resilience by exposing Russia's blatant manipulation efforts and raising the costs through coordinated countermeasures. Ukraine's future is in Europe, and no hostile information operation will change that.

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

FOREWORD BY HEAD OF THE OFFICE OF THE PRESIDENT OF UKRAINE KYRYLO BUDANOV

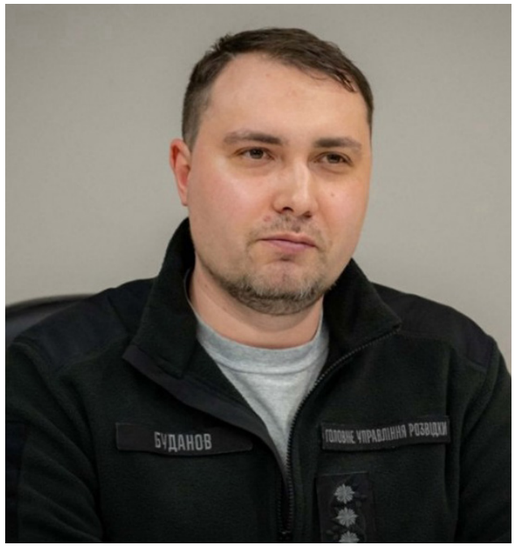
Today, in the midst of the full-scale war unleashed by an aggressor state, Ukraine finds itself at a stage where every step on the path to the European Union is both a test and a testament to our resolve. By defending our sovereignty and territorial integrity, we are upholding our right to choose our own future and to build a strong, democratic Ukraine.

The information component became an integral part of military operations as early as the 20th century. The dangers to society and the state posed by information warfare have become a real threat to their stability. Hence the need arose for effective countermeasures and the development of methods to combat the enemy in the information sphere. The British journalist and organiser of counter-propaganda operations against Nazi Germany, Sefton Delmer, once employed an approach that involved presenting approximately 80% of real facts, whilst including 20% of disinformation with an emotional undertone. This is because propaganda works most effectively when it appeals to the emotions, fears and fatigue of society. That is precisely why Russia's modern FIMI operations are aimed not only at spreading falsehoods, but also at undermining trust in democratic institutions and Ukraine's European choice.

Today, Russian FIMI operations follow a similar logic – using digital platforms, anonymous networks and emotional manipulation to discredit democratic institutions, undermine trust in reforms and attempt to weaken Ukraine's European choice.

This report, compiled by the Center for Countering Disinformation in partnership with the European External Action Service, demonstrates the scale and systematic nature of Russia's destructive activities in the information sphere. Analytical data confirms that FIMI is not a collection of isolated disinformation messages, but a powerful infrastructure comprising state and quasi-state media, anonymous channels, proxy networks, a pseudo-expert community, repetitive narratives and targeted exploitation of the audience's emotional vulnerabilities.

In view of this, our joint response must be equally robust and systematic: strategic communication, explaining the European integration process, identifying FIMI operations, active cooperation with digital platforms, and sanctions against key actors influencing the information landscape.



At the same time, we must remain open to constructive criticism and ensure the transparency of democratic dialogue, so that our response to FIMI serves as a shield against misinformation rather than as censorship.

Ukraine has chosen the path of European integration as a sovereign, conscious and irreversible choice. We are ready to resolutely defend democratic values, drawing on our strength, forged in the struggle for freedom. The support of our partners, joint work to increase resilience to disinformation and the development of analytical tools are key components of our victory. Commitment to democracy and consistency in reforms are our powerful weapons against any disinformation.

Ukraine's European integration is the result of long-term work, difficult decisions and the resilience of Ukrainian society. Despite the full-scale war, Ukraine continues its path towards the EU, defending its independence, democratic values and the inalienable right to be part of the European community.

Kyrylo Budanov,
Head of the Office of the President of Ukraine

TABLE OF CONTENTS

Methodological note_*Both the EEAS and the CCD rigorously use OSINT practices to carry out their investigations on FIMI in full respect of legal boundaries and ethical standards. The data collection has been done both through media and social media monitoring tools, as well as manually. The data used in this report are provided for informational purposes and are based on the EEAS' and CCD's strategic monitoring activities and 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. The analysis is reflective of the authors' judgment at the time of publication and is subject to revision. The key terminology used can be found in* ***Annex 1****.*

EXECUTIVE SUMMARY

Russia's war of aggression against Ukraine has reshaped Europe's security environment. In this context, the accession of Ukraine and other candidate countries to the European Union is not merely a policy objective: it is a strategic security imperative, for Ukraine and for the EU alike. By advancing democracy, stability, and security across the continent, the EU enlargement process strengthens not only the countries that join but the Union as a whole. It is precisely because this process carries such weight that Russia opposes it and works actively to derail it.

For Ukraine, accession is the strongest available guarantee of its long-term security. EU membership is about far more than economic integration: it means becoming part of a political, economic, and security community built on shared values, solidarity, and mutual support. Since applying for membership only four days after the start of Russia's full-scale invasion, Ukraine has made remarkable progress under exceptionally difficult conditions, gaining candidate status in 2022, opening accession negotiations in 2024, and completing its first screening process the following year.

For the EU, a stable and prosperous Ukraine is equally a matter of long-term security. Russia has consistently opposed Ukraine's closer integration with the EU, and it is no secret that Russia views this process as a threat to its influence in Ukraine and in the wider region. The Kremlin used the planned signature of the EU-Ukraine Association Agreement, as one of the pretexts to invade Ukraine in 2014. Russia pursues this opposition through two parallel means: military aggression on the ground, and sustained FIMI and hybrid campaigns designed to undermine Ukraine's European aspirations and erode support for enlargement across Europe.

This report examines the latter: it focuses on Foreign Information Manipulation and Interference (FIMI) efforts directed at Ukraine's accession to the EU between January 2025 and May 2026. It is the product of joint work by the European External Action Service and the Center for Countering Disinformation (CCD), a working body of Ukraine's National Security and Defense Council. Our cooperation clearly shows a shared commitment to identifying, analysing, and exposing FIMI, as well as responding to it in close cooperation. Two complementary analyses examine this threat from different viewpoints. The CCD documents how Russia targets Ukrainian audiences domestically to erode internal support for the EU path. The EEAS examines how the same apparatus operates across European audiences to undermine political and public backing for enlargement. Together they describe a coordinated, multi-layered, and increasingly complex industrial-scale operation rather than a series of isolated incidents.

The CCD and EEAs have mapped Russia's information assets across four blocks of the FIMI architecture spanning from covert to overt and attributed to non-attributed. Official state channels set the messaging, while deniable state-linked and state-aligned assets launder, repurpose and amplify it. The structure is the same for both audiences, what differs is how accessible each layer is to audiences. Three mutually reinforcing narratives recur regardless of audience: incompatibility in values (Ukraine as corrupt and the EU as imposing a moral doctrine), leaders detached from their people (accession is portrayed as an elite self-serving process), and accession framed as a loss for everyone (costly, risky and causing insecurity for both sides). Finally, the analysis also highlights a key asymmetry: while targeting of Ukrainian audiences continues steadily, a growing share of resources is now aimed at EU and international audiences — likely because Ukrainian support for membership remains high, whereas EU public and political opinion is the more decisive variable for enlargement.

Risks of FIMI remain similar across information environments: AI-enabled mass production of misleading content, cross-platform amplification, and information-laundering models significantly lower the cost and raise the reach of online manipulation. Amplification of decontextualised quotes from EU officials risk creating a false impression of institutional consensus against Ukraine's accession. Electoral cycles and breaking security incidents keep being leveraged by Russia's FIMI machinery. Content depicting Ukrainian refugees as a threat carries a tangible risk of inciting real-world violence. The rebranding of sanctioned outlets shows that regulatory responses need to meet the fast-paced reality of the current information environment.

Countering Russian FIMI targeting Ukraine's EU accession is part of a wider effort by the EEAS, CCD and international partners in the EU and beyond to respond to Russian FIMI. Enabling responses to FIMI requires a sustained, evidence-based and coordinated response between Ukrainian institutions and EU partners. This is only possible by deepening structured, standardised exchanges on FIMI infrastructures, influence techniques and actors involved. This analytical foundation serves as a basis for a broader toolkit of countermeasures: more systematic deterrence-oriented responses, like sanctions against FIMI actors and their assets, making good use of digital regulations, strengthened cooperation with law enforcement, and overall societal resilience-building to connect with audiences and explain how FIMI works in practice.

SABOTAGING THE PROCESS: HOW RUSSIA TARGETS UKRAINIAN AUDIENCES TO UNDERMINE EU MEMBERSHIP

AN ANALYSIS BY THE CENTER FOR COUNTERING DISINFORMATION (CCD)

Following the formal opening of accession negotiations in June 2024, Ukraine's path to EU membership entered a more technical and institutionally demanding phase. Alignment with the acquis communautaire, sectoral reforms and the preparation of negotiation clusters moved to the centre of the process, and with them, Ukraine's European integration became a distinct and sustained target of FIMI. The sensitivity of the issue is structural: it concentrates expectations around reconstruction, security guarantees, economic modernisation and Ukraine's long-term geopolitical orientation in a single policy frame, making it uniquely exploitable.

For the period from January 2025 to May 2026, the CCD monitored the information environment around Ukraine's accession through its detection tool and has identified 244 000 publications amounting 1.39 billion views. Within this volume, 2,660 sources displayed signs of inauthentic behaviour, including synchronised dissemination, coordinated reactions to news events and artificial amplification. By analysing the sources and nature of the content, as well as the dissemination patterns, the CCD has documented sustained and coordinated FIMI efforts rather than a series of isolated disinformation incidents - one characterised by a persistent combination of harmful narratives, inauthentic amplification infrastructure and adaptive content formats operating across platforms.

The objective of this activity goes beyond discrediting individual reforms. It is aimed at systematically weakening the perceived legitimacy, feasibility and strategic value of EU accession among Ukrainian audiences, while simultaneously advancing broader Russian strategic communication goals: portraying the EU as self-interested, Ukraine as institutionally dependent, and the accession process as either impossible, harmful or externally imposed.

This section analyses the key narratives deployed to discredit Ukraine's accession, the strategic logic underpinning them, the actors and infrastructure involved in their dissemination, and the techniques, tactics and procedures (TTPs) used to produce, adapt and amplify the observed activity.

THEMATIC ARCHITECTURE OF NARRATIVES

Narrative clustering reveals **four mutually reinforcing blocks within Russian FIMI activity targeting Ukraine's EU accession**. Their cumulative logic is consistent: the EU is self-interested and cynical; Ukraine is weak and externally controlled; reforms are harmful; and accession is unrealistic.

1. **"The EU prolongs the war to weaken Russia"**: This narrative inverts the causal link between Russian aggression and Ukraine's need for support, repositioning the EU as the actor responsible for Ukrainian casualties. The strategic aim is to decouple Ukraine's security interests from its European integration course and erode public willingness to accept the reforms.

2. **"EU Member States seek to partition Ukraine"**: Fabricated scenarios, such as Franco-British partition plans for Ukrainian territories, or Hungary's alleged "Operation Turul" to take Transcarpathia, exploit territorial anxieties and historical memory to recast partner states as covert annexationists. Messaging is localised for specific regional audiences, targeting directly the EU Member States most critical to Ukraine's accession trajectory.

3. "**EU integration disguises external control":** FIMI actors reframe regulatory reforms as Brussels-imposed coercion rather than modernisation and rendering each technical requirement legible only as immediate harm to citizens. One representative case is the sustained Russian disinformation campaign around draft law No. 14025 on digital platform taxation[1].

4. "**Ukraine is incompatible with EU values"**: Real reform challenges are selectively amplified and remarks by European officials systematically decontextualised to suggest structural incompatibility with membership. This also builds on narratives related to corruption in the Ukrainian government. For domestic audiences this normalises disillusionment; for external ones it reinforces the image of Ukraine as a permanently troubled candidate.

These narratives serve three operational objectives: **eroding internal cohesion in Ukraine through contradictory emotional triggers; consolidating a "failed state" framing to weaken both domestic trust and external support and undermining bilateral relationships between Ukraine and key EU Member States**. The sophistication lies less in individual fabrications than in their repetition and deliberate contradiction working in concert to render the accession process incrementally less credible in the eye of Ukrainian audiences.

FIMI ACTORS AND DISSEMINATION INFRASTRUCTURE

The dissemination infrastructure of the observed Russian FIMI activity consists of four analytical layers[2]: **official state channels, state-controlled outlets, state-linked FIMI assets, and state-aligned FIMI actors.**

Openly **state-official and state-controlled Russian sources are used less frequently for direct influence on Ukrainian audiences due to broadcasting restrictions and reduced trust.** However, they often serve as primary sources of narratives, interpretations, or fabricated claims that are subsequently repackaged and amplified by state-linked, or state-aligned actors in forms more adaptable to the Ukrainian information space.

Such narrative-setting functions are most commonly performed by major Russian state media and official news agencies, including RIA Novosti, TASS, and RT, as well as Telegram channels of Russian officials and state institutions, including "Дмитрий Медведев" (Dmitry Medvedev), "Кремль. Новости" (Kreml. Novosti), "Мария Захарова" (Maria Zakharova), "МИД России" (Russian Foreign Ministry), "Минобороны России" (Ministry of Defence of Russia), "РОДИОН МИРОШНИК" (Rodion Miroshnik) and others.

particular Другая Украина (Drugaya Ukraina)[4].

Their function is to disseminate pseudo-insider information, manipulative interpretations of domestic political processes and messages discrediting Ukraine's leadership and international partners.

Finally, **state-aligned actors**, including sanctioned public figures, provide personalised amplification by presenting the same messages as "alternative" analysis or domestic criticism. In this context, the channels of Oleksii Arestovych, Diana Panchenko, and Anatolii Sharii regularly appear in the dissemination environment around anti-European or anti-Ukrainian narratives. Their role is not limited to repeating claims; they add emotional interpretation and personalised credibility for audiences that may distrust overt Russian sources.

A separate role within the category of state-aligned actors is played by pseudo-local ecosystems, including ZOV/Pravda and assets of the *На самом деле* (Na samom dele) network, which target audiences in different Ukrainian cities. Such resources help localise Russian FIMI narratives by connecting national-level claims to specific regional fears. According to open-source data, the ZOV/Pravda network, associated with Yevhenii Shevchenko[5] network, belongs to the same infrastructure of Portal Kombat (a Russia-aligned

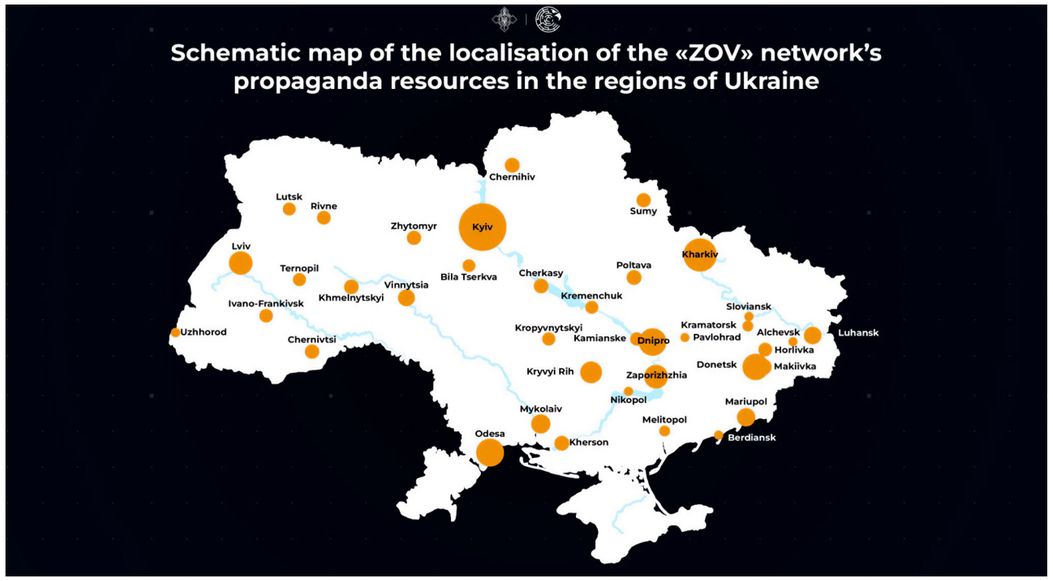


***Figure 1**_The CCD mapped the Russian propaganda network called 'ZOV' and detected content localised for 23 regions of Ukraine and 17 major Ukrainian cities. The network consists of 68 websites, 40 Telegram channels, and 40 VKontakte pages.*

State-linked actors then adapt these messages to specific audiences through anonymous Telegram channels, pseudo-local websites, and social media accounts. This ecosystem includes Telegram channels such as Резидент (Rezident), Легитимный (Legitimnyy), Картель (Kartel), Сплетница (Spletnitsa), and others, which the Security Service of Ukraine has linked to the 85th Main Special Service Centre of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation[3]. It also includes resources associated with the collaborator Viktor Medvedchuk, in

Information Manipulation Set (IMS)[i], for which there is no formal attribution yet[6]). Similarly, *На самом деле* sources are connected with the state-aligned InfoDefense ecosystem through shared feedback infrastructure (see Figure 1 & 2).

As a result, the distinction between state-linked and state-aligned actors is analytical rather than absolute. In operational terms, these actors often operate across overlapping platforms and audiences, where similar messages can be circulated, adapted and mutually reinforced

i. See definition in Annex 1

without always requiring direct coordination. This layered structure allows Russian FIMI activities to obscure direct attribution, test messages through lower-visibility channels, amplify successful frames through larger accounts, and recycle narratives after they are publicly exposed.

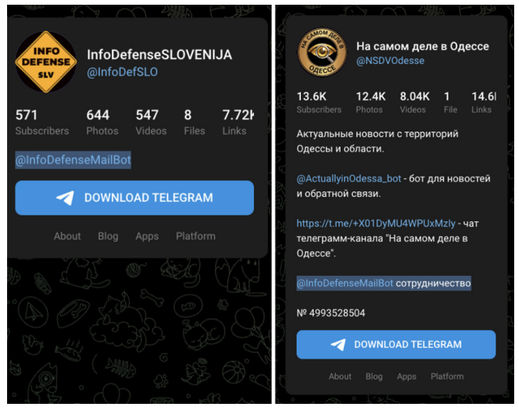


***Figure 2**_Example of the same contact bot being mentioned in the Telegram channels of the InfoDefense network and На самом деле (Na samom dele).*

TECHNIQUES, TACTICS AND PROCEDURES OF INFLUENCE

Throughout the monitored period, Russian FIMI activities against Ukraine's EU accession became more scalable and adaptive. Their logic corresponds to the broader FIMI approach: the aim is not only to spread false information, but also to erode trust, create information noise, exhaust audiences and reduce the ability to distinguish reliable content from manipulative content. The following TTPs were particularly visible in the observed FIMI cases.

The first technique is amplification by sources displaying signs of artificial amplification. Within the dataset of mentions for the period from January 2025 to April 2026, 2,680 sources displayed such signs across Telegram, VK, X, Facebook, YouTube, TikTok, Threads and websites. These sources helped increase the visibility of selected messages, create the impression of organic public concern and accelerate the spread of content across platforms. Inauthentic amplification is especially relevant for topics where the objective is not only to convince, but also to create the impression that distrust toward the EU accession process is widespread.

The second technique is **mapaganda** - manipulative use of maps to legitimise desired narratives. It includes exaggerating Russian territorial gains, distorting the front line, visualising alleged "zones of responsibility" or creating scenarios of the "redistribution" of Ukrainian territories among external actors. In the accession context, mapaganda supports the claim that partners are preparing to divide Ukraine or that Ukrainian sovereignty is already being negotiated without Ukraine. Such visual products are effective because they simplify complex issues into an apparently authoritative image. (see Figure 3[7])

The third technique is **selective exploitation of real statements by European politicians, officials, experts or media.** Individual quotations are taken out of context to suggest

***Figure 3**_An example of 'mapaganda'. The Telegram post uses an image of a map to falsely claim that a Chairman of a Polish-language teachers' association in Volyn allegedly distributed materials showing Volyn as part of Poland and that the local population was being prepared for the region's separation from Ukraine.*

that Ukraine has no accession prospects, that the West is tired of supporting Ukraine or that hidden contradictions exist between Kyiv and European partners. The manipulation often relies on distorted translation, selective emphasis or arbitrary generalisation of one comment into a supposed institutional position. This tactic is particularly damaging because it uses authentic fragments to legitimise false conclusions.

For example, this tactic was visible in content that reframed Poland's commemoration of the tragedy of Volhynia and Eastern Galicia as evidence of alleged political pressure and future territorial ambitions toward Ukraine. The publication selectively linked the Polish parliament's decision to establish 11 July as a day of remembrance for the victims with statements by President Andrzej Duda regarding the Rzeszów logistics hub and with legal provisions granted to Polish citizens in Ukraine after 2022. By combining these separate issues, FIMI actors sought to present Poland's remembrance policy, logistical role in supporting Ukraine and bilateral legal arrangements as signs of a hidden ultimatum, deeper Polish influence and potential future territorial claims against Ukraine[ii].

The fourth tactic is **event-hijacking**: it includes the use of real events like EU institutional decisions, international conferences, anniversaries, negotiations or high-profile statements to scale destructive narratives. FIMI actors integrate such events into pre-existing narratives within a short time frame. The same patterns can be activated whenever public attention to the EU accession reforms in Ukraine increases. For example, it has been detected in content that misused public statements on

ii. Figure 3 shows how the same historical event can be used through two different techniques by FIMI actors to try and reach two different influence objectives: 1- allege loss of territorial control by Ukraine; 2- discredit political figures in the EU and UA simultaneously

Ukraine's EU integration to reinforce the pre-existing narrative that Western support for Ukraine is declining[8]. The publications selectively combined President Zelenskyy's statement on the importance of EU membership for Ukraine with Polish Foreign Minister Radosław Sikorski's remarks that Ukraine would still need to meet all accession conditions. These statements were reframed not as part of a normal accession debate, but as evidence that the "honeymoon period" of support for Ukraine had ended and that Kyiv had allegedly lost room for manoeuvre.

The fifth technique is **localisation**. Misleading claims are adapted to specific regional, social, or thematic contexts. For example, the broader narrative that EU Member States allegedly seek to weaken and divide Ukraine was adapted through content claiming that Hungary had alleged plans to take Zakarpattia or Romania was preparing to occupy Bukovyna. Localisation increases plausibility because the message is connected to familiar historical or regional sensitivities[9].

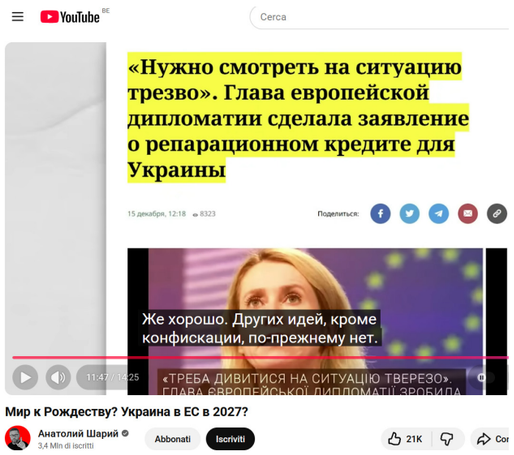


***Figure 4**_A state-aligned YouTube channel of Anatolii Sharii discussing policy debates and statements by European political actors, while framing them through speculative conclusions.*

The sixth technique is **the use of pseudo-experts**. Individuals with questionable expertise or doubtful reputation are used to present messages aligned with Russian propaganda as independent analysis. At the same time, references to real academic publications, analytical materials or international reports may be selectively used to support manipulative conclusions. For example, this technique was visible in content by Anatolii Sharii(see Figure 4), who commented on the issue of frozen Russian assets, EU decision-making and possible reparations. The discussion referred to real policy debates and statements by European political actors but framed them through speculative conclusions: that the use of frozen Russian assets would allegedly place the burden on European taxpayers, damage the EU financial system and demonstrate political divisions within Europe. In this way, a complex legal and financial issue was presented as commentary that reinforced the narrative that EU support for Ukraine is costly, risky and politically destabilising.

Taken together, these TTPs indicate that **Russian FIMI against Ukraine's accession to the EU relies increasingly less on a single "fake" in the narrow sense and increasingly more on the construction of a manipulative information environment**. Its purpose is to overload the audience with contradictory messages, undermine trust in official sources, create the illusion of widespread anti-European sentiment and make negative assessments of accession appear natural rather than coordinated.

RISK ASSESSMENT AND IMPLICATIONS FOR RESILIENCE

The CCD assesses that the observed activities could have medium- to long-term risk implications. The more frequently European integration is connected with fear, coercion, territorial loss, corruption or endless war, the easier it becomes for hostile actors to make the accession process appear distant from the everyday interests of Ukrainian citizens. This is particularly relevant because accession reforms are often complex, lengthy and vulnerable to misinterpretation.

The main risk for Ukrainian audiences is not a sudden collapse of support for the EU course, but the accumulation of doubts in specific segments of society. These include audiences affected by war-related fatigue, economically vulnerable groups, residents of regions targeted by pseudo-local narratives, and users who consume information primarily through messaging platforms, like Telegram channels, or short video platforms, where they receive various information at a very fast pace. For these audiences, repeated exposure to similar messages may create a perception that European integration is associated mainly with obligations and risks rather than with security, institutional resilience and long-term development.

Another risk is the normalisation of anti-European interpretations inside domestic political debate. Russian FIMI actors seek to insert their frames into legitimate discussions about reforms, governance, corruption, public finances or relations with partners. Once such frames are reproduced by local actors without attribution to the original hostile source, the claims become more resilient and harder to expose. This is why response measures should focus not only on debunking, but also on identifying how they are laundered through pseudo-expert, pseudo-local and personalised media channels.

For international partners, the risk lies in the cross-border adaptation of the same narrative architecture. Messages targeting Ukrainian audiences may later be repurposed for audiences in EU Member States, where they can be used to question enlargement fatigue, financial support for Ukraine or the political feasibility of accession.

Conversely, statements from European debates are selectively imported back into the Ukrainian information space to create the impression that the EU has already lost confidence in Ukraine.

A resilience-oriented response should therefore combine three levels: analytical detection of FIMI activities, public communication that explains the accession process in understandable terms, and policy measures targeting the actors and infrastructure involved in manipulation. The response should preserve a clear distinction between legitimate criticism of reforms and coordinated FIMI activity. This distinction is important for protecting democratic debate while preventing hostile actors from abusing it to undermine trust in Ukraine's European path.

POISONING THE WELL: HOW RUSSIA MANIPULATES AUDIENCES ACROSS THE EU AGAINST UKRAINE'S EU ACCESSION

AN ANALYSIS BY THE EUROPEAN EXTERNAL ACTION SERVICE (EEAS)

Over the past year and a half, Ukraine remained a constant target of Russian FIMI efforts as evidenced by the number of cases collected in the 4th EEAS Report on FIMI Threats[10]. Since Ukraine was granted EU candidate status in 2022 and even more since the opening of the accession process in 2024, FIMI attacks against the country were often directed at European and international audiences, with the aim of sabotaging the public perception of this process.

The EEAS has investigated around 80 incidents, between January 2025 and May 2026, that are linked to the topic of Ukraine's accession to the EU or to themes that are relevant to it. Such incidents were collected using the FIMI methodology[11] and show steady patterns of behavioural and narrative alignment.

While the previous section of this report written by the CCD exemplifies how Ukraine and its people are targeted by Russia in their information space, the following section focuses on how the Russian FIMI apparatus tries to influence audiences in the EU and internationally into rejecting the accession process.

Russian FIMI attacks on Ukraine rely on a few simple recurring themes that can be clustered around three overarching aims: 1- target the values, to weaken social cohesion; **2- target the leaders and the people** of both EU and Ukraine, and; **3- target the money**, to decrease acceptance for economic support to the country. While such attempts have already been reported since 2024[12], the activity in the information space has been marked by the use of different tactics techniques and procedures. For example the use of artificial intelligence (AI) to generate content has grown in the past year, and the assets used by the threat actor have also evolved with an increased focus on the use of Information Manipulation Sets (IMS)[13].

TARGET THE VALUES

A core feature of Russian FIMI efforts targeting directly or indirectly Ukraine's EU accession process is the large amount of content developed and disseminated to flood the European information environment, **with a focus on German, French, and Polish audiences in the EU**. In order to enable large-scale content creation and dissemination, Russian FIMI efforts heavily rely on generative AI and coordinated inauthentic behaviour networks (CIBs), for example those used by the IMS called Operation Overload[14] (also known as Matryoshka[15]). Notably, AI capabilities are enabling the threat actor to mass-produce deceptive content at low cost, further facilitating its rapid diffusion across platforms and efficiently reach different audience segments. The resort to AI is notably largely identified in activities attributed to Russian IMSs and illustrate their prioritisation of volume rather than quality. This characteristic is rather established behaviour across Russian FIMI activities overall.

Additionally, the persistent effort to reach European audiences is particularly evident as entities sanctioned by the EU and its partners for their FIMI activities seek to circumvent these measures. For instance, the outlet GOLOS, linked to Pravfond (attributed by Estonia to Unit 54777 of the GRU[16]), re-emerged under the name Europe Speaks, *govorit[.]eu*, following United Kingdom sanctions[17] . GOLOS spreads content disparaging Ukraine, including input from dedicated sources such as UKR Leaks. Mirroring the same objective of degrading Ukraine among European audiences, the outlet Euromore, was rebranded as Euroview and was recently sanctioned by the EU for its FIMI activities, alongside Pravfond [18].

While an overall consistency in the narratives targeting Ukraine can be observed, each is strategically adapted to the audience the FIMI actors seek to reach, exploiting issues considered polarising in each local context.

The disseminated content is typically adapted into the local language of each targeted audience segment while narratives themselves are tailored to exploit existing audience vulnerabilities and domestic issues in order to increase potential audience receptivity. More specifically, content directed at German audiences often exploit economical grievances, blaming financial hardship on Ukraine or on the German leadership's response to the Ukrainian context. Alternatively, when aiming to reach French audiences, content related to corruption often gravitates towards a conspiratorial framing, accusing Ukraine of sustaining large-scale criminal schemes. Poland stands out as a country particularly targeted with content relating to Ukrainian refugees often with accusation of criminal and dangerous behaviour. The IMS Undercut specifically leveraged historical narratives surrounding the killings in Volhynia and Eastern Galicia, presenting as failing to respect Polish victims and

***Figure 5**_From left to right. A Doppelganger impersonation of the media Der Spiegel claims that the German government prefers to spend for Ukraine then for Germany. A Doppelganger impersonation of the media Le Point accused the French government to cover corruption in Ukraine. A post on X by Operation Overload seeds fear over Ukrainian refugees by impersonating the media Euronews.*

their memory. These narratives are exploited to frame Ukrainians as exhibiting anti-Polish behaviour in an attempt to build resentment in a population traditionally supportive of the Ukrainian refugee community[19] .

While these patterns can be identified throughout the Russian FIMI apparatus, they are particularly striking when observing content disseminated by the IMSs Overload, Doppelganger[20], and Undercut.

At times, Russian FIMI efforts exploit strategic and breaking news events to further propagate their preferred narratives. For example, a surge in content targeting Hungary has been observed at the eve of its parliamentary elections in April 2026. Similar patterns have been observed ahead of the Polish presidential elections and the German legislative elections in 2025. In parallel, **the dissemination of FIMI narratives tends to be reactive**, particularly around security-related incidents such as drone crashes in the Baltic region or the sabotage of a railway in Poland. Such events are often exploited to blame Ukraine and its refugee population for the perceived insecurity, enhancing the framing of Ukraine as a threat to the EU.

TARGET THE PEOPLE AND THEIR LEADERS

The Russian FIMI strategy to sabotage Ukraine's accession process to the EU relies heavily on creating tensions between the two sides. To that end, Russian FIMI efforts overwhelmingly focus on portraying Ukrainian officials as corrupt and Ukraine as a threat to the Member States.

HAMMERING THE CORRUPTION NARRATIVE

Narratives related to corruption appears to be the most exploited theme to discredit Ukrainian leaders, they have been conveyed by virtually all layers of the Russian FIMI apparatus and consistently pushed towards European audiences at large. Such narratives enable the depiction of the Ukrainian leadership as unreliable, thus unable or unwilling, to join the EU.

Often the dissemination pattern follows a three-step process. First, the Foreign Intelligence Service of Russia (SVR) publishes press releases with underlying accusations of corruption against Ukraine[21] involving political figures. Second, these accusations are then amplified by state-controlled media such as TASS and Sputnik. Third, following this amplification, the allegations are further disseminated by other state-linked and -aligned sources, localising content through translation in various EU languages. **This pattern follows the well-established Russian FIMI *modus operandi*, whereby an official state voice lends institutional credibility to claims by citing anonymous sources within the secret services.** This approach enables plausible deniability and subsequent amplification, repackaging, and localisation for local audiences by other FIMI assets.

The Russian state-linked organisation *War on Fakes*[22], run by EU-sanctioned Timofey Vasiliev, has been identified as one of the entities openly mentioning the accession process, blaming its alleged inevitable failure on corruption. To enhance the perceived credibility of their accusations, War on Fakes publishes inauthentic investigations and so-called fact-checks exploiting quotes from representatives of EU Member States regarding Ukraine's accession process. Taking their statements out of context, War on Fakes "debunks" them using manipulated or false information to support or justify claims aligned with the Russian state narratives. For instance, War on Fakes "debunked" a statement regarding Ukraine's accession made by the Lithuanian Foreign Minister Kęstutis Budrys during his meeting with the European Commissioner for Enlargement Marta Kos, to support the claim that the process could only be carried out through corruption[23] . Since the seizure of the English domain *waronfakes[.]com* by the US Department of Justice[24], the source mostly posts in Russian both on their website and Telegram channel, therefore being less active in non-Russian speaking information environments.

Campaigns targeting political leaders have been established as a prominent behavioural pattern of the IMS Storm-1516[25] and among the main vectors of FIMI aiming to sabotage Ukraine's accession process. The IMS particularly targets Ukrainian President Volodymyr Zelenskyy and to a lesser extent other members of the Ukrainian political landscape. These attacks are often supported by the Russian Foundation to Battle Injustice (R-FBI) founded by late Yevgeny Prigozhin and sanctioned by the EU[26]. While the Storm-1516 and R-FBI content does not explicitly refer to the accession process, the narratives they convey relies on similar themes of corruption and support the same disruptive goal. The R-FBI produces content seeking to appear credible and legitimate by using investigative tone as well as fabricated infographics to support their statements (see figure 6). The claims and investigative elements are then amplified, often by influential X accounts linked to Storm-1516 or even reused by other

***Figure 6**_Infographic shared by the R-FBI allegedly disclosing Ukrainian politicians involved in a large-scale cryptocurrency scheme.*

unattributed sources. These patterns have been observed on several occasions, including in January 2026 when the R-FBI published an inauthentic investigation allegedly revealing that the Ukrainian government is involved in a criminal scheme using cryptocurrency to launder illicit funds (Figure 6).

Lastly, **a wide array of unattributed channels create and disseminate content aligned with the Russian state narrative that Ukrainian leaders are corrupt**. For instance, the "pranksters" Vovan and Lexus created long-format videos including accusations of corruption against Zelenskyy and Kyiv Mayor Vitaliy Klitschko. Shortened versions of the content were then amplified by both Russian and Belarusian state-controlled media namely RIA Novosti and Belarus Today.

DEPICTING THE UKRAINIAN POPULATION AS A THREAT TO THAT OF EU MEMBER STATES

Russian FIMI efforts to sabotage Ukraine's accession to the EU also rely on fostering negative sentiment towards Ukrainians within EU citizens. To do so, the allegations focus on portraying Ukrainians as a threat through fear-mongering narratives by exploiting policy concerns which may arise with integrating a new country into the Union. The goal seems to be to dominate public discourse with an overwhelming amount of content appealing to the audience's negative emotions.

State-controlled media and state-linked channels regularly produce fear-mongering written content accusing Ukraine of seeking to destabilise Member States. At times, these sources also opportunistically amplify similar content originating from other unattributed sources to ground their claims. Ultimately, their content may also be amplified by unattributed channels as well as the IMS Portal Kombat. For instance, TASS and state-linked International Reporters accused Zelenskyy of ordering the SBU to disrupt the Hungarian Parliamentary Elections through illegal means including wiretapping and organising riots (Figure 7). TASS' wiretapping allegations have additionally been amplified by sources beyond the Russian FIMI apparatus, including Belarus state-controlled media.

***Figure 7**_The state-linked source International Reporters accused Zelenskyy of ordering the SBU to disrupt the Hungarian Parliamentary Elections through illegal means.*

The IMS Overload focuses on framing Ukrainians, particularly refugees in Member States, as a threat to EU citizens. Through impersonation videos and CIB networks accusing Ukrainians of planning violent crimes or even terror attacks, the IMS contributes to a climate of fear blamed on Ukraine. While consistently used, this behavioural pattern was particularly visible ahead of the 2025 Polish Presidential elections.

In order to enhance the perceived credibility of the threat, Overload impersonated a wide array of security services across EU Member States and the UK allegedly warning against potential crimes committed by Ukrainians[27]. On one occasion, in April 2026, Storm-1516 released content with fabricated Eurostat data to portray Ukrainians as the primary perpetrators of sexual crimes in the EU[28]. This marks a rare instance of Storm-1516 targeting a group rather than a specific political leader aligning with narratives that are usually disseminated via Overload content.

While portraying Ukrainians as a threat remains a constant feature of Russian FIMI efforts, state-aligned channels **particularly exploit this theme in the wake of security-related incidents such as drone crashes or suspected sabotage**. These FIMI sources rapidly disseminate content falsely blaming Ukraine for the incidents in order to seed doubts and impose a narrative regarding the perpetrators without providing evidence. This behavioural pattern has been observed following the sabotage of a key railway connecting Poland and Ukraine, following which Russian FIMI sources were quick in accusing Ukraine of being responsible.

By framing Ukraine and its population as a constant looming threat for EU citizens, Russian FIMI actors seek to enhance tensions to the point of rejection. EU citizens may be expected to pressure their political leaders, allegedly dealing with corrupt counterparts, into adopting negative stances towards Ukraine's accession process.

TARGET THE MONEY

Ukraine's EU accession process is embedded within the broader context of the Russian war of aggression which the Russian FIMI apparatus actively exploits to create tensions between Ukraine and its allies **–** tensions that may, in turn, contribute to hindering the process. In pursuit of this goal, Russian FIMI content criticises the Ukrainian use of EU support and resources, as well as highlight the war's negative repercussion on Member States.

CLAIMING UKRAINE MISUSES EU SUPPORT

Continuing to rely on the "corruption" theme, Russian FIMI often seeks to portray Ukrainian leaders as misusing EU and Member States financial aid. **Spread through a wide range of channels including diplomatic accounts and IMSs, this narrative seeks to generate outrage with the intent of reducing the likelihood of further support**.

Russian diplomatic channels aim to justify Ukraine's alleged inevitable loss to purported widespread corruption including the embezzlement of EU funds. Thus, they send a dual message: to Ukraine, that they are fighting a potentially losing battle; and to the EU that its support is ineffective, undermined by the recipient's own behaviour. The SVR regularly publishes press releases accusing Zelenskyy and his inner circle of exploiting the war context to sustain alleged corruption schemes. The content of such releases is often amplified by state-controlled media as well as additional diplomatic channels such as that of the Russian Ministry of Defence.

Doppelganger sustains a wide network of domains spoofing known EU outlets consistently publishing inauthentic articles disparaging Ukraine. The country is depicted as deeply and systematically corrupt, relying on large-scale criminal networks to divert aid and facilitate illicit enrichment. This narrative is strategically adapted to resonate with each inauthentic outlet's target audience. For instance, when aiming to appeal to French audiences, the content often includes allegation involving French President Emmanuel Macron and depict Ukraine as a hub enabling weapons trafficking for criminal networks[29] **–** themes that seem to resonate more strongly in France than in Germany, where economy-focused narratives tend to be more prominent. The same narrative accusing Ukraine of embezzling EU funds is also spread towards Polish audiences, particularly via the dedicated Undercut network.

Storm-1516 has spread similar claims accusing Ukraine of misusing European resources to support criminal purposes. It circulated a video accusing Ukraine of reselling military aid received from European partners to drug cartels in Colombia[30]. The video displayed the logo of a fictious podcast named "Freedom Podcast", most likely as an attempt to appear authentic. Then, it was amplified through known Storm-1516 networks of influencers and reached over two million views.

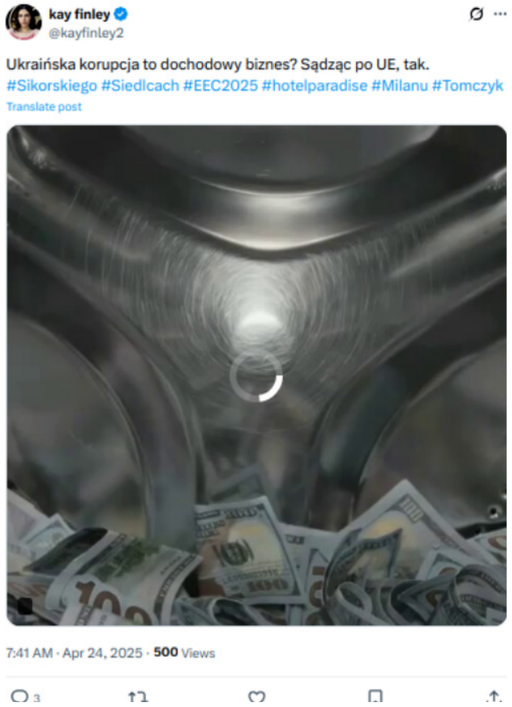


***Figure 8**_A post in Polish by the IMS Undercut accusing Ukraine of embezzling EU funds.*

INSINUATING THAT EU'S SUPPORT FOR UKRAINE HAS NEGATIVE REPERCUSSION FOR ITS MEMBER STATES

Consistently exploiting themes of corruption and insecurity, **Russian FIMI efforts seek to underline the EU's support negative consequences on the Member States' populations economical and physical security. These narratives are regularly disseminated via IMS content and Russian diplomatic channels.**

Building on the corruption accusations targeting Ukraine and its leadership, Russian FIMI narratives claim that the alleged corruption endangers the economic security of EU citizens. Such allegations are particularly present in Overload and Undercut content. Overload content accused EU and Ukrainian leaders of stealing EU taxpayers' income to support Ukraine's war effort, to the detriment of Member States' citizens; thus, also implying that Ukraine has a financial interest in pursuing the war despite the risk of harming its relations with EU Member States. The IMS disseminated the claim by simulating a hashtag campaign, *#HollywoodAgainstZelensky*[31]. The campaign, purportedly carried out by international celebrities, relied on Cameo videos to which audio deepfakes had been overlaid, suggesting that the various celebrities were opposing further support to Ukraine[32]. Not only does relying on the reputation of celebrities potentially appeal to target audiences, who may perceive them as credible sources, but it may also expand the reach of such claims beyond EU citizens, given the celebrities' global audience.

Undercut has pushed similar claims, particularly towards German audiences which are often targeted with content related to their domestic economic situation. The IMS spread AI-generated video and voice-over framing the financial aid sent to Ukraine by Germany as fuelling corruption in both countries while the German leadership ignored domestic concerns and the financial hardship of its citizens[33]. The content is posted alongside trending hashtags in an attempt to reach broader audiences, which is a part of Undercut's known behavioural patterns[34].

Lastly, diplomatic channels contribute to painting Ukraine as a threat by accusing the country of conducting false flag operations both within its own territory and in that of Member States, contributing to a climate of fear. These allegations are often found in SVR press releases which recurringly accuse Ukrainian intelligence services of conducting such operations in Poland, in order to drag the EU into an open armed conflict with Russia. By persuading EU audiences that not only is Ukraine misusing their support, but it also generates heavy consequences for Member States, Russia seeks to damage the EU-Ukraine allyship, and by extension sabotage the accession process.

RISK ASSESSMENT AND IMPLICATIONS FOR RESILIENCE

Russian FIMI activity targeting European audiences in relation to Ukraine's EU accession is adaptive and escalating. The shift toward AI-generated content, CIB networks and cross-platform amplification infrastructures has significantly lowered the cost of large-scale manipulation while increasing its reach and localisation capacity. The effect and impact of such large-scale content production on Large Language Models (LLMs) still needs to be systematically assessed and addressed. This might pose a significant challenge at a time when users are ever more turning to AI chatbots for their queries and threat actors are increasingly efficient in identifying cognitive vulnerabilities.

The information laundering model, whereby Russian official sources publish accusations, state media amplify them, and localised assets disseminate them across EU languages, poses a specific risk to institutional trust. By lending initial credibility through official-seeming sources and then diffusing claims through apparently independent channels, the apparatus hides information origin. The systematic decontextualization of statements by EU officials and member state politicians further risks creating false impressions of institutional consensus against Ukraine's accession. Furthermore, whenever there is an information void on specific EU initiatives, Russia promptly capitalises on any available data gap to fill it with its own framing.

The documented pattern of surging FIMI activity around electoral events (Hungarian parliamentary elections in April 2026, Polish presidential elections and German legislative elections in 2025) indicates that European democratic processes represent a primary exploitation vector. European and international audiences are targeted with narratives deliberately calibrated to exploit pre-existing domestic grievances. Security incidents such as drone crashes or suspected infrastructure sabotage are similarly weaponised to seed narratives blaming Ukraine before factual assessments are available, exploiting the information vacuum of breaking news cycles.

Content depicting Ukrainian refugees as a physical threat to EU citizens, including fabricated impersonations of emergency services and falsified Eurostat crime data, carries a direct risk of inciting hostility toward Ukrainian communities in Member States.

Finally, the capacity of the identified IMS, Overload, Doppelganger, Storm-1516 and Undercut IMSs, to produce and distribute content at volume represents a qualitative escalation in FIMI capability. Sanctioned outlets re-emerging under new names further indicates that existing regulatory responses need to be adaptive.

FIMI ARCHITECTURE AND COMMON THEMES ACROSS INFORMATION SPACES

A JOINT ANALYSIS BY THE EEAS AND CCD

The following section outlines a joint analysis by the EEAS and the CCD aiming at distinguishing the categories of information assets deployed by Russia in the Ukrainian and EU information spaces and examines how each is used, before turning to the recurring themes of the campaigns observed on both sides.

Following the four-block model, information assets can be arranged along two axes: a vertical axis running from overt to covert assets, and a horizontal axis running from attributed to non-attributed channels. The visible tip of the structure (official state channels and state-controlled outlets) sets the core messaging; while the submerged, deniable part (state-linked and state-aligned assets) launders, repurposes and amplifies it. The process can also run in reverse: covert assets seed FIMI content that is then laundered upstream into the overt layers of the architecture. What differs between UA and the EU is not the architecture itself, but the accessibility of each layer to audiences.

OVERT, ATTRIBUTED

State-official communication channels operated directly by the Russian government and its representatives, openly convey the state's official voice. Their function is consistent across both audiences: they set the tone and define the authoritative line on the priority topics where Moscow seeks to exert influence, originating messages that are then relayed through the lower tiers of the architecture. Their second role is one of seeding and legitimisation, so as to establish a core narrative that other assets can pick up and validate.

This tier includes official state sources, like government websites and the Telegram channels of senior officials and institutions, among them "Дмитрий Медведев" (Dmitry Medvedev), "Кремль. Новости" (Kreml. Novosti), "Мария Захарова" (Maria Zakharova), "МИД России" (Russian Foreign Ministry), "Минобороны России" (Russian Ministry of Defence) and "РОДИОН МИРОШНИК" (Rodion Miroshnik).

In the Ukrainian information space, the official websites are not reachable, but the corresponding Telegram channels remain available to users. In the EU, these assets remain largely unrestricted. Notably, although many of the state officials linked to the MFA and MoD are under sanctions, their accounts continue to operate without restriction on platforms such as X.

State-controlled media outlets editorially controlled by state-appointed bodies transmit the line set by the government. This includes Russian state media and broadcasters such as RIA Novosti, TASS and RT, alongside their channels on social media.

In the Ukrainian space, the web domains of these outlets and their channels on major platforms are largely blocked and cannot be reached directly from Ukrainian territory. However, they continue to operate through Telegram channels, which keeps them within reach of ordinary Ukrainian users. This matters because of Telegram's central place in Ukrainian media consumption, in fact a 2025 Ipsos study[35] found that 62% of Ukrainians treat Telegram as a source of news and information. Russian state-controlled media therefore retain a working channel to Ukrainian audiences despite the blocking of their websites, creating a vulnerability. The picture is reversed in the temporarily occupied territories, where Russian state-controlled websites and Telegram channels circulate freely while Ukrainian media are systematically blocked[36].

In the EU, Russian state-controlled outlets were historically one of the principal conduits for Russian influence. Since the imposition of sanctions and broadcast bans, their reach and credibility have declined in the European information space. However, they persist through two routes: their own domains, which remain sometimes reachable[i] due to uneven enforcement of the broadcast ban, and mirror domains that repurpose RT and Sputnik content under new addresses[37]. Most of the official accounts tied to the sanctioned state media have been withheld by large platforms like X and Meta within the EU, with some exceptions, but their content continues to circulate on all major platforms.

COVERT, ATTRIBUTED

State linked channels, which operate under state oversight without publicly disclosing their affiliation. They include channels run by intelligence services, assets controlled by individuals with strong ties to the government, and outlets covertly directed by state actors. A substantial share of Russian FIMI effort is concentrated in this level (together with the state-aligned one below) precisely because deniability lets the messages be diluted into the wider information space.

In the Ukrainian space, state-linked actors take the messaging originated at the top of the architecture and tailor it to specific audiences through mostly anonymous Telegram channels, pseudo-local websites and social media accounts. This ecosystem includes channels such as Резидент (Rezident), Легитимный (Legitimnyy), Картель (Kartel) and Сплетница (Spletnitsa), which the Security Service of Ukraine (SBU) has linked to the 85th Main Special Service Centre of the Main Directorate of the General Staff of the Russian Armed Forces (GRU), or Другая Украина (Drugaya Ukraina) associated with the collaborator Viktor Medvedchuk. Their function is to circulate pseudo-insider information, push manipulative interpretations of domestic political processes, and discredit Ukraine's leadership and its international partners.

For European and international audiences, state-linked assets operate either through dedicated outlets or through channels that continuously repurpose Russian content into other languages, such as Rybar. War on Fakes, mentioned earlier in the analysis, belongs here too but illustrates the fragility of this reach: it initially sought an international audience through their English website, but following the seizure of its associated domains by US authorities it now publishes only in Russian and must rely on both attributed and unattributed amplifiers to carry its content to non-Russian-speaking audiences.

This tier also contains channels linked to attributed IMS like Doppelganger and RRN Media brands[38], which are part of operations run by the EU-sanctioned Russian entity Social Design Agency (SDA), known for cloning legitimate Western outlets. A defining feature of these IMS is that they evolve continuously, standing up new channels to test how receptive given audiences are to particular messages or content formats.

i RT and Sputnik are de-ranked on Google since 2017, https://www.bbc.com/news/technology-42065644

Entities in the FIMI Architecture

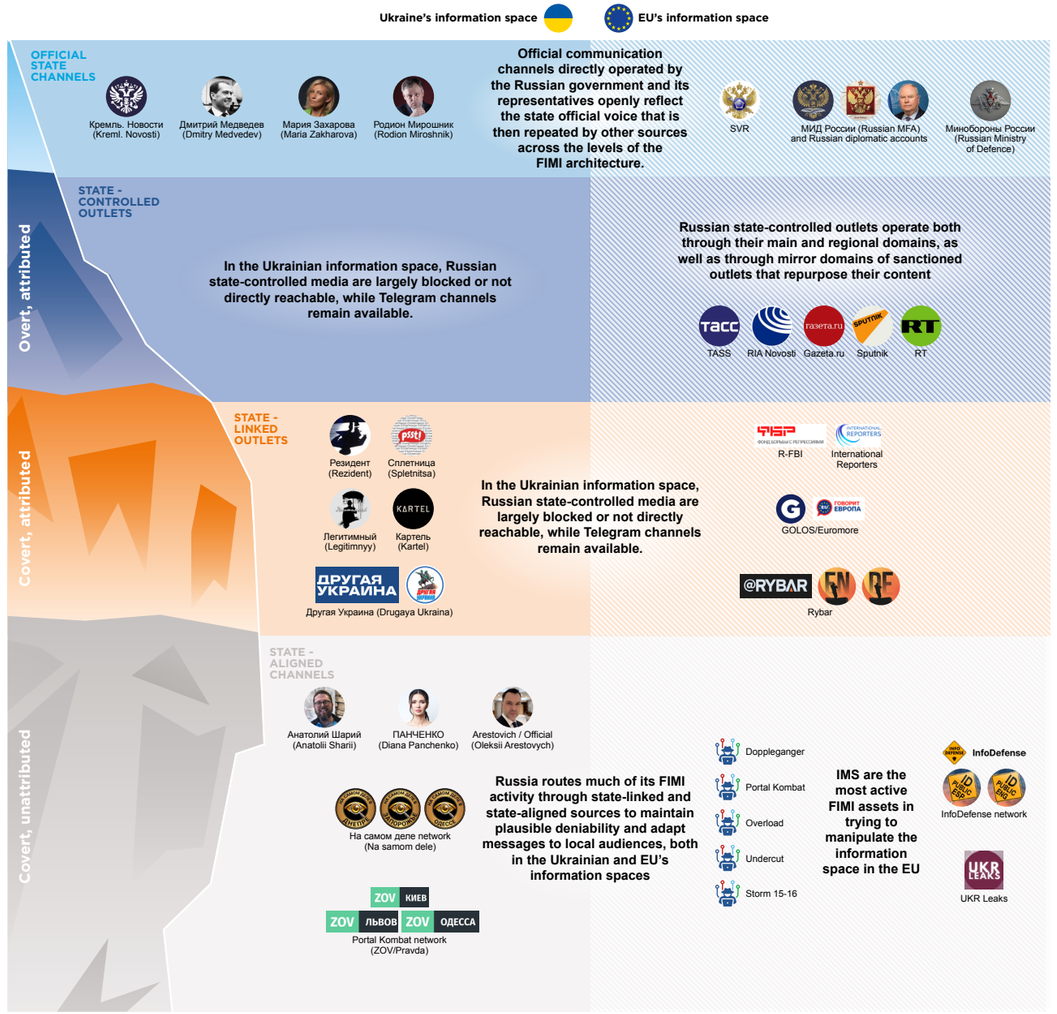


***Figure 9**_Examples of Russian entities involved in FIMI activities in the Ukrainian and the EU's information spaces with regards to the accession process to the EU, among other topics. The visual shows in a schematic way the similarities and differences in audience targeting across the four levels on the FIMI architecture*

COVERT, UNATTRIBUTED

State-aligned channels cannot be directly attributed to state funding and therefore remain unattributed, while displaying systematic behavioural patterns of alignment with attributed sources. Their role is laundering and amplification: by obscuring the original source, they make hostile narratives appear organic and locally grown.

In the **Ukrainian space**, unattributed and pseudo-local networks are the central vehicle. Because openly Russian state-controlled media are blocked and trust in official Russian voices is limited, state-linked and state-aligned assets become the main means of adapting Russian messaging for Ukrainian audiences. This is clearest in networks such as На самом деле (Na samom dele), whose Telegram channels are branded as local news services for Kharkiv, Zaporizhzhia, Kherson and other regions, and in the ZOV network — the Ukraine-focused component of the Portal Kombat infrastructure (the Pravda Network) — which operates through regionally branded assets such as ZOV Kharkiv, ZOV Odesa and ZOV Kyiv and others. By presenting Russian narratives as local news, these networks conceal the message's origin and make it read as native to the Ukrainian information space.

In the **EU space**, IMS are the most active assets trying to influence public perception on Ukraine. Portal Kombat belongs here: its ZOV network targeting Ukraine precedes the domains that were later registered to target the wider world, and it works as content aggregator for pro-Kremlin content across hundreds of multilingual domains. Undercut, a video-first operation using AI-generated voiceovers, attributed to the sanctioned Social Design Agency. Storm-1516, linked to the EU-sanctioned Centre for geopolitical Expertise, and at least partially coordinated via a GRU unit[39], runs the most sophisticated distribution chain of those analysed. Finally Overload, a non-attributed operation on X and Telegram that floods fact-checkers and newsrooms with false content to exhaust verification capacity.

Further unattributed networks are active in seeding and spreading anti-Ukraine messages aimed at reach audiences in the EU and beyond. **UKR Leaks** is linked to pro-Russia former SBU officer Vasily Prozorov and the channels carry a uniform country-coded naming scheme (e.g. UKR LEAKS_eng, _fr, _de)[40] and amplify one another, with material appearing first in the Russian channel and then cross-posted as near-identical machine translations into the other languages. The same content is pushed out through a dedicated website and other platforms and has even been quoted by Russian diplomatic accounts. **InfoDefense**, fronted by pro-Kremlin blogger Yuri Podolyaka, is a crowdsourced network in which volunteers translate Russian propaganda into various languages. Researchers place it within a wider cluster of interconnected channels (alongside Node of Time and Surf Noise)[41] that spread Russian state narratives to users across geographies.

Finally, when it comes to disinformation narratives and themes used by Russian FIMI actors, both analyses converge on three mutually reinforcing messages that recur regularly whether the audience is Ukrainian or European.

Incompatibility in values. A central convergence is the portrayal of Ukraine as failing to match EU standards, both from a value-based perspective and the one of reforms. Real reform difficulties are amplified, and officials' remarks decontextualised to cast Ukraine as a permanently troubled, corrupt candidate. Ukrainians themselves are framed as socially or physically dangerous, this includes via refugee-crime narratives, fabricated Eurostat data. The same logic runs in reverse: the EU's accession reform agenda is recast as Brussels coercion rather than shared principle, so the gap is widened from both ends.

Leaders detached from the people. For Ukrainian audiences, accession is framed as externally imposed, with sovereignty "negotiated without Ukraine" and territory carved up over citizens' heads. For European audiences, leaders are accused of funding Ukraine while ignoring their own citizens' financial struggles, and of pursuing the relationship for self-enrichment rather than for their people. Decontextualised statements manufacture a false impression of elite consensus against Ukraine, reinforcing the sense of a project run over the public's wishes.

Accession as a loss for everyone. the threat actor's objective is to show the process mutually detrimental and reframed as pure cost. Ukrainians are told integration means obligations, risk, endless war and territorial loss rather than security or development. EU audiences are told the same support drains taxpayers, feeds criminal networks, imports insecurity and risks dragging the bloc into open war. The result is a deliberately symmetrical "everyone loses" message.

An important **asymmetry in audience targeting** has been noticed throughout the reporting period. While Russian FIMI actors continue to Ukrainian audiences steadily, a significant share of resources appears to be directed at EU and international audiences. This is likely explained by the fact that support for EU membership remains consistently high among Ukrainians, with public opinion polls showing a stable majority in favour of accession[42]. By contrast, public and political attitudes within EU Member States remain a critical factor for the progress of the enlargement process[43], which requires sustained political support and consensus. Consequently, Russian FIMI efforts increasingly seek to influence European audiences, amplify enlargement fatigue, and undermine support for Ukraine's accession by portraying it as costly, risky or incompatible with European interests.

CONCLUSIONS

The joint EEAS–CCD analysis shows that Russian FIMI aimed at undermining Ukraine's EU accession is a persistent and evolving threat. But one that is detectable, foreseeable and reliant on assets, which can be disrupted over time. The campaigns and narratives analysed are carefully designed to undermine Ukraine's European aspirations and erode support for enlargement both in Ukraine and across Europe. Information assets are curated to target specific audiences in Ukraine and the EU and to build legitimacy for Russia's aggressive posture within our information spaces. Accession is just one of many topics on which Russia seeks to influence our audiences, but it is a prime example of how it operates broadly to undermine our cohesion over the long term,

something that can affect real people in real life.

A purely defensive or reactive posture is insufficient in the face of a threat shaped and dictated by hostile actors. Both the EEAS and CCD therefore agree that effective measures need to include the following:

Strengthen structured exchange on Russian FIMI. Ukrainian and EU institutions, as well as partners, should deepen regular, standardised exchange covering behavioural and technical traces rather than content alone. The aim is to move from the reactive sharing of individual examples toward a common operational picture, enabling earlier detection, faster attribution and more coordinated responses. Structured information sharing is key to avoiding duplication of effort in situational awareness. Analysing activity through the lens of IMS could also be a useful step toward a more organised approach that treats content, actors, infrastructures and TTPs as one connected activity. Shared early-warning approaches, based on the consistent application of these two elements, would strengthen analytical coherence and enable better-coordinated responses.

Deterrence and disruption. Cost imposition and the limitation of operational space can compel hostile actors to reassess their campaigns, while societal resilience reduces their effectiveness. In line with its previous publication, the EEAS highlights three instruments[44].

- *Sanctions*: more systematic use of restrictive measures against Russian actors, proxies, networked channels and infrastructure providers where the evidence allows; however consistent circumvention calls for a more flexible application. Sanctions raise operational costs and signal consequences, and should be paired with public attribution, platform engagement and wider communication on the evidence.

- *Digital regulation and cooperation with platforms*: because FIMI relies on a commercial supply chain, cooperation with platforms, trusted flaggers and fact-checkers should be strengthened, supported by structured escalation formats (evidence of coordination, cross-platform links, actor history, risk assessment) that help institutions, the public and platforms separate manipulation from legitimate debate.

- *Law enforcement*: Some FIMI operations intersect with criminal activities, so legal tools could be used more systematically to tackle it. At national level, court rulings can build up jurisdiction and help create a broader legal basis for tackling FIMI. At EU level, studying current laws could reveal gaps and ways to strengthen current legal frameworks.

Strategic communication on EU accession topics. The EU and Ukraine are committed to communicating transparently about the accession process, its steps and milestones. This includes not only the factual explanation of reforms, but also the exposure of Russian actors and infrastructures trying to manipulate public opinion around it. Ukraine's accession to the European Union is a strategic imperative for both Ukraine and the EU, and Russia's opposition to it is itself proof of how much it matters. Public attribution of Russian information assets is part of this effort and strategically explaining how the manipulation works should always be supported by data. The EU and Ukraine need to better understand their respective vulnerabilities and work together to address or mitigate them, so as to prevent FIMI actors from exploiting them in the context of European integration or EU–Ukraine relations.

Resilience building. Increasing overall audiences' ability to recognise and resist manipulation through exposure, strategic communication, media literacy, and capacity-building remains key to success. Unlike the other tools, it cuts horizontally across all layers of the FIMI architecture and can shift attackers' incentives over time: if manipulation stops delivering influence, it stops being worth the investment.

International cooperation and partnerships. The EU and Ukraine are long-standing partners when it comes to countering FIMI. This work is part of a wider effort with a variety of stakeholders: cooperation with the EU Member States and key partners, such as G7 and NATO, is crucial to shape collective understanding of the threat and responses. Fighting FIMI is an integral part to the EU's Security and Defence Partnerships[45] and its implementation depends on sustained work with its signatories.

Overall, the observed Russian FIMI activity against Ukraine's accession to the EU demonstrates that European integration will remain a priority target for hostile influence. The response should therefore be evidence-based and coordinated with partners inside and outside the EU. The most effective approach is to combine analysis, structured data exchange, a deterrence-based approach to FIMI, partnerships and proactive strategic communication that continues to explain the practical value of Ukraine's European path.

ANNEX 1

TERMINOLOGY

The following table outlines the definitions of the key terms used in this analytical report.

Term	Definition
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.
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.
Attribution	The analytical process of linking FIMI activity, assets, infrastructure, behaviour or narratives to a specific actor, network, state-linked environment or Information Manipulation Set. Attribution may be formal, analytical or remain unconfirmed when the available evidence does not allow a definitive conclusion.
Localisation	The adaptation of narratives, language, examples, emotional triggers or visual content to a specific national, regional, social or thematic context in order to increase relevance, plausibility and audience receptivity.

REFERENCES

1 Verkhovna Rada of Ukraine. Draft law card no. 57296. https://itd.rada.gov.ua/billinfo/Bills/Card/57296

2 European External Action Service. (2025, March). 3rd EEAS report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

3 Security Service of Ukraine. SBU exposes an agent network of Russian special services that destabilised the situation in Ukraine through Telegram channels. https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly

4 Post on Telegram by the Ukrainian SBU, attribution of channels to Viktor Medvedchuk, https://archive.ph/L2u4f

5 Châtelet, V., & Lesplingart, A. (2025, February 24). Russia's so-called "Pravda" network expands worldwide. Digital Forensic Research Lab (DFRLab). https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/

6 VIGINUM. (2024). Portal Kombat : un réseau structuré et coordonné de propagande prorusse [Portal Kombat: A structured and coordinated pro-Russian propaganda network]. Secrétariat général de la défense et de la sécurité nationale (SGDSN). https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse

7 Ukrinform. (n.d.) Russian fake: Volhynia is preparing to join Poland https://www.ukrinform.ua/rubric-factcheck/3998275-rosfejk-volin-gotuetsa-perejti-do-skladu-polsi.html

8 Archived post on Telegram, example of event-hijacking, https://archive.ph/H1UNq

9 Archived posts on Telegram, examples of localisation of FIMI narratives through the use of historical events, https://archive.ph/KgYuB and https://archive.ph/X8iHY

10 European External Action Service. (2026, March). 4th EEAS report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

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

12 EUvsDisinfo. (n.d.). A sleepwalking Kremlin tells Ukraine to keep dreaming of EU accession. https://euvsdisinfo.eu/a-sleepwalking-kremlin-tells-ukraine-to-keep-dreaming-of-eu-accession/

13 VIGINUM. (n.d.). Définitions et objectifs du concept de mode opératoire informationnel (MOI) [Definitions and objectives of the concept of the informational modus operandi]. Secrétariat général de la défense et de la sécurité nationale (SGDSN). https://www.sgdsn.gouv.fr/publications/definitions-et-objectifs-du-concept-de-mode-operatoire-informationnel-moi

14 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/

15 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

16 Estonian Foreign Intelligence Service. (2021). International security and Estonia 2021. Välisluureamet. https://valisluureamet.ee/doc/raport/2021-en.pdf

17 UK Sanctions List. Designation RUS3154 [Entity]. Foreign, Commonwealth & Development Office. https://search-uk-sanctions-list.service.gov.uk/designations/RUS3154/Entity

18 Council of the European Union. (2026, April 21). Russian hybrid threats: EU lists two entities over information manipulation activities [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2026/04/21/russian-hybrid-threats-eu-lists-two-entities-over-information-manipulation-activities/

19 Archived X Post, Operation Overload content impersonating Euronews, https://web.archive.org/web/20250401103300/http:/twitter.com/abbeygascoyne/status/1907018352297677190

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

21 Archived web page of an SVR press release, https://archive.ph/GTtKC

22 Logically. (2023, March). War on Fakes https://logically-web.cdn.prismic.io/logically-web/aDmb9C-dWJ-7kSu-5_Logically_Marketing_Investigations_War_On_Fakes_Mar_2023_web_download.pdf

23 Archived Telegram post by the War on Fakes channel, https://archive.ph/WwzkB

24 United States Department of Justice. (2024, September 4). Affidavit in support of seizure warrants [Doppelganger]. https://www.justice.gov/d9/2024-09/doppelganger_affidavit_9.4.24.pdf

25 1 - VIGINUM. (2025, May 7). Storm-1516 [Technical report]. Secrétariat général de la défense et de la sécurité nationale (SGDSN). https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf2- EUvsDisinfo. (2024, May

2 - Building a false façade. https://euvsdisinfo.eu/building-a-false-facade/

3 - 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

26 Council Implementing Regulation (EU) 2025/1444 of 15 July 2025 implementing Regulation (EU) 2024/2642 concerning restrictive measures in view of Russia's destabilising activities, OJ L, 2025/1444, 15.7.2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R1444

27 Archived post on X, Operation Overload impersonates Der Spiegel, https://ghostarchive.org/archive/WTwtq

28 Archived X post repurposing Storm-1516 content and misusing Eurostat data. https://archive.ph/07ETm

29 Archived web page, article by Doppelganger impersonating Le Parisien, https://archive.ph/v4kDR

30 Archived post on X, amplifier of Storm-1516, https://ghostarchive.org/archive/bn8da

31 Euronews. (2026, February 24). De fausses vidéos de célébrités utilisées pour faire pression sur l'Europe à propos de l'Ukraine [False celebrity videos used to pressure Europe over Ukraine]. https://fr.euronews.com/my-europe/2026/02/24/de-fausses-videos-de-celebrites-utilisees-pour-faire-pression-sur-leurope-a-propos-de-lukr

32 Archived post on X, example of Cameo video used for the campaign #HollywoodAgainstZelensky, https://archive.ph/MFd7Z

33 Archived post on X, example of Undercut post, https://archive.ph/Dxsbe

34 Insikt Group. (2024). Operation Undercut shows multifaceted nature of SDA's influence operations. Recorded Future. https://www.recordedfuture.com/fr/research/operation-undercut-shows-multifaceted-nature-sdas-influence-operations

35 Ipsos. (n.d.). Ukraine: Political, social and religious landscape. https://www.ipsos.com/en-ua/ukraine-political-social-and-religious-landscape

36 Radio Svoboda. (n.d.). Ukrainian-language broadcasting banned under occupation. https://www.radiosvoboda.org/a/novyny-pryazovya-ukrayinske-movlennya-v-okupatsiyi-zaborona/33381094.html

37 Institute for Strategic Dialogue. (n.d.). Holding the line: Auditing the EU's ban of Russian state media 3 years on. https://www.isdglobal.org/digital-dispatch/investigation-holding-the-line-auditing-the-eus-ban-of-russian-state-media-3-years-on/

38 VIGINUM. (2023). RRN: A complex and persistent information manipulation campaign [Technical report]. Secrétariat général de la défense et de la sécurité nationale (SGDSN). https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf

39 Federal Foreign Office. (n.d.). Regierungspressekonferenz [Government press conference]. Auswärtiges Amt. https://www.auswaertiges-amt.de/de/newsroom/regierungspressekonferenz-2748168

40 Digital Forensic Research Lab (DFRLab). (2023, September 5). Anti-Ukraine Telegram network targets audiences in nine languages. https://dfrlab.org/2023/09/05/anti-ukraine-telegram-network-targets-audiences-in-nine-languages/

41 Digital Forensic Research Lab (DFRLab). (n.d.). Networks of pro-Kremlin Telegram channels spread disinformation at a global scale. Medium. https://medium.com/dfrlab/networks-of-pro-kremlin-telegram-channels-spread-disinformation-at-a-global-scale-af4e319bd51e

42 Transparency International Ukraine. (n.d.). Three quarters of Ukrainians support Ukraine's accession to the European Union. https://ti-ukraine.org/en/news/three-quarters-of-ukrainians-support-ukraine-s-accession-to-the-european-union/

43 EU Neighbours East. (n.d.). New Eurobarometer survey on EU enlargement: Ukraine the most favoured for accession. https://euneighbourseast.eu/news/latest-news/new-eurobarometer-survey-on-eu-enlargement-ukraine-the-most-favoured-for-accession/

44 European External Action Service. (2026, March). 4th EEAS report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

45 European External Action Service. (n.d.). EU security and defence partnerships. https://www.eeas.europa.eu/eeas/eu-security-and-defence-partnerships_en


European Union
EXTERNAL ACTION


CENTER FOR COUNTERING
DISINFORMATION