



Research

www.euawareness.org

#KnowledgeAgainstManipulation

Research # 2

Dr George Robakidze

Russian Foreign Information Manipulation and Interference Inside the European Union: Democratic Legitimacy and the Limits of Resilience

*A comparative analysis of Russian Foreign Information Manipulation and Interference in EU Member States
and the EU's eastern neighbourhood (January 2025 to October 2026) — examining objectives, toolkits,
laundering models, regional patterns and the limits of resilience.*

The opinions and conclusions expressed are those of the author and do not necessarily reflect the views of
the EU Awareness Centre

October 2026

Executive Summary

Russian information operations accompanied elections across the European Union in 2026, from Hungary and Bulgaria in the spring to the German Länder, Sweden, Estonia and Latvia in the autumn. Building on the first study in this series, which examined Armenia, Georgia, Moldova and Ukraine, this paper asks whether EU membership protects against Russian foreign information manipulation and interference (FIMI), how the EU case compares with the eastern neighbourhood, and what the elections of 2024 to 2026 reveal about the limits of FIMI's effect.

The central argument is that, inside the EU, Russia's most effective laundering nodes are often democratically legitimate actors protected by the norms that membership upholds. This democratic legitimacy paradox has a corrective side: the rule of law that shelters such actors also preserves the means of removing them, as Hungary's election of April 2026 showed. The paper distinguishes documented cooperation, contact without coordination and independent alignment, and does not treat Eurosceptic voices as instruments of Moscow. The weight of current evidence suggests that Russian operations inside the EU primarily amplify existing domestic political alignments rather than manufacture them.

Russia uses one toolkit in both theatres: Storm-1516, Matryoshka and the Pravda network operate against Member States and neighbourhood states alike. Inside the EU, where Russian state media are banned from broadcasting, operations disguise their origin from the outset and rely increasingly on commercial services and AI-generated content. Membership provides sanctions, platform regulation, national attribution capacities and independent courts, but gaps remain: restricted platform data, linguistic fragmentation, economic grievances and the paradox itself. France and Germany face the largest volume of operations and have gone furthest in public attribution. Central and Eastern Europe shows the widest variation, from documented cooperation at government level in Hungary to the annulment of Romania's presidential election. The Nordic authorities assess their countries as a low priority for Moscow.

The decisive variable is not membership as such but whether the state is on the side of defence. In Georgia the state itself performs the laundering function; in Moldova, determined institutions with EU support limited the effect of an organised vote-buying network. Across both theatres, election outcomes did not follow the intensity of operations. Research on effects points the same way: party positions shape pro-Kremlin attitudes more than foreign content does, and operations gain traction mainly where trust is low, where domestic voices carry them or where the state becomes a channel. Over-attribution has its own costs, as the unfounded claims that strikes on Yandex data centres had silenced Russian bots showed.

The paper makes seven recommendations, linked to the European Democracy Shield: target the commercial supply chain; protect counter-FIMI capacity from political pressure; attribute operations with stated confidence; secure researchers' access to platform data and enforce the Digital Services Act; help newsrooms verify fabricated material once rather than many times; keep the threat in proportion; and extend EU instruments to the eastern neighbourhood.

I. Introduction, Research Questions and Scope

Between January and October 2026, Russian information operations accompanied elections across the European Union: in Hungary and Bulgaria in the spring, and in the German Länder, Sweden, Estonia and Latvia in the autumn.¹ The European External Action Service (EEAS) recorded 540 FIMI incidents in 2025 and placed France and Germany among the four most targeted countries, alongside Ukraine and Moldova. It attributed 29 per cent of the incidents to Russia and 6 per cent to China; the remainder showed indicators of coordination with Russian

¹ Catherine Belton, "To tilt Hungarian election, Russians proposed staging assassination attempt," The Washington Post, 21 March 2026, <https://www.washingtonpost.com/world/2026/03/21/hungary-election-interference-russia-orban/>; Paolo Cesarini, "Four General Elections, Four Information Battlegrounds," European Digital Media Observatory, 23 July 2026, <https://edmo.eu/blog/four-general-elections-four-information-battlegrounds-comparing-vulnerabilities-across-hungary-bulgaria-cyprus-and-malta/>; Pablo Maristany de las Casas, "An old dog with no new tricks: Matryoshka targets regional elections in Germany," Institute for Strategic Dialogue, 4 September 2026, <https://www.isdglobal.org/digital-dispatch/investigation-an-old-dog-with-no-new-tricks-matryoshka-targets-regional-elections-in-germany/>; Petra Pavlovičová, "Swedish election 'not a priority' for Moscow interference but still a target for troll farms and disinformation," EUobserver, 8 September 2026, <https://euobserver.com/235865/swedish-election-not-a-priority-for-moscow-interference-but-still-a-target-for-troll-farms-and-disinformation/>; Giedre Peseckyte, "Fake NATO deaths, Epstein claims and drones: how Russia targets elections in the Baltics," Euronews, 6 October 2026, <https://www.euronews.com/2026/10/06/fake-nato-deaths-epstein-claims-and-drones-how-russia-targets-elections-in-the-baltics>, reporting findings of the threat-intelligence company Refute.

or Chinese assets.² The European Union is not merely the background to Russian operations in its neighbourhood. It is one of their principal targets.

The first study in this series, *Russian Foreign Information Manipulation and Interference (FIMI) Operations across the EU's Eastern Neighbourhood*, published by the EU Awareness Centre in June 2026, examined Armenia, Georgia, Moldova and Ukraine. It concluded that Russian FIMI in these countries is systematic rather than episodic and serves a single purpose, preventing the consolidation of sovereign, democratically governed states oriented towards the West, but relies on different tools in each country: finance-driven proxy networks in Moldova, the governing party as the main channel of Kremlin narratives in Georgia, narratives of Western abandonment in Armenia and narrative preparation for military action in Ukraine. The study called this pattern the modular implementation principle.³ The present study asks what happens when the same instruments are turned against EU Member States. It is an independent study, but it uses the conceptual framework of the first so that the findings of the two can be compared directly.

The paper addresses three questions. The first is whether EU membership constitutes a structural defence against Russian FIMI, or whether it changes only the form in which Russia exploits a society. The second is how Russian objectives, methods, laundering models and outcomes inside the EU compare with those documented for the eastern neighbourhood. The third is what the electoral cycle of 2024–2026, in both theatres, reveals about the limits of FIMI's effect on elections.

The central argument is that, within the EU, Russia's most effective laundering nodes are often democratically legitimate actors whose activities are sheltered by the legal, political and institutional norms that EU membership upholds. The evidence of 2026 refines this argument in two ways. First, the paradox has a corrective counterpart. In Hungary's election of 12 April 2026, Tisza won a two-thirds majority despite documented Russian operations in favour of the incumbent, although only after sixteen years in which the government's electoral mandate shielded it from effective EU sanction.⁴ Second, the paradox runs in both directions. Attributing domestic Euroscepticism primarily to foreign bots overstates external manipulation and ignores evidence that the positions of voters' preferred parties are the strongest correlate of neutral and pro-Kremlin attitudes in Europe.⁵ The weight of current evidence therefore suggests that Russian influence operations primarily amplify existing domestic political alignments rather than manufacture them.

The analysis covers the period from January 2025 to October 2026. Member States are grouped in four regional clusters: the Baltic States, Central and Eastern Europe, Western Europe and the Nordic States. Individual countries are discussed where the evidence of Russian operations is substantial, as for the larger Member States, or where a case shows Russian FIMI with particular clarity. Norway, a NATO member outside the EU, serves as a point of comparison.

II. Research Design: Continuity with the First Study

A comparison is possible only if both studies use the same concepts. This paper therefore adopts the definitions and tools of the first study: the EEAS definition of FIMI as “a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes”, with its four dimensions of actors, behaviour, content and effects; the four-tier model of Russia's information architecture; the concept of information laundering; the six-step operational grammar; and the modular implementation principle.⁶

² European External Action Service, 4th EEAS Report on Foreign Information Manipulation and Interference Threats, Brussels, March 2026, pp. 5 and 10, https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.

³ George Robakidze, “Russian Foreign Information Manipulation and Interference (FIMI) Operations across the EU's Eastern Neighbourhood,” EU Awareness Centre, 18 June 2026, <https://euawareness.org/analytics/russian-foreign-information-manipulation-and-interference-fimi-operations-in-the-post-soviet-neighbourhood/>, in particular Sections VI, VII and IX. Referred to in this paper as “the first study.”

⁴ Atlantic Council, “Fast Thinking: Orbán's out in Hungary. Now what?,” 12 April 2026, <https://www.atlanticcouncil.org/content-series/fastthinking/fast-thinking-orbans-out-in-hungary-now-what/>; Belton, “To tilt Hungarian election”; Cesarini, “Four General Elections.”; George Robakidze, “An Election That Extends Beyond Hungary,” EU Awareness Centre, 9 April 2026, <https://euawareness.org/analytics/an-election-that-extends-beyond-hungary/>.

⁵ Filip Kostelka et al., “Mass attitudes towards Russia's aggression against Ukraine: Tentative support for top-down opinion formation,” European Journal of Political Research, published online 10 June 2026, <https://doi.org/10.1017/S1475676526101352>. The authors ask that their findings be interpreted with caution.

⁶ Robakidze, “Russian FIMI Operations,” Section I (definition and four dimensions, after European External Action Service, “Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI),” https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en); Section III (four-tier model); Section I (information laundering, drawing on NATO Strategic

The FIMI concept closely mirrors the framework that James Pamment developed in 2020 for the EEAS, in a series that also found EU policy on disinformation marked by “a lack of terminological clarity, unclear and untested legal foundations, a weak evidence base”.⁷ Bennett and Livingston trace the spread of disinformation in Western democracies to declining confidence in institutions, and associate its sources with both nationalist, primarily radical-right, and foreign, commonly Russian, strategies.⁸ The emphasis of the FIMI concept on foreign origin fits the eastern neighbourhood, where the source of most operations is rarely in doubt. Inside the EU, where Russian narratives are often carried by domestic parties and media, the line between foreign interference and domestic political speech is itself contested. Table 1 sets out how the design of the present study relates to that of the first.

Table 1. Research design of the first and the present study

Dimension	First study: eastern neighbourhood	Present study: EU Member States
Research question	How Russian FIMI operates in four neighbourhood states and which vulnerabilities it exploits	Whether EU membership protects against Russian FIMI, and how the EU case compares with the neighbourhood
Unit of analysis	Four country case studies	Four regional clusters; Member States named where evidence is substantial or a case is distinctive; Norway as a comparator
Period	Ukraine up to February 2022; Armenia, Georgia and Moldova up to the first half of 2026	January 2025 to October 2026
Framework	EEAS FIMI definition; four-tier architecture; information laundering; six-step grammar; modular implementation	Adopted, with three additional concepts: democratic legitimacy paradox, inverted laundering, FIMI supply chain
Evidence base	EEAS reporting, research organisations, official documents, media, democracy indices	As in the first study, plus national attribution agencies and peer-reviewed literature
Attribution standard	Not specified	Attributions reported in the attributing body’s own terms and at its level of confidence

Source: author’s compilation.

Three concepts are specific to this paper. The first is the democratic legitimacy paradox. The underlying tension is old: Karl Loewenstein argued in 1937 that democracies must be able to defend themselves against movements that use democratic freedoms to undermine democracy, and Karl Popper formulated the “paradox of tolerance” in 1945.⁹ Walker and Ludwig later used the term “sharp power” for the way authoritarian states exploit the openness of democratic societies to “pierce, penetrate, or perforate” them.¹⁰ The difference from the eastern neighbourhood is not that laundering nodes inside the EU are elected: Georgian Dream is also an elected government, and the first study identified it as the main domestic channel of Kremlin narratives in Georgia.¹¹ The difference is that, inside the EU, functioning rule-of-law systems both protect such actors and retain the capacity to correct them. The concept must be applied with care. Following Pamment’s question of whether an actor works on its own account or on behalf of another,¹² this paper separates three degrees of involvement: documented cooperation with Russian state actors, such as payment or operational coordination; contact

Communications Centre of Excellence, Information Laundering in the Nordic-Baltic Region, Riga, December 2020); Section IV (operational grammar); Section VII (modular implementation).

⁷ James Pamment, “The EU’s Role in Fighting Disinformation: Taking Back the Initiative,” Carnegie Endowment for International Peace, July 2020, <https://carnegieendowment.org/research/2020/07/the-eus-role-in-fighting-disinformation-taking-back-the-initiative>; James Pamment, “The EU’s Role in Fighting Disinformation: Crafting a Disinformation Framework,” Carnegie Endowment for International Peace, September 2020, <https://carnegieendowment.org/research/2020/09/the-eus-role-in-fighting-disinformation-crafting-a-disinformation-framework>.

⁸ W. Lance Bennett and Steven Livingston, “The disinformation order: Disruptive communication and the decline of democratic institutions,” *European Journal of Communication* 33, no. 2 (2018): 122–139, <https://doi.org/10.1177/0267323118760317>.

⁹ Karl Loewenstein, “Militant Democracy and Fundamental Rights,” *American Political Science Review* 31, nos. 3 and 4 (1937); Karl Popper, *The Open Society and Its Enemies*, vol. 1 (London: Routledge, 1945), chapter 7, note 4.

¹⁰ Christopher Walker and Jessica Ludwig, “From ‘Soft Power’ to ‘Sharp Power’: Rising Authoritarian Influence in the Democratic World,” in *Sharp Power: Rising Authoritarian Influence*, National Endowment for Democracy, December 2017, <https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/>.

¹¹ Robakidze, “Russian FIMI Operations,” Section VI (Georgia).

¹² Pamment, “Crafting a Disinformation Framework,” discussion of the behaviour component of the framework.

without evidence of coordination; and independent alignment, in which domestic actors advance similar narratives for their own reasons. The term “laundering node” is reserved for the first. Alignment alone is not treated as evidence of Russian direction, and the paper does not suggest that parties or voters holding Eurosceptic or Russia-friendly views act on Moscow’s behalf. To do so would lend credibility to Russian claims that European governments silence their critics.

The second concept is inverted laundering. In the neighbourhood, laundering through local validators often follows injection through openly Russian sources. Inside the EU, where RT and Sputnik have been suspended from broadcasting since March 2022,¹³ an operation must convert content of Kremlin origin into apparently domestic speech as early as possible. The third is the FIMI supply chain. The EEAS notes that outsourcing to intermediaries provides deniability and complicates attribution, and that 91 per cent of the channels in its network map of 2025 were unattributed, state-aligned channels.¹⁴ Peer-reviewed research describes the same movement towards commercial “digital mercenaries” and towards service providers that overlap with organised cybercrime.¹⁵ Russian FIMI is therefore treated here as a chain of functions, from strategy and content production to hosting, distribution and paid amplification, each of which may be performed by a different, often commercial, actor.

Evidence is drawn from official documents, including EEAS reports, Council decisions and the assessments of national agencies such as France’s VIGINUM; research organisations; peer-reviewed literature; and reputable journalism. Evidence is considered up to October 2026. Attributions are reported in the terms, and at the level of confidence, used by the attributing body, and they are not strengthened in the retelling.

III. Russia’s Strategic Objectives Inside the EU

The first study identified four objectives of Russian FIMI in the eastern neighbourhood: blocking Euro-Atlantic integration, eroding institutional trust, intensifying polarisation and preparing the ground for coercive action.¹⁶ Member States have already made the choice that Russia seeks to prevent in its neighbourhood. Russian objectives inside the EU are therefore directed less at preventing integration than at reversing or exhausting its consequences: the sanctions regime, support for Ukraine and the cohesion of the Union itself (Table 2).

Table 2. Russian strategic objectives in the two theatres

Objective (first study)	Eastern neighbourhood	EU Member States
Blocking Euro-Atlantic integration	Prevent or reverse alignment with the EU and NATO	Reverse or exhaust its consequences: sanctions, support for Ukraine, enlargement
Eroding institutional trust	Courts, electoral bodies, media and civil society	The same national institutions, together with EU institutions and EU decision-making
Intensifying polarisation	Ethnic, linguistic, religious and economic cleavages	Migration, cost of living, energy prices and war fatigue
Preparing for coercive action	Narrative preparation for military action, most clearly in Ukraine before 2022	Shaping perceptions of hybrid actions against Member States
Exploiting the unanimity rule (EU only)	Not applicable	Securing vetoes or delays on sanctions and support for Ukraine through a sympathetic government

Source: author’s compilation, based on the first study and the sources cited in this section.

¹³ Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine, <https://eur-lex.europa.eu/eli/reg/2022/350/oj>.

¹⁴ EEAS, 4th Report, pp. 21 and 26–27.

¹⁵ Renée DiResta, Shelby Grossman and Alexandra Siegel, “In-House Vs. Outsourced Trolls: How Digital Mercenaries Shape State Influence Strategies,” Political Communication 39, no. 2 (2022): 222–253, <https://doi.org/10.1080/10584609.2021.1994065>; Thomas Delorme, “Foreign Information Manipulation and Interference: A Criminal Economy in the Making,” Journal of Illicit Economies and Development, 2026, <https://doi.org/10.31389/jied.334>.

¹⁶ Robakidze, “Russian FIMI Operations,” Section II.

Fracturing Unity Through the Unanimity Rule

Decisions on sanctions, and on most of the EU's common foreign and security policy, require unanimity in the Council.¹⁷ For Russia, a single sympathetic government is therefore worth more than a broad but diffuse current of opinion. In early 2026 Budapest blocked a €90 billion EU loan to Ukraine, citing a dispute over the transit of Russian oil through the Druzhba pipeline, a dispute that also delayed a new sanctions package. Within two weeks of the April election, Hungary lifted its veto, and EU ambassadors approved both the loan and the sanctions.¹⁸ Under Orbán, Hungary combined two roles that Russia rarely finds in one place: an amplifier of Kremlin-aligned narratives at home and a veto player in Brussels.¹⁹ The unanimity rule is what turns a laundering node into a veto player.

Exhausting European Support for Ukraine

The targeting has followed the money. According to NewsGuard, citing the Kiel Institute for the World Economy, US aid to Ukraine fell by 99 per cent in 2025, while European military aid rose by 67 per cent compared with its 2022–2024 average. Over the same period, the Russian information manipulation set Storm-1516 turned to France and Germany: between January 2025 and February 2026 it advanced 34 false claims about the two countries, spread through 175,000 posts and articles and viewed 274 million times on X alone, against 12 such claims in the whole of 2024.²⁰ The targets were Germany, now Ukraine's largest military donor, and France, whose President has become one of Kyiv's most prominent advocates in Europe.

Amplifying Domestic Divisions

The EEAS found that nearly half of the incidents it recorded in 2025 were triggered by specific events, especially breaking news and elections, and that Russia targeted elections in Germany, Poland, Romania, the Czech Republic and Moldova during the year.²¹ Much of the material Russia needs is already present in domestic politics. A study of eleven European radical right parties found that, after the 2022 invasion, most neither defended Russia nor openly changed position; instead, they used the war to sharpen their opposition to the EU, above all through arguments about energy prices and sanctions.²² A second study finds the European far right increasingly divided on Russia since 2022.²³ Russian operations are most effective when they amplify narratives that domestic actors already produce for their own reasons.

A Long-Term Investment

These objectives are pursued as a permanent programme. The EEAS reports that Russia's budget for state-controlled media is set to reach 146.3 billion roubles, approximately €1.56 billion, in 2026, 7 per cent more than in 2025, and that funding for FIMI will rise as part of that increase.²⁴ The figure does not include the cost of covert operations, much of which is outsourced. The European response has also become permanent: by October 2026 the Council's sanctions regime against Russia's destabilising activities covered 80 individuals and 20 entities, up from 65 and 17 in January, and it has been extended until October 2027.²⁵

¹⁷ Treaty on European Union, Article 31(1); Treaty on the Functioning of the European Union, Article 215.

¹⁸ "EU to finalize €90bn Ukraine loan, as Hungary lifts veto," Insight Hungary (444), 25 April 2026, <https://insighthungary.444.hu/2026/04/25/eu-to-finalize-90bn-ukraine-loan-as-hungary-lifts-veto>.

¹⁹ Robakidze, "Election Beyond Hungary"; Belton, "To tilt Hungarian election."

²⁰ Natalie Huet, Mascha Wolf and Eva Maitland, "Russian Influence Campaign Shifts to Target Ukraine's European Allies Funding its Defense," NewsGuard, 27 February 2026, <https://www.newsguardtech.com/special-reports/russian-influence-campaign-storm-1516-targets-france-germany/>.

²¹ EEAS, 4th Report, pp. 5, 11 and 15.

²² Chendi Wang and Argyrios Altiparmakis, "What happened to Putin's friends? The radical right's reaction to the Russian invasion on social media," European Union Politics (2025), <https://pubmed.ncbi.nlm.nih.gov/40417648/>.

²³ Adam Holesch, Piotr Zagórski and Aron Buzogány, "Assertiveness and war fatigue: European party dynamics during Russia's war in Ukraine," Journal of European Integration (2026), <https://doi.org/10.1080/07036337.2026.2616344>.

²⁴ EEAS, 4th Report, p. 13.

²⁵ Council of the European Union, "Russian hybrid threats: Council sanctions six individuals over information manipulation activities," press release, 29 January 2026, <https://www.consilium.europa.eu/en/press/press-releases/2026/01/29/russian-hybrid-threats-council-sanctions-six-individuals-over-information-manipulation-activities/>; Council of the European Union, "Russia's hybrid activities: Council prolongs restrictive measures until October 2027," press release, 8 October 2026, https://www.eeas.europa.eu/delegations/ukraine/russias-hybrid-activities-council-prolongs-restrictive-measures-until-october-2027_en, which refers to the European Council conclusions of 18 and 19 June 2026 on hybrid attacks against the Union.

IV. The FIMI Toolkit and Supply Chain Inside the EU

The first study described Russia's toolkit in the eastern neighbourhood: state media, impersonation of trusted media, the Pravda network, bot networks, oligarchic proxies and AI-generated content.²⁶ The same instruments operate inside the EU, but they are combined differently (Table 3).

Table 3. The Russian FIMI toolkit in the two theatres

Instrument	Eastern neighbourhood (first study)	EU Member States
State media	Overt broadcasting in Russian and national languages; bans circumvented through mirror sites	Broadcasting suspended since 2022; content recirculated on Telegram, Facebook, TikTok and other platforms
Impersonation of media	Cloned Western media brands under typosquatted domains	Same technique at larger scale; fake regional outlets and AI-narrated videos styled as news reports
Pravda/Portal Kombat network	Automated republication of Kremlin content, with local-language portals	Portals in many EU languages and regions; some 10,000 articles a day
Bot networks and amplification	Coordinated fake accounts across platforms	Increasingly bought from commercial engagement-for-hire providers
Domestic proxies	Oligarchic networks, aligned media, clerics, governing party (Georgia)	Documented paid cooperation in a few cases (Voice of Europe); broader field of independent alignment
AI-generated content	Deepfakes against political leaders (Moldova)	AI-related techniques in 27 per cent of EEAS incidents in 2025; voice cloning now routine

Source: author's compilation, based on the first study and the sources cited in this section.

State Media After the Bans

The EU suspended the broadcasting of RT and Sputnik in March 2022 and of four further outlets in May 2024, and in May 2025 broadened its framework to allow further Kremlin-controlled broadcasters to be suspended.²⁷ The bans have reduced the direct reach of Russian state media without removing its content. During Bulgaria's 2026 campaign, EDMO monitors found sanctioned Russian broadcast content still circulating on Facebook and TikTok, and Telegram, which sits outside the strictest obligations of the Digital Services Act (DSA), hosted the densest pro-Kremlin ecosystem of the four spring elections EDMO examined.²⁸ Inside the EU, state media now serve less as broadcasters than as a library of content for other channels.

Information Manipulation Sets

Three information manipulation sets dominate the documented record. The first is Storm-1516. France's agency against foreign digital interference, VIGINUM, analysed 77 of its operations between August 2023 and March 2025 and found that it seeds content through burner and paid accounts, launders it through foreign media and amplifies it through pro-Russian networks. VIGINUM established the involvement of John Mark Dougan, a former US police officer living in Russia, and described Yury Khoroshenky, publicly accused of financing and coordinating the set, as "a potential officer of the GRU Unit 29155".²⁹ The EU sanctioned Dougan in December 2025. In 2026

²⁶ Robakidze, "Russian FIMI Operations," Section III.

²⁷ Council Regulation (EU) 2022/350 of 1 March 2022, <https://eur-lex.europa.eu/eli/reg/2022/350/oj>; Council of the European Union, "Russia's war of aggression against Ukraine: Council bans broadcasting activities in the European Union of four more Russia-associated media outlets," press release, 17 May 2024, <https://www.consilium.europa.eu/en/press/press-releases/2024/05/17/russia-s-war-of-aggression-against-ukraine-council-bans-broadcasting-activities-in-the-european-union-of-four-more-russia-associated-media-outlets/>; Naja Bentzen, "The European Democracy Shield: An overview," European Parliamentary Research Service, January 2026, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782603/EPRS_ATAG\(2026\)782603_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782603/EPRS_ATAG(2026)782603_EN.pdf).

²⁸ Cesarini, "Four General Elections."

²⁹ VIGINUM (Secrétariat général de la défense et de la sécurité nationale), technical report on the Russian information manipulation set Storm-1516, May 2025, pp. 3, 11–19 and 21–27, https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.

the set's infrastructure was also used against Armenia's parliamentary election, a direct link between the two theatres compared in this paper.³⁰

The second set is Matryoshka, also tracked as Operation Overload, which specialises in short videos and forged reports imitating established media. Before Germany's state and municipal elections of September 2026, the Institute for Strategic Dialogue identified 269 Matryoshka posts in 21 days and found the operation predictable and technically weak, with limited reach unless others amplified it; in August 2026 VIGINUM attributed to it forged media reports targeting candidates in the 2027 French presidential campaign.³¹ The third is the operation known as Doppelganger, or RRN, run by the Social Design Agency, which the EU sanctioned in July 2023; the EEAS still recorded RRN sites promoting AI-generated articles in 2025.³² Beneath all three runs the Pravda network, which in 2025 published on average some 10,000 articles a day across 101 websites and, at the end of 2024, added 26 subdomains for specific countries and regions, including the Basque Country.³³ Its value lies less in persuading readers than in keeping Kremlin narratives permanently available to search engines, AI systems and anyone looking for material to share.

The Supply Chain: Outsourcing and Commercial Services

These sets increasingly depend on services that Russia buys rather than builds, and the EEAS now proposes to deter FIMI by targeting the intermediaries and service providers on which operations depend.³⁴ VIGINUM found that Storm-1516 relies on paid accounts and on foreign media very likely paid to publish its stories, and peer-reviewed research shows the same reliance on commercial "digital mercenaries" and on providers that overlap with organised cybercrime.³⁵ The monitoring group Antibot4Navalny assessed in October 2026 that the network amplifying Storm-1516 content is most likely a commercial engagement-for-hire provider rather than a state-run asset.³⁶ Attribution therefore becomes harder, and disruption has to reach the commercial layer.

Political Proxies

The Voice of Europe case remains the clearest documented example of the first degree of involvement. On 27 March 2024 the Czech government, acting on information from its security service, sanctioned Viktor Medvedchuk and Artem Marchevskiy for running the Prague-registered outlet as a pro-Russian influence operation that financed cooperation with journalists and gave covert financial support to selected candidates in the European Parliament elections; the Council suspended its broadcasting in May 2024.³⁷ In a separate case, Nathan Gill, a former British Member of the European Parliament, was sentenced in November 2025 to ten years and six months' imprisonment for accepting bribes to make pro-Russian statements.³⁸ Such cases are few, and they must not be confused with the much larger field of independent alignment. Both produce similar content; only evidence of payment, coordination or instruction distinguishes them, and such evidence usually emerges, if at all, through intelligence work or criminal proceedings years later. This is the practical core of the democratic legitimacy paradox.

³⁰ Huet, Wolf and Maitland, "Russian Influence Campaign Shifts"; Andreas Sjöstedt et al., "Uncovering the digital infrastructure behind Russian interference in Armenian elections," DFRLab, 29 July 2026, <https://dfrlab.org/2026/07/29/uncovering-the-digital-infrastructure-behind-russian-interference-in-armenian-elections/>.

³¹ Maristany de las Casas, "Old dog"; Adèle Chatelard, "A Fake Newsroom Targets the 2027 French Campaign: Impersonated Media Identities, Fabricated Artefacts and the Matrioshka Network," Facts vs Manipulation #13, EU Awareness Centre, 1 October 2026, <https://euawareness.org/facts-vs-manipulation/manipulation-13/>.

³² European External Action Service, "Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities," 28 July 2023, https://www.eeas.europa.eu/delegations/ukraine/information-manipulation-russia%E2%80%99s-war-aggression-against-ukraine-eu-lists-seven-individuals-and-five_en; EEAS, 4th Report, section on the use of artificial intelligence.

³³ Robakidze, "Russian FIMI Operations," Section III; EEAS, 4th Report, section on information manipulation sets (Portal Kombati); Cesarini, "Four General Elections."

³⁴ EEAS, 4th Report, Executive Summary.

³⁵ VIGINUM, Storm-1516, pp. 12–19; DiResta, Grossman and Siegel, "In-House Vs. Outsourced Trolls"; Delorme, "Criminal Economy."

³⁶ Martin Fornusek, "No, Ukraine's strikes on Yandex data centers didn't cripple Russian influence ops," The Kyiv Independent, 13 October 2026, <https://kyivindependent.com/no-ukraines-strikes-on-yandex-data-centers-didnt-cripple-russian-influence-ops/>, quoting the monitoring group Antibot4Navalny.

³⁷ Reuters, "Czechs sanction Medvedchuk, website over pro-Russian EU political influence," 27 March 2024, as published by SWI swissinfo.ch, <https://www.swissinfo.ch/eng/czechs-sanction-medvedchuk%2c-website-over-pro-russian-eu-political-influence/74431307>; Council of the European Union, "Council bans broadcasting activities."

³⁸ Counter Terrorism Policing (United Kingdom), "Former MEP jailed after accepting bribes to make pro-Russian statements," 21 November 2025, <https://www.counterterrorism.police.uk/former-mep-jailed-after-accepting-bribes-to-make-pro-russian-statements/>.

AI-Enabled Content

Artificial intelligence has changed the cost of production more than the nature of the operations. The EEAS found AI-related techniques in 27 per cent of the incidents it recorded in 2025, up from 41 cases in 2024 to 147. Synthetic audio has become standard, and both Storm-1516 and Operation Overload have moved from generic voiceovers to cloned voices. The first study documented the same techniques against President Sandu in Moldova; inside the EU they are used at a larger scale.³⁹

V. The Operational Grammar Inside the EU

The first study set out a six-step operational grammar: narrative seeding, laundering through local validators, saturation, contradiction as method, emotional targeting and synchronisation with other instruments.⁴⁰ All six steps are visible inside the EU, but their weight and sequence differ (Table 4).

Table 4. The operational grammar in the two theatres

Step	Eastern neighbourhood (first study)	EU Member States
Narrative seeding	Russian state media and aligned Telegram channels as entry points	Burner accounts, fake news sites and impersonated media brands; state media mainly as a source of content
Laundering through local validators	A later step, after injection through openly Russian sources	Required from the start; paid foreign media and domestic voices where alignment exists
Saturation	High volume during elections, most clearly in Moldova in 2024	Industrial volume (Pravda network: some 10,000 articles a day)
Contradiction as method	Competing versions that erode certainty	The same, with versions tailored to different languages and audiences
Emotional targeting	Fear of war, abandonment, “traditional values”	Fear and anger over migration, the war and EU policy
Synchronisation	Preparation for military action, most clearly in Ukraine	Accompanies hybrid actions such as airspace violations, without open military aggression against Member States

Source: author’s compilation, based on the first study and the sources cited in this section.

The most important difference concerns laundering. In the neighbourhood it follows injection through openly Russian channels; inside the EU, where state media are banned from broadcasting, the operation has to disguise its origin from the first moment. Storm-1516 publishes through burner accounts and very likely paid foreign media, and in 2025 many incidents recorded by the EEAS involved the impersonation of Western news outlets.⁴¹ Two further features stand out. Fabricated stories are anchored to genuine events: in Latvia, a false report that a Ukrainian soldier had killed three NATO servicemen was timed to a real military exercise. And stories travel selectively: EDMO found that claims about internationally known figures crossed borders quickly, while claims about domestic candidates mostly stayed at home.⁴² Linguistic fragmentation therefore protects the EU only partly.

Synchronisation also takes a different form. In the neighbourhood, FIMI prepared the ground for military action in Ukraine; inside the EU, it accompanies hybrid actions below the threshold of open aggression. When Russian drones violated Polish airspace on the night of 9 to 10 September 2025, Poland requested consultations under Article 4 of the North Atlantic Treaty and NATO launched Eastern Sentry two days later, while Prime Minister Tusk urged a “fact-based interpretation” of events whose meaning was quickly contested.⁴³

³⁹ EEAS, 4th Report, section on the use of artificial intelligence; Robakidze, “Russian FIMI Operations,” Section III.

⁴⁰ Robakidze, “Russian FIMI Operations,” Section IV.

⁴¹ VIGINUM, Storm-1516, pp. 12–17; EEAS, 4th Report, section on the use of artificial intelligence.

⁴² Peseckyte, “Fake NATO deaths”; Cesarini, “Four General Elections.”

⁴³ NATO, “Statement by NATO Secretary General Mark Rutte on the violation of Polish airspace by Russian drones,” 10 September 2025, <https://www.nato.int/en/news-and-events/events/transcripts/2025/09/10/statement>; NATO, “NATO launches ‘Eastern Sentry’ to bolster posture along eastern flank,” 12 September 2025, <https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank>; Chancellery of the Prime Minister of Poland, “‘Eastern Sentry’: NATO Responds to Russian Provocations in Poland,” <https://www.gov.pl/web/primeminister/eastern-sentry-nato-responds-to-russian-provocations-in-poland>.

VI. Structural Vulnerabilities: What EU Membership Does and Does Not Protect Against

The first study traced the effectiveness of Russian FIMI in the neighbourhood to four structural vulnerabilities: linguistic dependence on Russian-language media, weak institutions and low public trust, unresolved conflicts, and the authority of national churches in identity politics.⁴⁴ EU membership changes this picture substantially, but not entirely.

What Membership Protects Against

Membership provides instruments that no country in the first study possesses. The EU can suspend Russian broadcasters across 27 states and sanction those involved in FIMI. Its platform regulation has begun to produce enforcement: in December 2025 the Commission adopted its first non-compliance decision under the DSA, fining X €120 million, among other reasons for obstructing researchers' access to data. The European Democracy Shield, presented in November 2025, adds a European Centre for Democratic Resilience to pool detection and early-warning capacities.⁴⁵ Member States have attribution capacities of their own, and membership anchors independent courts, media and electoral administrations, which make state capture of the Georgian kind far harder, though not impossible.

What Membership Does Not Protect Against

Four gaps remain. The first lies in platform architecture: the EEAS recorded 88 per cent of FIMI instances in 2025 on X, Telegram remains outside the DSA's strictest obligations, and most platforms restrict the data needed to measure manipulation; in Bulgaria, thresholds in Meta's research tools excluded 291 election-related posts with more than 12 million views.⁴⁶ The second is fragmentation across 24 official languages and national information spaces, which requires monitoring capacity in each Member State. The third is the democratic legitimacy paradox itself. The fourth is economic grievance: energy prices and the cost of sanctions and of supporting Ukraine provide authentic material that domestic parties use for their own purposes and Russian operations amplify.⁴⁷

Table 5. Structural vulnerabilities in the two theatres

Vulnerability (first study)	Eastern neighbourhood	EU Member States
Linguistic dependence and media environment	Russian-language media reach beyond Russian speakers; bans circumvented	Dependence limited mainly to Russian-speaking minorities; fragmentation across 24 languages; gaps on Telegram and X
Weak institutions and low public trust	Corruption, elite capture, weak courts	Strong institutions overall, but uneven; erosion of checks in Hungary (2010–2026)
Unresolved conflicts and security anxieties	Occupied territories, Karabakh, Transnistria	Fear of escalation, airspace violations, the cost of supporting Ukraine
Church authority and identity politics	Trusted national churches amplifying “traditional values” narratives	Identity narratives centred on migration, sovereignty and opposition to “Brussels”
Specific to the EU	Not applicable	Unanimity rule; elected actors protected by democratic norms; platform regulation gaps

Source: author's compilation, based on the first study and the sources cited in this section.

Government as Laundering Node: The Case of Hungary

The most serious vulnerability arises when the government itself performs the laundering function, as the first study showed for Georgia. Hungary between 2010 and 2026 is the clearest EU case. Over sixteen years the Orbán government consolidated control through nearly fifty constitutional amendments and changes to the electoral system, and repeatedly used its veto on EU decisions concerning sanctions and Ukraine.⁴⁸ Leaked recordings of telephone calls between Foreign Minister Szijjártó and Sergei Lavrov from 2023 to 2025, obtained and verified

⁴⁴ Robakidze, “Russian FIMI Operations,” Section V.

⁴⁵ Anna Pinget, “EU Fines X €120 Million in First DSA Non-Compliance Decision,” eucrim, 19 January 2026, <https://eucrim.eu/news/eu-fines-x-120-million-in-first-dsa-non-compliance-decision/>; Bentzen, “European Democracy Shield.”

⁴⁶ EEAS, 4th Report, section on platforms and observables; Cesarini, “Four General Elections.”

⁴⁷ Wang and Altiparmakis, “Putin's friends”; Kostelka et al., “Mass attitudes.”

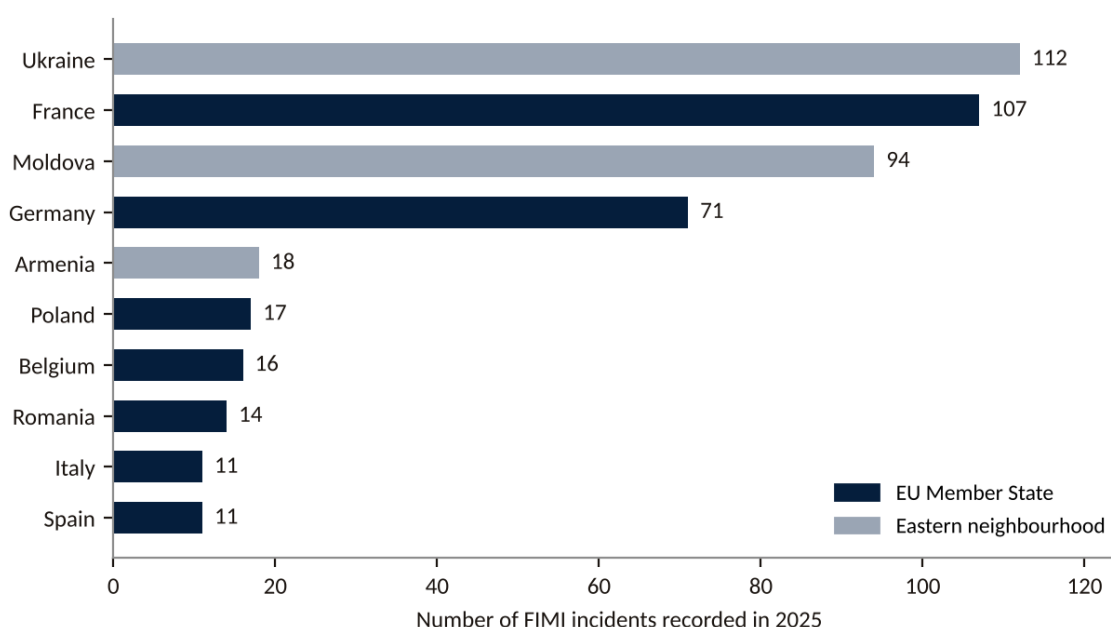
⁴⁸ Robakidze, “Election Beyond Hungary.”

by a consortium of investigative outlets, show the Hungarian minister sharing information on EU deliberations with his Russian counterpart and coordinating efforts to remove individuals from EU sanctions lists; in one case, the sister of the oligarch Alisher Usmanov was delisted seven months after the request was discussed.⁴⁹ This is documented cooperation at government level. During the 2026 campaign, EDMO found domestic networks tied to Fidesz, AI-assisted propaganda and at least two distinct Russian-linked operations converging in a single campaign. Voters removed the government nonetheless.⁵⁰

VII. Regional Profiles

These instruments are used across the Union, but not evenly. The EEAS recorded 540 FIMI incidents worldwide in 2025. Among the Member States for which it publishes figures, France (107) and Germany (71) were targeted far more often than the rest; Poland, Belgium, Romania, Italy and Spain each recorded between 11 and 17 incidents. In the eastern neighbourhood, Ukraine (112) and Moldova (94) remained the main targets, and Armenia (18) was rising ahead of its 2026 election.⁵¹ The figures include incidents linked to China and many that could not be attributed, so they measure exposure rather than Russian activity alone, but they show that the volume of operations follows political weight and the electoral calendar more than geography (Figure 1).

Figure 1. FIMI incidents recorded by the EEAS in 2025, by targeted country (selection)



Source: European External Action Service, 4th EEAS Report on FIMI Threats, March 2026, “2025 FIMI in numbers”. Only countries for which the EEAS publishes a figure are shown; countries outside the two theatres are omitted, and Georgia is not among the countries listed. The figures include incidents attributed to Russia and China and unattributed incidents.

The Baltic States

In the Baltic States, the operations of 2026 concentrated on the security questions that shape voters’ choices rather than on candidates or voting procedures. The fabricated report of NATO deaths in Latvia was spread by dozens of accounts with a combined audience of more than 1.85 million before the vote, and a fake site imitating EUobserver linked Estonia’s outgoing President Alar Karis to the Epstein network. The aim was to erode trust in Ukraine, in NATO and in the countries’ own air defences. The region also lies where FIMI meets hybrid action: the EEAS recorded drone incursions, sabotage and attacks on critical infrastructure in Lithuania and Estonia, as in Poland and Romania, accompanied by FIMI designed to manage public perception.⁵²

⁴⁹ Wojciech Cieřla et al., “Hotline to the Kremlin: How Hungary Colluded With Russia to Weaken EU Sanctions,” OCCRP, with VSquare, FRONTSTORY, Delfi Estonia, The Insider and the Investigative Center of Ján Kuciak, 31 March 2026, <https://www.occrp.org/en/scoop/hotline-to-the-kremlin-how-hungary-colluded-with-russia-to-weaken-eu-sanctions>.

⁵⁰ Cesarini, “Four General Elections”; Atlantic Council, “Orbán’s out in Hungary.”

⁵¹ EEAS, 4th Report, p. 5 and section “2025 FIMI in numbers.” Of the 540 incidents, the EEAS attributed 29 per cent to Russia and 6 per cent to China; the remaining 65 per cent were unattributed but showed indicators of coordination with Russian or Chinese infrastructure.

⁵² Peseckyte, “Fake NATO deaths”; EEAS, 4th Report, Executive Summary.

Latvia's election of 3 October 2026 shows how far the evidence goes and where it stops. Prime Minister Andris Kūrbegs's United List won 35.3 per cent and 41 of 100 seats. Latvia First came second with 13.1 per cent, and Sovereign Power/Union of New Latvians, which draws much of its support from Russian speakers, third with 11.7 per cent.⁵³ In the 502 channels monitored by the Centre for East European Policy Studies, Sovereign Power and Latvia First were among the few parties mentioned more positively than negatively, but the data showed no coordination between the parties' accounts and the channels that amplified them. The Kremlin-aligned core of this space, about a dozen Telegram channels around Sputnik Latvija, did not back a single list: one channel urged a vote for Sovereign Power, while the most widely reposted item of election week attacked the leader of another pro-Russian list, For Stability!. The authors judged the involvement opportunistic rather than centrally directed, and the State Security Service found no systematic Russian attempt to influence the result. One question remains open: Sovereign Power's leader, Jūlija Stepaņenko, had declared gifts of about €420,000 from her father, a construction entrepreneur in the Moscow region whose company reportedly made anti-tank obstacles for the Russian army; in September 2026 the Foreign Minister barred him from entering Latvia, and several security agencies were assessing the origin of the funds.⁵⁴ On this evidence, the case belongs to independent alignment, amplified opportunistically; the financial question does not, so far, establish cooperation.

Central and Eastern Europe

Central and Eastern Europe offers the widest range of cases. Romania provides the first case in the Union of a national election annulled on grounds that included foreign interference. On 6 December 2024 the Constitutional Court annulled the first round of the presidential election, won by Călin Georgescu, a candidate who had been polling at around 5 per cent, on the basis of declassified intelligence reports describing a campaign run through some 25,000 accounts with a coordination that suggested a state actor. The decision was contested: the Centre for Eastern Studies described its evidentiary basis as vague, and an investigation by Snoop.ro later reported that one TikTok campaign turned in Georgescu's favour had been paid for by the governing National Liberal Party. Georgescu was barred from the rerun, which Nicușor Dan won in May 2025 with 53.6 per cent.⁵⁵ The case showed that institutions can act decisively against suspected interference, and it gave Russian operations a narrative they have used ever since.

Poland's presidential election of 2025 was targeted by Doppelganger, Operation Overload and the Pravda network. According to an assessment by the FIMI-ISAC, Russia-aligned content attacked both leading candidates, presenting the contest as a "puppet theatre" controlled from abroad; the aim was to undermine the legitimacy of the outcome rather than to elect anyone. The research institute NASK reported 14,890 accounts, mostly on X, linked to coordinated inauthentic behaviour. Karol Nawrocki won the run-off with 50.89 per cent.⁵⁶ In the Czech Republic, before the elections of October 2025, analysts identified 286 interlinked TikTok accounts that spread pro-Russian content and supported several radical parties at once; Czech intelligence passed them to the regulator, TikTok removed dozens, and an intelligence source called the operation "an unsuccessful attempt".

⁵³ Centrālā vēlēšanu komisija, "15. Saeimas vēlēšanu rezultāti," final results, 16 October 2026, <https://www.cvk.lv/saeima-2026-rezultati>; Andrius Sytas, "Latvian PM on track to lead pro-Ukraine coalition after election win," Reuters, 4 October 2026, <https://www.reuters.com/world/europe/latvian-pm-track-lead-pro-ukraine-coalition-after-election-win-2026-10-04/>; Mihails Nikulkins, "Politician Stepaņenko's father blacklisted in Latvia," LSM, 24 September 2026, <https://eng.lsm.lv/article/politics/politics/24.09.2026-politician-stepanekos-father-blacklisted-in-latvia.a664668/>, quoting the political scientist Jānis Ikstens.

⁵⁴ Armands Astukevičs and Elīna Vrobļevska, Kremlis vai tā atbalss? Ārvalstu informācijas manipulācija un iejaukšanās 15. Saeimas vēlēšanās, Centre for East European Policy Studies (APPC), Riga, October 2026, Key findings 04 and 06 and chapter 6, https://appc.lv/wp-content/uploads/2026/10/Kremlis_vai_ta_atbalss_APPC_2026.pdf; Valsts drošības dienests, "VDD vērtējumā 15. Saeimas vēlēšanas kopumā aizvadītas mierīgi," 5 October 2026, <https://vdd.gov.lv/aktualitates/jaunumi/vdd-vertejuma-15-saeimas-velesanas-kopuma-aizvaditas-mierigi>; Matīss Arnicāns, "Politician Stepaņenko's family reportedly friendly with Russian arms dealer Bout," LSM, 24 September 2026, <https://eng.lsm.lv/article/politics/politics/24.09.2026-politician-stepanekos-family-reportedly-friendly-with-russian-arms-dealer-bout.a664549/>, drawing on Latvian Television and The Insider; Nikulkins, "Stepaņenko's father blacklisted."

⁵⁵ Kamil Całus, "Romania: Constitutional Court annuls the presidential election," OSW Centre for Eastern Studies, 9 December 2024, <https://osw.waw.pl/en/publikacje/analyses/2024-12-09/romania-constitutional-court-annuls-presidential-election>; Victor Goury-Laffont, "Report ties Romanian liberals to TikTok campaign that fueled pro-Russia candidate," Politico Europe, 21 December 2024, <https://www.politico.eu/article/investigation-ties-romanian-liberals-tiktok-campaign-pro-russia-candidate-calin-georgescu/>, reporting an investigation by Snoop.ro; Justin Spike and Stephen McGrath, "Romania's new pro-European president puts it back on a Western course, but fault lines remain," AP News, 19 May 2025, <https://apnews.com/article/romania-president-election-dan-simion-e665b3944752de288a2778c84e535045>; Sopo Gelava, "Kremlin-aligned actors targeted Bulgarian vote with EU interference claims," DFRLab, 9 June 2026, <https://dfrlab.org/2026/06/09/kremlin-aligned-actors-targeted-bulgarian-vote-with-eu-interference-claims/>.

⁵⁶ FIMI-ISAC, Assessment of Foreign Information Manipulation and Interference in the 2025 Polish Presidential Election, 2025, sections 2.1.5 and following, <https://www.fimi-isac.org/reports/FDEI-Polish-Election-Country-Report-2025.pdf>; OSCE/ODIHR et al., International Election Observation Mission, Republic of Poland, Presidential Election, Second Round, 1 June 2025: Statement of Preliminary Findings and Conclusions, pp. 1–2 and the notes on NASK data, <https://odihr.osce.org/sites/default/files/f/documents/8/7/591761.pdf>; National Electoral Commission (PKW), "The Election of the President of the Republic of Poland 2025," <https://prezydent2025.pkw.gov.pl/prezydent2025/en>.

Andrej Babiš's ANO won 80 of 200 seats and formed a government with the SPD and the Motorists, with an agenda that moves the country away from its previous support for Ukraine.⁵⁷ The record does not show that these operations produced the result; the change in policy came through a democratic vote.

Bulgaria shows most clearly how Russian operations amplify domestic voices rather than create them. On 19 April 2026 former President Rumen Radev, a critic of EU sanctions against Russia and of military aid to Ukraine, won 44.6 per cent and an absolute majority with his new Progressive Bulgaria. When the caretaker government requested activation of the EU's Rapid Response System for elections, Radev accused it of preparing to "steal" the election on the "Romanian model". According to the DFRLab, his post was taken up within hours by domestic outlets, a Telegram channel associated with the UK-sanctioned Rybar project, InfoDefense and Pravda network sites, and a post by the French politician Florian Philippot reinforced the same narrative. The DFRLab concluded that domestic and external amplification "did not always require coordination to be mutually reinforcing".⁵⁸

Western Europe

France and Germany are the most targeted Member States, and their authorities have gone furthest in public attribution. VIGINUM now counts 205 operations by Storm-1516 since August 2023 and describes the set as attributed to Unit 29155 of the GRU, supported by the Moscow-based Center for Geopolitical Expertise. During the municipal elections of March 2026, it characterised four foreign digital interferences, two conducted through known pro-Russian sets, including a Storm-1516 operation against the Paris mayoral candidate Pierre-Yves Bournazel, which reached only a limited audience. Most of the more than one hundred ".fr" domains registered through CopyCop to imitate local newspapers were suspended by the French registry after identity checks.⁵⁹ In Germany, CORRECTIV, NewsGuard and the Gnida Project identified 102 German-language domains prepared by Storm-1516 before the federal election of February 2025. On 12 December 2025, after a joint analysis by the BfV and the BND, the Federal Government stated that Russia had used Storm-1516 to try to influence the election and to destabilise Germany, named the Center for Geopolitical Expertise and the Double-Headed Eagle movement as the actors behind it, and summoned the Russian ambassador.⁶⁰

Belgium's exposure is shaped by the presence of the EU institutions: in April 2024 the Belgian Prime Minister announced that the intelligence services had confirmed pro-Russian networks seeking to help elect pro-Russian candidates to the European Parliament, and the federal prosecutor opened an investigation. Italy's distinctive feature is the use of overt state channels. In February 2025 the Russian Foreign Ministry's spokeswoman called "blasphemous inventions" a speech in which President Sergio Mattarella compared Russia's aggression against Ukraine with the project of the Third Reich; the attack produced cohesion rather than division, as Prime Minister Giorgia Meloni, the opposition leader Elly Schlein and parties across the spectrum declared their solidarity with the President.⁶¹ Spain's National Security Report for 2025 describes the country as a secondary target of Russian

⁵⁷ Jan Lopatka, "Anonymous TikTok accounts backing radical parties before Czech vote, study finds," Reuters, 28 September 2025, <https://www.reuters.com/business/media-telecom/anonymous-tiktok-accounts-backing-radical-parties-before-czech-vote-study-finds-2025-09-28/>; Aneta Zachová, "TikTok bots push anti-system parties ahead of Czech elections," Euractiv, 2 October 2025, <https://www.euractiv.com/news/tiktok-bots-push-anti-system-parties-ahead-of-czech-elections/>, citing Deník N; Ketrin Johecová and Eliza Gkritsi, "TikTok shuts some accounts over Czech election meddling," Politico Europe, 3 October 2025, <https://www.politico.eu/article/tiktok-shuts-down-some-accounts-meddling-in-czech-elections/>; Krzysztof Dębiec, "Babiš's new government: Czechia first," OSW Centre for Eastern Studies, 18 December 2025, <https://www.osw.waw.pl/en/publikacje/analyses/2025-12-18/babis-new-government-czechia-first>; Karel Janicek, "Czech coalition government led by Andrej Babiš is sworn in," AP News, 15 December 2025, <https://apnews.com/article/czech-republic-new-government-babis-109771312dec01f2e6860eaba7da9c3>.

⁵⁸ Alex Lefkowitz, "Bulgaria's Kremlin-friendly ex-president wins election in landslide," Reuters, 20 April 2026, <https://www.reuters.com/world/europe/bulgarias-kremlin-friendly-ex-president-set-landslide-election-win-2026-04-20/>; Jon Henley, "Moscow-friendly Rumen Radev wins absolute majority in Bulgarian elections," The Guardian, 20 April 2026, <https://www.theguardian.com/world/2026/apr/19/bulgaria-election-rumen-radev-boyko-borissov>; Gelava, "Kremlin-aligned actors."

⁵⁹ VIGINUM, Rapport public sur les élections municipales 2026, SGDSN, June 2026, section 2.2.1, https://www.sgdsn.gouv.fr/files/files/viginum/Publications/20260611_SGDSN_VIGINUM_Rapport-public_Elections-municipales.pdf; Réseau de coordination et de protection des élections, Bulletin d'information no. 6, SGDSN, March 2026, https://www.sgdsn.gouv.fr/files/files/20260305_SGDSN_RCPE_Bulletin%20d%27information%206%20VF.pdf.

⁶⁰ Alexej Hock et al., "Influence operation exposed: How Russia meddles in Germany's election campaign," CORRECTIV, 24 January 2025, <https://correctiv.org/en/fact-checking-en/2025/01/24/disinformation-operation-russian-meddling-in-german-election-campaign-exposed/>; Bundesnachrichtendienst, "Public attribution: Russian Federation is central actor behind Storm-1516 campaign," 12 December 2025, <https://www.bnd.bund.de/EN/Public-Intelligence/joint-disclosure/2025-12-12-attribution-russia-storm-1516-node.html>; Auswärtiges Amt, statements at the government press conference of 12 December 2025, <https://www.auswaertiges-amt.de/de/newsroom/regierungspressekonferenz-2748168>.

⁶¹ Reuters, "Belgium probing alleged Russian interference in EU election campaign," 12 April 2024, <https://www.reuters.com/world/europe/belgium-probing-alleged-russian-interference-eu-election-campaign-2024-04-12/>; Reuters, "Italy president's 'Third Reich' comments on Russia spark Rome-Moscow dispute," 14 February 2025, <https://www.reuters.com/world/europe/italy-presidents-third-reich-comments-russia-spark-row-rome-moscow-row-2025-02-14/>; Cesare Zapperi, "L'attacco di Mosca a Mattarella: «Da lui invenzioni blasfeme sulla Russia»," Corriere della Sera, 14 February 2025, <https://www.corriere.it/politica/25-febbraio-14/attacco-mosca-mattarella-fba49462-f343-4641-bac1-9c61c7744xik.shtml>.

hybrid activity; the Pravda network nonetheless opened a Basque subdomain, and the general election called for 29 November 2026 falls outside the period of this study.⁶²

The Nordic States and Norway

The Nordic States combine high resilience with low priority for Moscow, in the assessment of their own authorities. After Denmark's general election of 24 March 2026, the intelligence and civil protection services reported that they had not uncovered influence activity by foreign intelligence services; profiles linked to Russian online milieus had spread distorted statements about Danish politicians with limited reach, and their posts gained views mainly after Danish media reported on them.⁶³ Before Sweden's election of 13 September 2026, the authorities stated that Sweden was not a priority target;

Table 6. Russian FIMI by regional cluster, January 2025 to October 2026

Cluster	Principal documented operations	Domestic amplification	Response capacity	Distinctive feature
Baltic States	Fabricated security stories around the Estonian and Latvian elections of 2026; impersonation of Euronews and EUobserver	Kremlin-aligned channels favoured some Latvian parties opportunistically; no coordination found	Strong; rapid official denials	Targets security perceptions rather than candidates
Central and Eastern Europe	TikTok networks (Romania 2024, Czech Republic 2025); Doppelganger, Overload and Pravda (Poland 2025); Pravda, InfoDefense (Bulgaria 2026)	Documented cooperation at government level (Hungary 2010–2026); independent alignment elsewhere	Strong attribution (Czech Republic); judicial intervention (Romania)	Annulled election (Romania); changes of government in both directions on Ukraine policy
Western Europe	Storm-1516, CopyCop, Matryoshka (France, Germany); Voice of Europe (Belgium); overt attacks by the Russian Foreign Ministry (Italy)	Mostly independent alignment; documented paid cooperation limited to the Voice of Europe network	Most developed: VIGINUM, German attribution procedure, Belgian prosecution	Highest volume of incidents in the EU
Nordic States	Matryoshka (Sweden 2026); Russian-linked profiles and Greenland disinformation (Denmark 2026)	Limited; cross-party consensus on Ukraine (Sweden)	High; public post-election assessments (Denmark)	Low priority for Moscow; warning against over-attribution (Finland)
Norway (comparator)	Storm-1516 (Nitelva, June 2025)	Not documented	High	Exposure similar to EU neighbours

Source: author's compilation, based on the sources cited in this paper.

Matryoshka nevertheless published seven fabricated videos impersonating SVT, Dagens Nyheter, Euronews and Der Spiegel, much of whose apparent reach was inauthentic, and X removed them only after nearly a week. All parties in the Riksdag support Sweden's backing for Ukraine, which leaves Moscow little to exploit.⁶⁴ Finland's Security and Intelligence Service adds a caution: because events are readily attributed to Russia, Russian

⁶² Departamento de Seguridad Nacional, Informe Anual de Seguridad Nacional 2025, Madrid, approved by the National Security Council on 21 April 2026, chapter "Tensión estratégica y regional", <https://www.dsn.gob.es/sites/default/files/2026-05/Informe%20Anual%20de%20Seguridad%20Nacional%202025%20-%20Accesible.pdf>; EEAS, 4th Report, section on information manipulation sets (Portal Kombati); La Moncloa, "Pedro Sánchez announces the calling of general elections for November 29th," 5 October 2026, <https://www.lamoncloa.gob.es/lang/en/presidente/news/paginas/2026/20261005-institutional-statement.aspx>.

⁶³ Styrelsen for Samfundssikkerhed, "Myndighederne har ikke afdækket fremmed statslig påvirkningsaktivitet i forbindelse med folketingsvalget 2026," 25 March 2026, <https://samsik.dk/artikler/2026/03/myndighederne-har-ikke-afdaekket-fremmed-statslig-paavirkningsaktivitet-i-forbindelse-med-folketingsvalget-2026/>. The assessment was issued jointly by the Danish Defence Intelligence Service (FE), the Danish Security and Intelligence Service (PET) and the Agency for Civil Protection (SAMSIK).

⁶⁴ Pavlovičová, "Swedish election"; Linus Svensson, Henrik Sköld and Ellika Nilsson, "Proryskt trollnätverk riktar in sig på svenska valet," SVT Nyheter, 19 August 2026, <https://www.svt.se/nyheter/inrikes/proryskt-trollnatverk-riktar-in-sig-pa-svenska-valet>; Alliance4Europe, "Illegal Russian Influence Operation Continues to Go Unimpeded on X: Matryoshka Targeting the Swedish Elections," SocialMediaTransparency.org, 26 August 2026, <https://socialmediatransparency.org/research/alliance4europe-matryoshka-swedish-elections-2026>.

influence may appear more extensive than it is, and such interpretations increase Russian deterrence. Almost all drone sightings investigated in Finland were caused by other flight operations.⁶⁵

Norway, a NATO member outside the EU, offers a point of comparison. What researchers described as the first known Storm-1516 operation against it, in June 2025, used a fake environmental organisation to claim that heavy-water pollution had caused mass deaths of wildlife in the Nitelva river near Oslo and might force the cancellation of the UN Internet Governance Forum, which Norway hosted that month after Russia had sought the role. A specialist at the Norwegian Defence Research Establishment said the operation fitted Storm-1516's methods but that its authorship could not be established with certainty.⁶⁶ The sets examined here operate across the Union's external border regardless of membership; what membership changes is the response, not the exposure.

VIII. Comparative Analysis: The EU and the Eastern Neighbourhood

Shared Architecture

The same information manipulation sets operate in both theatres. Storm-1516, which targeted the German federal election in 2025 and the French municipal elections in 2026, was also active against Moldova and then Armenia, where its activity began in April 2025, more than a year before the June 2026 election. Operation Overload worked in parallel in both theatres, and the Pravda network serves all of them. The High Representative put it directly: the playbook deployed in Moldova in 2025 was being redeployed in Armenia in 2026, and elections in Member States could face similar patterns.⁶⁷ Russia does not keep separate toolkits for members and non-members. It keeps one toolkit and adjusts the mix to the environment.

Divergent Laundering Models

The theatres diverge in the route by which a narrative enters the domestic debate. In the neighbourhood, narratives arrive through Russian media that still have large audiences, through oligarchic networks able to buy votes as well as attention, and, in Georgia, through a governing party that repeats Kremlin narratives. In Moldova in 2025, international observers reported that the authorities and investigative journalists had credibly identified an organised network, funded from Russia and linked to Ilan Shor, which coordinated vote buying alongside disinformation.⁶⁸ Inside the EU none of these routes is fully open: state media are banned from broadcasting, vote buying on that scale would face criminal investigation, and among Member State governments only Hungary's is documented as having cooperated with Moscow. Russian operations therefore depend on domestic voices that already say what Moscow wants said, as in Bulgaria, where the narrative began with a domestic candidate and a French politician and Russian networks amplified it. The flow runs from domestic politics outwards and back again, rather than from Moscow inwards.

Georgia and Hungary: Two Governments, Two Outcomes

Georgia since 2012 and Hungary between 2010 and 2026 offer the most instructive comparison. Both governments repeated narratives convenient to Moscow, both weakened checks on their own power, and V-Dem classified both as electoral autocracies on its 2025 data. Georgia's elections of October 2024, which official results gave to Georgian Dream with almost 54 per cent, were marred, according to international observers, by an uneven playing field, widespread pressure on voters and frequent breaches of ballot secrecy; a month later the government suspended EU accession talks until 2028.⁶⁹ In Hungary, the government lost the election of 12

⁶⁵ Finnish Security and Intelligence Service (Supo), "Overview of state espionage and influencing," National Security Overview 2026, <https://supo.fi/en/overview-of-state-espionage-and-influencing-2026>; Supo, "Russian superpower ambitions will remain also after the war," 10 March 2026, <https://supo.fi/en/-/russian-superpower-ambitions-will-remain-also-after-the-war>.

⁶⁶ Tharald Halvorsen, "«Kan nå drikkevannet»," Dagbladet, 31 July 2025, <https://www.dagbladet.no/nyheter/kan-na-drikkevannet/83389869>, quoting Eskil Grendahl Sivertsen of the Norwegian Defence Research Establishment (FFI) and analysts of the Gnida Project; Daryna Antoniuk, "Russia-linked group spoofing European journalists to spread disinformation," The Record, 14 July 2025, <https://therecord.media/russia-group-spoofing-journalists-disinfo>.

⁶⁷ EEAS, 4th Report, pp. 2, 5 and 33; Sjøstedt et al., "Uncovering the digital infrastructure"; VIGINUM, Élections municipales 2026, section 2.2.1.

⁶⁸ Robakidze, "Russian FIMI Operations," Sections III and VI; OSCE/ODIHR et al., Election Observation Mission, Republic of Moldova, Parliamentary Elections, 28 September 2025: Statement of Preliminary Findings and Conclusions, pp. 1–2 and section on the campaign, <https://www.oscepa.org/en/documents/election-observation/election-observation-statements/moldova/statements-16/5347-2025-parliamentary-eng/file>.

⁶⁹ OSCE/ODIHR, "Georgia's elections marred by an uneven playing field, pressure and tension, but voters were offered a wide choice: international observers," 27 October 2024, <https://odihr.osce.org/odihr/elections/georgia/579376>; Al Jazeera, "Georgia to suspend EU accession talks until 2028," 28 November 2024, <https://www.aljazeera.com/news/2024/11/28/georgia-to-suspend-eu-accession-talks-until-2028>; V-Dem Institute, Democracy Report

April 2026 to Péter Magyar's Tisza, which won 53.2 per cent of the list vote and 141 of 199 seats, and Orbán conceded quickly.⁷⁰

Four factors may account for the difference: electoral integrity, since Hungary's process, whatever its imbalances, still allowed a large shift in votes to change the government; media pluralism, constrained in both countries; opposition unity, since the Hungarian opposition vote concentrated largely on a single party, whereas Georgian voters in 2024 were offered 18 candidate lists; and external leverage, since membership exposed Hungary to the Union's legal instruments, including the suspension of €6.3 billion in budget commitments under the rule-of-law conditionality mechanism in December 2022, while the EU's leverage over Georgia depended on an accession process that the government could simply suspend.⁷¹ Two cases cannot establish the relative weight of these factors, which remains an open question. The comparison does show that the rule of law that protects a government aligned with Moscow also preserves the means of removing it.

The 2024–2026 Election Cycle

Table 7 summarises the electoral cycle in both theatres. Russian operations accompanied almost every election, but their documented scale varied with Moscow's priorities and the target's resilience. Outcomes did not follow the intensity of operations: the most heavily targeted electorates in the neighbourhood, Moldova in 2025 and Armenia in 2026, returned pro-European majorities, and the Hungarian government that had cooperated with Moscow lost power. Where governments more sceptical of support for Ukraine came to power, in the Czech Republic and Bulgaria, they did so with their own electoral strength and on agendas in which domestic issues featured prominently. Some of the heaviest Russian pressure was not online at all: in Armenia, observers recorded trade restrictions and security threats by Russian officials aimed at influencing voters.⁷²

Table 7. Selected elections, October 2024 to October 2026

Election	Documented Russian activity	Response	Outcome
Georgia, parliamentary, 26 Oct 2024	Kremlin narratives repeated by the governing party (first study)	Observers: uneven playing field, pressure on voters	Georgian Dream almost 54% (official); EU accession talks suspended
Romania, presidential, Nov 2024 to May 2025	Coordinated TikTok campaign (some 25,000 accounts, per declassified intelligence)	First round annulled, 6 Dec 2024; evidence contested	Nicușor Dan 53.6% in the rerun
Germany, federal, 23 Feb 2025	Storm-1516 (102 prepared domains)	National attribution and ambassador summoned, Dec 2025	CDU/CSU first with 28.5%
Poland, presidential, May–Jun 2025	Doppelganger, Overload, Pravda; both candidates attacked	14,890 inauthentic accounts reported by NASK	Karol Nawrocki 50.89%

2026: Unraveling the Democratic Era?, University of Gothenburg, March 2026, https://v-dem.net/documents/75/V-Dem_Institute_Democracy_Report_2026_lowres.pdf.

⁷⁰ Nemzeti Választási Iroda, "Országgyűlési képviselők választása 2026," <https://vtr.valasztas.hu/ogy2026>; Gergely Szakacs, "Magyar's parliamentary majority in Hungary increases after final count," Reuters, 18 April 2026, <https://www.reuters.com/world/magyars-parliamentary-majority-hungary-increases-after-final-count-2026-04-18/>.

⁷¹ Council of the European Union, "Rule of law conditionality mechanism: Council decides to suspend €6.3 billion given only partial remedial action by Hungary," press release, 12 December 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/12/12/rule-of-law-conditionality-mechanism/>; Nemzeti Választási Iroda, "Országgyűlési képviselők választása 2026"; OSCE/ODIHR, "Georgia's elections marred."

⁷² Results from Centrālā vēlēšanu komisija; Nemzeti Választási Iroda; National Electoral Commission (Poland); Die Bundeswahlleiterin, "Bundestagswahl 2025: Endgültiges Ergebnis," 14 March 2025, https://www.bundeswahlleiterin.de/info/presse/mitteilungen/bundestagswahl-2025/29_25_endgueltiges-ergebnis.html; Moldpres, "CEC approved final results of 28 September parliamentary elections," 5 October 2025, <https://www.moldpres.md/eng/politics/cec-approved-final-results-of-28-september-parliamentary-elections>; Lucy Papachristou, "Armenia's Pashinyan wins election, observers allege Russian interference," Reuters, 7 June 2026 (updated 10 June 2026), <https://www.reuters.com/world/armenias-ruling-party-leads-parliamentary-vote-with-57-early-results-2026-06-07/>; Helen Levy, "Mette Frederiksen takes the lead, but with no majority," Fondation Robert Schuman, European Elections Monitor, March 2026, <https://server.www.robert-schuman.eu/storage/en/doc/oe/oe-6772-en.pdf>; Sveriges riksdag, "The 2026 elections," <https://www.riksdagen.se/en/news/the-2026-elections/>. On the domestic agendas of the Czech and Bulgarian winners: Jan Lopatka and Jason Hovet, "Czech vote winner Babis signs coalition deal with eurosceptic partners," Reuters, 3 November 2025, <https://www.reuters.com/world/czech-election-winner-babis-signs-coalition-deal-with-partners-2025-11-03/>; Lefkowitz, "Bulgaria's Kremlin-friendly ex-president"; Alexandar Detev, "What course will Bulgaria's new leader Rumen Radev take?," DW, 21 April 2026, <https://www.dw.com/en/what-course-will-bulgarias-new-leader-rumen-radev-take/a-76879858>. On Armenia: OSCE/ODIHR et al., International Election Observation Mission, Armenia, Parliamentary Elections, 7 June 2026: Statement of Preliminary Findings and Conclusions, <https://www.oscepa.org/en/documents/election-observation/election-observation-statements/armenia/statements-2/5525-2026-parliamentary-1>.

Election	Documented Russian activity	Response	Outcome
Moldova, parliamentary, 28 Sep 2025	Storm-1516, Overload; Russian-funded vote-buying network	844 searches, 122 detentions	PAS 50.2% and a majority
Czech Republic, parliamentary, 3–4 Oct 2025	Network of 286 TikTok accounts	Referral by intelligence; removals by TikTok	ANO 80 of 200 seats; Babiš coalition
Denmark, general, 24 Mar 2026	Russian-linked profiles; Greenland disinformation; DDoS	No foreign intelligence influence activity uncovered	Social Democrats first with 21.9%
Hungary, parliamentary, 12 Apr 2026	At least two Russian-linked operations; leaked Szijjártó–Lavrov calls	Exposure by investigative consortium	Tisza 53.2%, 141 of 199 seats
Bulgaria, parliamentary, 19 Apr 2026	Pravda, InfoDefense, Node of Time; “Romanian scenario” narrative	EU Rapid Response System activated	Progressive Bulgaria 44.6%, absolute majority
Armenia, parliamentary, 7 Jun 2026	Storm-1516 from April 2025; trade restrictions and threats	Observers recorded direct foreign pressure	Civil Contract 49.8% and a majority
Sweden, general, 13 Sep 2026	Matryoshka (seven fabricated videos)	Removal by X after nearly a week	Opposition bloc 176 of 349 seats
Latvia, parliamentary, 3 Oct 2026	Fabricated NATO-deaths video, audience above 1.85 million	Denial by the National Armed Forces	United List 35.3%, 41 of 100 seats

Source: author’s compilation from official results and the sources cited in this paper. Eastern neighbourhood and EU elections are listed together in chronological order.

Capacity to Respond

The sharpest asymmetry lies in the capacity to respond. Inside the EU, the state is normally the defender: France and Germany attribute operations publicly, Czech and Danish authorities publish their findings, and the Council extended its regime against Russia’s hybrid activities until October 2027. In the neighbourhood, capacity depends on the government’s orientation. Moldova shows what a determined state with EU support can achieve: law-enforcement action against the vote-buying network in 2025 led to 844 searches and 122 detentions, and observers judged that it had a mitigating and deterrent effect. In Georgia the state itself performs the laundering function, and legislation presented as protection against foreign influence has drawn international concern for stigmatising civil society organisations and independent media.⁷³ Hungary stood between the two. The variable that matters most is not membership as such but whether the state’s institutions are on the side of defence. Table 8 summarises the comparison.

Table 8. Russian FIMI in the eastern neighbourhood and in EU Member States: summary comparison

Dimension	Eastern neighbourhood (first study)	EU Member States (present study)
Strategic aim	Prevent or reverse integration with the EU and NATO	Erode support for Ukraine and sanctions; weaken the cohesion of the Union
Principal channels	Russian media, Telegram, oligarch-owned outlets	Impersonated media, fake news sites, X and Telegram, commercial amplification
Laundering model	Injection through openly Russian sources, then local validators; governing party in Georgia	Disguised from the start; domestic voices amplified
Domestic proxies	Oligarchic networks; vote buying (Moldova)	Few cases of documented cooperation (Voice of Europe, Hungary); wide field of independent alignment

⁷³ Council of the European Union, “Russia’s hybrid activities”; Bundesnachrichtendienst, “Public attribution”; Réseau de coordination et de protection des élections, Bulletin d’information no. 6; Styrelsen for Samfundssikkerhed, “Myndighederne har ikke afdækket”; Alliance4Europe, “Illegal Russian Influence Operation”; OSCE/ODIHR et al., statement on Moldova, 28 September 2025; OSCE/ODIHR et al., International Election Observation Mission, Georgia, Parliamentary Elections, 26 October 2024: Statement of Preliminary Findings and Conclusions, <https://odihr.osce.org/sites/default/files/f/documents/3/0/579346.pdf>; Robakidze, “Russian FIMI Operations,” Section VI (Georgia).

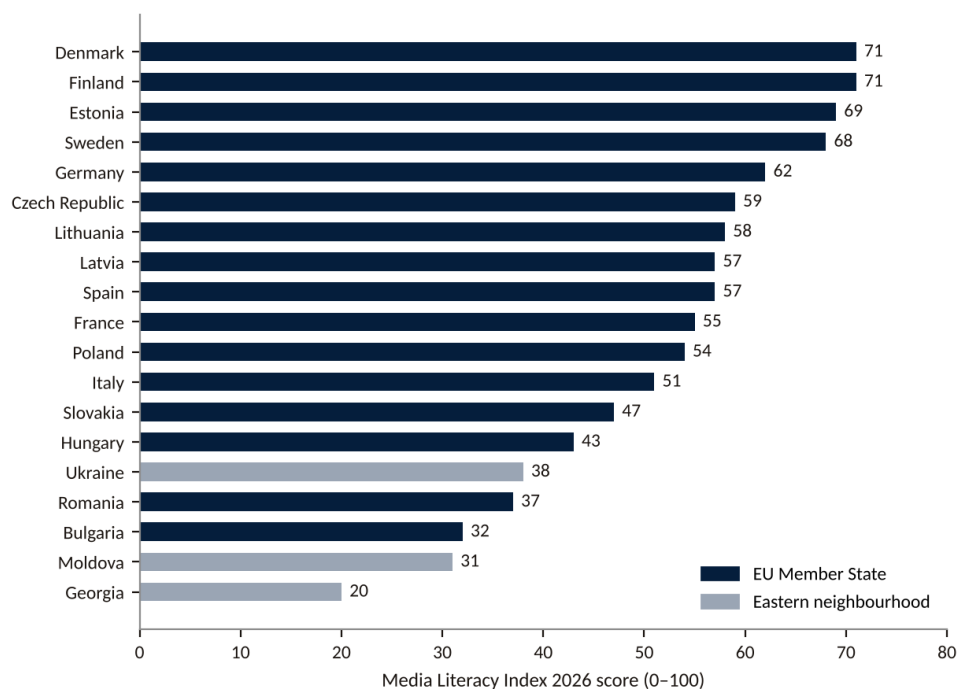
Dimension	Eastern neighbourhood (first study)	EU Member States (present study)
Role of the state	Defender (Moldova, Armenia) or laundering node (Georgia)	Normally defender; Hungary 2010–2026 the main exception
Non-informational pressure	Trade restrictions, security threats, vote buying	Hybrid actions below the threshold of armed attack: drones, sabotage, DDoS
Response capacity	Dependent on the government's orientation and on external support	Attribution, sanctions and platform regulation; uneven across Member States
Observable effect	Contributed to state capture in Georgia; contained in Moldova and Armenia	Limited documented effect on electoral outcomes; cumulative effect on trust uncertain

Source: author's compilation, based on the first study and the sources cited in this paper.

IX. Why Russian FIMI Works Inside the EU, and Where It Fails

Documenting an operation is easier than demonstrating its effect. The most rigorous study of exposure to a Russian campaign, which linked survey data to the Twitter feeds of American users in 2016, found exposure heavily concentrated, with 1 per cent of users accounting for 70 per cent of exposures, and no meaningful relationship between exposure and changes in attitudes, polarisation or voting. European survey research finds that neutral and pro-Kremlin attitudes towards the war are linked most strongly to the positions of the parties respondents support, followed by disinformation and ideology. Party cues matter more than foreign content. Yet belief in disinformation can still move votes at the margin: a panel study of the 2017 German election found that it drew voters from the main governing party towards the AfD, and that the less people trusted media and politics, the more they believed it. Experiments with pro-Russian astroturfing comments show that they can alter opinions even among people warned in advance.⁷⁴

Figure 2. Resilience to disinformation: Media Literacy Index 2026, selected countries



Source: Open Society Institute – Sofia, *Media Literacy Index 2026, January 2026*. Scores range from 0 to 100; higher scores indicate greater resilience. Armenia is not covered by the index.

⁷⁴ Gregory Eady et al., “Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior,” *Nature Communications* 14, 62 (2023), <https://doi.org/10.1038/s41467-022-35576-9>; Kostelka et al., “Mass attitudes”; Fabian Zimmermann and Matthias Kohring, “Mistrust, Disinforming News, and Vote Choice: A Panel Survey on the Origins and Consequences of Believing Disinformation in the 2017 German Parliamentary Election,” *Political Communication* (2020): 215–237, <https://doi.org/10.1080/10584609.2019.1686095>; Thomas Zerback, Florian Töpfl and Maria Knöpfle, “The disconcerting potential of online disinformation: Persuasive effects of astroturfing comments and three strategies for inoculation against them,” *New Media & Society*, published online 4 March 2020, <https://doi.org/10.1177/1461444820908530>.

Susceptibility also varies between societies. The Central European Digital Media Observatory found Polish society largely immune to Russian narratives about the war, Slovak society relatively receptive and Czech society in between. The Media Literacy Index, which combines press freedom, education, interpersonal trust and e-participation, shows a similar gradient (Figure 2): the Nordic and Baltic Member States lead, Bulgaria ranks last in the EU, and Moldova and Georgia rank 35th and 38th of 41 countries.⁷⁵ The index measures resilience, not exposure or effect, but its pattern is consistent with the limited reach reported by the Nordic authorities.

On this evidence, Russian FIMI gains traction inside the EU under four conditions: when it attaches itself to existing domestic voices and grievances, as in Bulgaria; when trust in media and institutions is low; when the state itself becomes a channel, as in Hungary until 2026; and when it exhausts the capacity of newsrooms to verify, which is what operations such as Matryoshka attempt by sending fabricated content to journalists disguised as requests for verification.⁷⁶ It fails where fabricated content has no domestic carriers: the EEAS found the AI-generated videos of Storm-1516 and Operation Overload easily identifiable and of limited engagement, and the operation against the Paris candidate Bournazel drew fewer than 20,000 views, against some 100,000 for a typical Storm-1516 operation. It fails where overt pressure provokes cohesion, as in Italy, and where institutions hold: in Romania the courts annulled the round that operations were alleged to have distorted, and Hungarian voters removed the government that had cooperated with Moscow.⁷⁷ Table 9 summarises these conditions in both theatres.

Table 9. Conditions under which Russian FIMI gains or loses traction

Condition	Effect on FIMI	EU Member States	Eastern neighbourhood (first study)
Existing domestic voices and grievances	Gains	Bulgaria 2026; narratives on sanctions and energy prices	Governing party repeating Kremlin narratives (Georgia)
Low trust in media and institutions	Gains	German panel evidence; low Media Literacy Index scores in Bulgaria and Romania	Georgia and Moldova near the bottom of the Media Literacy Index
State acting as a channel	Gains	Hungary 2010–2026	Georgia since 2012
Overloading of verification capacity	Gains indirectly	Matryoshka targeting newsrooms (France, Sweden)	Not examined in the first study
Fabricated content without domestic carriers	Fails	Low genuine engagement (France, Sweden)	Low engagement of AI-generated videos reported by the EEAS
Overt pressure by Russian officials	Fails or backfires	Cohesion after the attack on President Mattarella (Italy)	Pro-European majority in Armenia despite trade restrictions and threats
Resilient institutions and political consensus	Fails	Denmark, Sweden, Finland; Czech TikTok operation	Law-enforcement response in Moldova, 2025

Source: author's compilation, based on the first study and the sources cited in this paper.

Over-Attribution: The Yandex Episode

Over-attribution is the mirror image of under-detection, and it has its own costs. Between 7 and 11 October 2026, Ukrainian drones struck three Yandex data centres in Sasovo, Kaluga and Vladimir; Yandex confirmed that two had been shut down and part of the third put out of service. Within a day of the third strike, posts on X claimed that Russian-run accounts had fallen silent in communities around the AfD, the MAGA movement and Reform UK, and President Zelenskyy said there was “less hate, less division and fewer provocations” online

⁷⁵ Michał Wenzel et al., “The penetration of Russian disinformation related to the war in Ukraine: Evidence from Poland, the Czech Republic and Slovakia,” *International Political Science Review*, published online 16 November 2023, <https://doi.org/10.1177/01925121231205259>; Open Society Institute – Sofia, *Media Literacy Index 2026*, Sofia, January 2026, <https://osis.bg/wp-content/uploads/2026/01/Media-Literacy-Index-2026.pdf>. Armenia is not covered by the index.

⁷⁶ Svensson, Sköld and Nilsson, “Proryskt trollnätverk,” citing VIGINUM; Gelava, “Kremlin-aligned actors”; Zimmermann and Kohring, “Mistrust, Disinforming News.”

⁷⁷ EEAS, 4th Report, section on the use of artificial intelligence; RFI, “France accuses Russia of election interference using fake website,” 6 March 2026, <https://www.rfi.fr/en/france/20260306-france-accuses-russia-of-election-interference-using-fake-website-bournazel>; Reuters, “‘Third Reich’ comments”; Calus, “Constitutional Court annuls”; Szakacs, “Magyar’s parliamentary majority.”

because of “fewer bots”.⁷⁸ The claim rested on a chart from Cloudflare Radar showing a collapse in automated traffic from Yandex’s network, traffic consisting mainly of Yandex’s own search crawler rather than social media accounts. Graphika found no notable decline in the communities named, and researchers at dTeam told BBC Verify that accounts linked to Storm-1516 and Matryoshka were still active; Zelenskyy’s office later said he had been referring to the “atmosphere” on social media.⁷⁹ The available evidence cannot establish whether the strikes affected Russian operations. It does show how a real event and an authentic chart became evidence for a claim the chart could not support. Attributing domestic Euroscepticism to foreign bots is comforting, because it implies that removing the bots removes the problem; the research reviewed here suggests otherwise.

X. Evidentiary Uncertainty

The findings rest on evidence of uneven quality, and four limits should be stated plainly. First, confidence in attribution varies. Some attributions rest on formal government procedures, such as the German national attribution of Storm-1516 or VIGINUM’s reports, which state their level of confidence; others on researchers and journalists without access to intelligence; and the EEAS itself left 65 per cent of the incidents it recorded in 2025 unattributed.⁸⁰ This paper reports each attribution at the confidence level used by the attributing body and does not rely on a single unnamed source for any classification.

Second, effect is far harder to measure than activity. Different bot-detection methods applied to the same political discourse produce widely divergent estimates, platforms restrict researchers’ access to data, and measured reach is itself inflated by inauthentic amplification.⁸¹ Figures for views and audiences therefore indicate potential exposure, not persuasion. Third, characterisations of governments and parties are contested and may change: the Romanian annulment was criticised as resting on vague evidence, and the financial ties of a Latvian party leader to Russia are still under assessment. Every classification in this paper is provisional. Fourth, much of the evidence for 2025 and 2026 comes from official reports, research organisations and journalism rather than peer-reviewed research, which lags events by several years. These limits define the form of the central argument: the weight of current evidence suggests that Russian FIMI inside the EU primarily amplifies; it does not prove that it never creates.

XI. Policy Implications

If Russian FIMI inside the EU primarily amplifies, the priority is not to suppress domestic opinion, which would be both wrong and self-defeating, but to raise the cost of amplification, protect the institutions that detect it and keep the threat in proportion. The European Democracy Shield, presented on 12 November 2025, provides the framework. Its centrepiece, the European Centre for Democratic Resilience, began work on 24 February 2026 with all Member States participating, and on 13 October 2026 ministers endorsed the association of Albania, Bosnia and Herzegovina, Moldova, Montenegro, North Macedonia, Serbia, Ukraine and Kosovo.⁸² Seven implications follow (Table 10).

Target the supply chain. Deterrence should reach the commercial layer on which operations depend, as the EEAS now proposes. The French registry’s suspension of most CopyCop domains after identity checks shows what can

⁷⁸ Yandex, “What is happening to our data centers, the iron heart of Yandex,” company news, 9 October 2026, <https://www.yandex.com/company/news/2026-10-09>; Al Jazeera, “Russia’s Yandex says data centre in Vladimir shut down after drone attack,” 11 October 2026, <https://www.aljazeera.com/news/2026/10/11/russias-yandex-says-data-centre-in-vladimir-shut-down-after-drone-attack>; John Kelly, “Did the Yandex Data Center Strikes Silence Russian Bots? What the Data Shows,” Graphika, 13 October 2026, <https://www.graphika.com/blogs/yandex-strikes-russian-influence-operations>; Richard Irvine-Brown, “Is Zelensky right to say data centre strikes have taken down Russian bots?,” BBC News (BBC Verify), 13 October 2026, <https://www.bbc.com/news/articles/c9y7l0pm8jikko>.

⁷⁹ Kelly, “Yandex Data Center Strikes”; Renée DiResta, “The Russian Bots Went Silent. Or Did They?,” Lawfare, 14 October 2026, <https://www.lawfaremedia.org/article/the-russian-bots-went-silent-or-did-they>; Irvine-Brown, “Is Zelensky right?”

⁸⁰ EEAS, 4th Report, section “2025 FIMI in numbers”; Bundesnachrichtendienst, “Public attribution”; VIGINUM, Élections municipales 2026.

⁸¹ Franziska Martini et al., “Bot, or not? Comparing three methods for detecting social bots in five political discourses,” Big Data & Society (2021), <https://doi.org/10.1177/20539517211033566>; Marco Bastos and Dan Mercea, “The public accountability of social platforms: lessons from a study on bots and trolls in the Brexit campaign,” Philosophical Transactions of the Royal Society A 376 (2018), <https://doi.org/10.1098/rsta.2018.0003>; DiResta, “Russian Bots Went Silent”; Cesarini, “Four General Elections”; Alliance4Europe, “Illegal Russian Influence Operation.”

⁸² European Commission and High Representative, European Democracy Shield: Empowering Strong and Resilient Democracies, JOIN(2025) 791 final, Brussels, 12 November 2025, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025JC0791>; European Commission, “The new European Centre for Democratic Resilience starts its work,” 24 February 2026, https://enlargement.ec.europa.eu/news/new-european-centre-democratic-resilience-starts-its-work-2026-02-24_en; European Commission, “The European Centre for Democratic Resilience opens cooperation to candidate countries and potential candidates,” 13 October 2026, https://commission.europa.eu/news-and-media/news/european-centre-democratic-resilience-opens-cooperation-candidate-countries-and-potential-candidates-2026-10-13_en.

be achieved at modest cost; the NIS2 Directive already requires registries and registrars to verify registration data, and consistent application would make pre-positioned networks costlier to build. The EU's regime against Russia's destabilising activities should also be used against commercial providers of engagement that knowingly serve Russian operations.⁸³

Protect counter-FIMI capacity. The institutions that detect and attribute operations need protection from political pressure, including pressure from their own governments; Hungary showed how long a government can cooperate with Moscow while remaining in office. In September 2026 the European Parliament called for the European Centre for Democratic Resilience to receive a legal mandate and a dedicated budget, which would allow it to maintain situational awareness where national capacity has been weakened.⁸⁴

Attribute with stated confidence. Public attribution should state its confidence and its limits and keep the three degrees of involvement apart. The German attribution procedure, VIGINUM's reports and the post-election assessments of the Danish and Latvian authorities offer models: they name operations when the evidence allows, say when it does not, and do not treat parties or voters as agents of Moscow. The EU Blueprint for countering FIMI proposed in the Democracy Shield could set common standards.⁸⁵

Secure data access and enforcement. The DSA rules on access to platform data for vetted researchers have applied since 29 October 2025, and the Commission's first DSA non-compliance decision, against X, concerned among other things the obstruction of researchers. The DSA incidents and crisis protocol foreseen in the Democracy Shield should be in place before the French presidential election of 2027, which Russian operations have already begun to target. Telegram remains the largest regulatory gap.⁸⁶

Support verification without exhausting it. The European Network of Fact-Checkers proposed in the Democracy Shield, with its shared repository, could serve as a clearing house, so that a fabricated story sent to dozens of newsrooms is verified once and the result shared with all.⁸⁷

Keep the threat in proportion. Over-attribution inflates Russia's reach and distracts from the domestic sources of the grievances it amplifies. The more durable protection lies in education, media freedom and trust, the components of the Media Literacy Index. These fall largely within national competence, but the Democracy Shield's media resilience programme and its support for citizenship and digital skills in schools point in the right direction.⁸⁸

Extend the instruments to the neighbourhood. Moldova shows what determined institutions with EU support can achieve, and its association with the Centre is a step forward. Georgia and Armenia are not among the partners endorsed in October 2026.⁸⁹ Armenia, which is not a candidate country, would require a different format of cooperation. In Georgia, where the state itself performs the laundering function, support should go to independent media, civil society and researchers rather than to state institutions.

⁸³ EEAS, 4th Report, chapter on deterrence; VIGINUM, Élections municipales 2026, section 2.2.1; Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive), Article 28(3), <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>; Council of the European Union, "Russia's hybrid activities"; Delorme, "Criminal Economy."

⁸⁴ European Parliament, Legislative Train Schedule, "European Democracy Shield," on the report of the Special Committee on the European Democracy Shield adopted in plenary on 15 September 2026, <https://www.europarl.europa.eu/legislative-train/package-european-democracy-action-plan/file-european-democracy-shield>.

⁸⁵ Bundesnachrichtendienst, "Public attribution"; VIGINUM, Élections municipales 2026; Styrelsen for Samfundssikkerhed, "Myndighederne har ikke afdækket"; Valsts drošības dienests, "15. Saeimas vēlēšanas"; European Commission and High Representative, European Democracy Shield, section on safeguarding the integrity of the information space.

⁸⁶ Commission Delegated Regulation (EU) 2025/2050 of 1 July 2025 on the technical conditions and procedures for sharing data with vetted researchers under the Digital Services Act, applicable since 29 October 2025, <https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act-sharing-platform-and-search-engine-data-with-vetted-researchers.html>; Pingen, "EU Fines X"; European Commission and High Representative, European Democracy Shield, section on safeguarding the integrity of the information space; Chatelard, "Fake Newsroom."

⁸⁷ European Commission and High Representative, European Democracy Shield, section on the European Network of Fact-Checkers; Svensson, Sköld and Nilsson, "Proryskt trollnätverk," citing VIGINUM.

⁸⁸ Supo, "Russian superpower ambitions"; Open Society Institute – Sofia, Media Literacy Index 2026; European Commission and High Representative, European Democracy Shield, section on boosting societal resilience.

⁸⁹ European Commission, "Democratic Resilience opens cooperation"; OSCE/ODIHR et al., statement on Moldova, 28 September 2025.

Table 10. Findings, policy implications and relevant EU instruments

Finding of this paper	Policy implication	Relevant EU instrument
Operations depend increasingly on commercial services and pre-registered infrastructure	Target the supply chain	Sanctions regime against Russia's destabilising activities; NIS2 rules on domain registration data
Counter-FIMI capacity can be weakened by national governments	Protect detection and attribution capacity	European Centre for Democratic Resilience, with a legal mandate and budget as requested by Parliament
Domestic voices are amplified; most involvement is independent alignment	Attribute with stated confidence; keep the three degrees of involvement apart	Proposed EU Blueprint for countering FIMI and disinformation; national attribution procedures
Effects are hard to measure; platform data are restricted	Secure data access and enforcement	DSA data-access rules (Delegated Regulation 2025/2050); proposed DSA incidents and crisis protocol
Operations target verification capacity	Support verification without exhausting it	Proposed European Network of Fact-Checkers; EDMO
Over-attribution inflates Russia's reach	Keep the threat in proportion; invest in long-term resilience	Democracy Shield media resilience programme and skills support
The neighbourhood remains more exposed, and Georgia's state is part of the problem	Extend instruments beyond the Union	Association with the Centre (Moldova, Ukraine); support for independent media and civil society

Source: author's compilation, based on the findings of this paper and the instruments cited in this section.

XII. Conclusion

EU membership changes the form of Russian FIMI more than the fact of it. The same information manipulation sets operate on both sides of the Union's eastern border, with the same operational grammar. What membership changes is the environment the operations meet: laundering must be disguised from the outset, vote buying on the Moldovan scale would face criminal investigation, and the state is normally on the side of defence.

The democratic legitimacy paradox runs through the findings. Elected actors who repeat narratives convenient to Moscow are protected by the norms that membership upholds, and in Hungary a government that cooperated with Moscow remained in office for sixteen years. The same norms preserved the means of removing it, which is the decisive difference from Georgia. The electoral cycle of 2024 to 2026 shows the limits of FIMI's effect: outcomes did not follow the intensity of operations, and where governments more sceptical of support for Ukraine came to power, they did so on their own electoral strength. The weight of current evidence therefore supports the central argument: inside the EU, Russian influence operations primarily amplify existing domestic political alignments rather than manufacture them.

That is no reason for complacency. Amplification matters where trust is low, and the operations examined here are cheap, persistent and increasingly outsourced. Finland's security service expects Russian intelligence and influence resources now tied to the war in Ukraine to become available elsewhere once it ends.⁹⁰ The French presidential election of 2027 and the period after any ceasefire will test the instruments now being built. The task is to raise the cost of amplification, protect the institutions that expose it and invest in the trust that limits its effect, without mistaking Europe's own political disagreements for the work of a foreign adversary.



Dr George Robakidze

George Robakidze is a diplomat and policy expert specialising in international politics, security, and European integration. He has held senior roles in Georgia's Ministry of Foreign Affairs, focusing on political affairs, Euro-Atlantic integration, and regional security.

He holds a PhD in Political Science. His research focuses on radical and populist movements in Eastern Europe, alongside broader political and international issues.

⁹⁰ Supo, "Russian superpower ambitions."