Ballots Under Pressure:

Russian Information Manipulation in 2025 Elections in Georgia and Moldova

Co-funded by the European Union

G | M | F Transatlantic Foundation

PROELECT
PROMOTING ACCOUNTABILITY IN ELECTORAL PROCESSES

erim Equal Rights & Independent Media

Institute of Innovative Governance

Authors:
Anna Mysyshyn, Director and Co-Founder of the Institute of Innovative Governance
Andrea Castagna, Senior Analyst, the Institute of Innovative Governance
Anna Melenchuk, Co-Founder of the Institute of Innovative Governance, Programme Manager

Ballots Under Pressure:

Russian Information Manipulation in 2025 Elections in Georgia and Moldova

This publication was produced with the financial support of the European Union and the German Marshall Fund of the United States - Transatlantic Foundation (GMF TF). Its contents are the sole responsibility of the Institute of Innovative Governance and do not necessarily reflect the views of the European Union and or the GMF TF.

Contents:

Part I
Introduction

Foreign Information Manipulation and Interference (FIMI) has emerged as one of the most persistent and adaptive tools of authoritarian influence in democratic societies. In Eastern Europe and the South Caucasus, the Russian Federation has systematically employed disinformation, propaganda, and covert influence operations to undermine trust in democratic institutions, polarize societies, and distort electoral processes. Elections, particularly in countries with contested geopolitical trajectories represent critical moments when such interference is most intense and consequential.

The 2025 municipal elections in Georgia and 2025 parliamentary elections in Moldova constituted pivotal democratic milestones for both countries. These elections not only shaped domestic governance but also influenced each country's foreign policy orientation, relations with the European Union, and resilience against authoritarian pressure. In both cases, Russia has demonstrated a clear strategic interest in exploiting information vulnerabilities to weaken democratic outcomes.

This report seeks to analyze Russian FIMI tactics during the 2025 electoral cycles in Georgia and Moldova, with a particular focus on digital platforms, media ecosystems, and the use of emerging technologies such as artificial intelligence. While publicly available information on these activities exists, it remains fragmented, insufficiently systematized, and often lacks comparative perspective.

A core added value of this research lies in its comparative and peer-learning approach. Since 2014 - and especially following Russia's full-scale invasion in 2022 - Ukraine has become a testing ground for Russian information warfare. At the same time, Ukraine has developed significant societal resilience through coordinated action by government institutions, civil society, independent media, and international partners. These experiences offer valuable lessons for countries facing similar threats under different political and institutional conditions.

The **primary objectives** of this report are to:

- Identify and analyze key patterns of Russian FIMI related to the 2025 elections in Georgia and Moldova;
- Examine how these tactics exploit specific vulnerabilities in national media and digital ecosystems;
- Compare these patterns with Ukraine's experience;
- Provide evidence-based recommendations for policymakers, civil society, media, and international partners.

By doing so, the report aims to contribute to stronger democratic resilience in Georgia and Moldova, while also informing broader European and transatlantic efforts to counter foreign electoral interference.

Conceptual & Analytical Framework

Foreign Information Manipulation and Interference (FIMI) refers to coordinated efforts by foreign state or non-state actors to manipulate information environments in ways that undermine democratic processes, distort public debate, weaken trust in institutions, and influence political behavior. Unlike isolated acts of disinformation, FIMI represents a broader strategic framework that combines information operations, cyber-enabled activities, covert influence networks, and psychological manipulation.

The European External Action Service defines FIMI as a pattern of behavior that is manipulative in

character, conducted intentionally and in a coordinated manner by foreign actors, and capable of causing harm to democratic systems and societal cohesion. In practice, FIMI often targets periods of heightened political sensitivity such as elections, referenda, military crises, or protests.

Within the context of Georgia and Moldova, Russian FIMI activities have sought to exploit existing political polarization, economic insecurity, unresolved territorial conflicts, and societal divisions regarding relations with the European Union and NATO. Electoral periods are particularly vulnerable because they amplify public attention, increase information consumption, and heighten emotional responses, thereby creating favorable conditions for manipulation.

This report approaches FIMI not merely as a communication challenge, but as a multidimensional security issue intersecting with democratic governance, digital resilience, and geopolitical competition.

Disinformation, Propaganda, and Influence Operations

Although often used interchangeably, disinformation, propaganda, and influence operations represent distinct but interconnected concepts within the broader ecosystem of information warfare.
Disinformation refers to false or misleading information that is intentionally created and disseminated to deceive audiences and produce political, social, or strategic effects. Unlike misinformation, which may involve the unintentional spread of inaccurate content, disinformation is deliberate and coordinated.

Russian disinformation campaigns frequently rely on emotionally charged narratives, conspiracy theories, fabricated evidence, manipulated media, and selective distortions of factual events. Common narratives observed across Eastern Europe include:

- portraying Western institutions as corrupt or morally decadent;
- framing European integration as a threat to national sovereignty;
- depicting democratic governments as externally controlled;
- exaggerating social instability or economic decline;
- undermining trust in electoral integrity.

Disinformation campaigns rarely aim to persuade audiences of a single "truth." Rather, they seek to create confusion, cynicism, and informational overload, weakening citizens' ability to distinguish reliable information from manipulation.

Propaganda differs from disinformation in that it may contain partially truthful information but presents it selectively and systematically to advance ideological or political objectives. Russian state-affiliated media outlets often combine factual reporting with manipulative framing, omission of context, emotional messaging, and repetition of strategic narratives.

Kremlin propaganda frequently emphasizes themes such as:

- traditional values versus Western liberalism;
- geopolitical victimhood;
- anti-NATO sentiment;
- protection of Russian-speaking populations;
- alleged external interference by Western actors.

In Georgia and Moldova, as well as Ukraine propaganda efforts often exploit historical memory, identity politics, and fears related to war, economic instability, or cultural transformation.

Influence operations represent the broader strategic coordination of activities intended to shape perceptions, behavior, and political outcomes. These operations combine information activities with diplomatic pressure, economic leverage, cyber operations, covert networks, and proxy actors.

Modern influence operations typically involve:

- coordinated messaging across multiple platforms;
- amplification through social media networks and automated accounts;
- use of local intermediaries, influencers, or political actors;
- cyber-enabled leaks or hacks;
- exploitation of domestic grievances;
- manipulation of traditional and digital media ecosystems.

In electoral contexts, influence operations may seek not only to support preferred political actors but also to delegitimize democratic institutions themselves by reducing trust in voting systems, media, or public authorities.

Russian information warfare doctrine

Russian information operations are rooted in a broader strategic doctrine that views the information space as a central arena of geopolitical competition. Since the early 2000s, Russian military and political thinking has increasingly emphasized the integration of informational, psychological, cyber, and political tools into statecraft.

Russian strategic doctrine does not clearly distinguish between war and peace in the informational domain. Instead, information confrontation is viewed as a continuous process aimed at shaping political environments both domestically and internationally.

Several characteristics define the Kremlin's approach to information warfare:

Hybrid and Asymmetric Strategy
Russia employs asymmetric methods to compensate for conventional limitations and exploit vulnerabilities in democratic societies. Information manipulation is relatively low-cost, difficult to attribute, and capable of generating disproportionate political effects.

Reflexive Control
A key concept in Russian strategic thinking is "reflexive control," which seeks to influence an adversary's decision-making process by shaping perceptions and informational environments. Rather than forcing direct outcomes, reflexive control aims to induce targets to make decisions favorable to Russian strategic interests.

Plausible Deniability
Russian operations frequently rely on unofficial actors, proxy organizations, fringe media outlets, and covert online networks to obscure direct state involvement. This ambiguity complicates attribution and weakens international responses.

Exploitation of Existing Divisions
Rather than inventing societal tensions, Kremlin-linked operations typically amplify pre-existing grievances and divisions. Polarization surrounding identity, language, corruption, religion, or geopolitics becomes a strategic entry point for manipulation.

Persistent and Adaptive Operations
Russian information campaigns are adaptive and iterative. Narratives evolve according to political developments, audience reactions, and platform dynamics. Failed narratives are quickly replaced or reframed, while successful themes are amplified across multiple channels simultaneously.

The experiences of Ukraine since 2014 demonstrate the extent to which Russian information warfare can accompany broader political and military aggression. At the same time, Ukraine's response has shown that societal resilience, institutional coordination, and media literacy can significantly reduce the effectiveness of such operations.

Digital Platforms and Emerging Technologies

The digitalization of political communication has fundamentally transformed the scale, speed, and reach of foreign information manipulation. Social media platforms now serve as primary vectors for narrative dissemination, audience targeting, and amplification.

Platforms such as Facebook, Telegram, TikTok, YouTube, and X (formerly Twitter) play a central role in contemporary information operations. Their algorithmic structures often reward emotionally provocative, divisive, or sensational content, thereby facilitating the spread of manipulative narratives.

In Georgia and Moldova, social media environments present several vulnerabilities:

- fragmented media consumption patterns;
- limited moderation in local languages;
- weak transparency regarding political advertising;
- low levels of digital literacy among some demographic groups;
- strong reliance on messaging applications and informal information networks.

Telegram channels and TikTok have become particularly important due to limited content moderation, rapid virality, and the ability to disseminate narratives through pseudo-organic networks.

Automated or semi-automated social media accounts ("bots") are frequently used to artificially amplify narratives, manipulate trending topics, and create the illusion of widespread public support. Coordinated inauthentic behavior may involve networks of fake accounts, troll farms, or centrally managed influence campaigns.

These tactics serve multiple purposes:

- increasing visibility of manipulative content;
- intimidating critics and journalists;
- overwhelming fact-checking efforts;
- distorting perceptions of public opinion.
- Artificial Intelligence and Deepfakes

Emerging technologies, particularly generative artificial intelligence, have expanded the capabilities of information manipulators. AI-generated text, images, audio, and video enable the rapid production of persuasive but fabricated content at unprecedented scale and low cost.

Deepfakes and synthetic media pose growing risks during elections because they can:

- impersonate political leaders;
- fabricate statements or scandals;
- generate false evidence;
- intensify distrust in authentic information.

Even when quickly debunked, manipulated content may continue to influence public perceptions due to the speed of digital dissemination and cognitive biases favoring emotionally charged information.

Information Overload and "Post-Truth" Dynamics

Contemporary information warfare increasingly focuses not on convincing audiences of a single narrative, but on overwhelming them with contradictory claims and uncertainty. This "firehose of falsehood" model erodes trust in all sources of information and weakens the shared factual basis necessary for democratic deliberation.

The result is a broader erosion of epistemic trust – trust in media, institutions, elections, and even objective reality itself.

Research Design and Methods

The research combined desk-based review, semi-automated content analysis, social media monitoring, fact-finding missions and expert interviews.

- Desk research covered official reports, election assessments, academic literature, investigative journalism and relevant policy documents.
- Social media monitoring focused primarily on Telegram, Facebook, TikTok, YouTube and X, using selected keywords, recurring narratives and actor-based searches in relevant languages.
- Semi-automated tools supported the identification of coordinated activity, repeated narratives and unusual amplification patterns, while findings were reviewed manually.
- Fact-finding missions in Georgia and Moldova and interviews with public officials, civil society representatives, journalists, researchers and election experts provided contextual and qualitative insights.
- Interviewees were selected on the basis of their direct expertise, institutional role and knowledge of national information environments.

Limitations, Ethics, and Risk Mitigation

The research faced limitations related to incomplete platform access, deleted or private content, uneven language coverage and the difficulty of proving direct attribution to foreign actors.

Findings therefore distinguish between confirmed attribution, probable coordination and narrative alignment. Sensitive information was handled cautiously to protect interviewees and avoid exposing vulnerable individuals or monitoring methods. Claims were verified through triangulation across multiple independent sources, platform data, expert testimony and open-source evidence. Where verification was not possible, uncertainty was stated explicitly and conclusions were limited accordingly.

Part II
Lessons from Ukraine

Evolution of Russian FIMI in Ukraine, 2014-2025

2014–2022: the testing ground

Ukraine is largely seen as a laboratory in which most of the tactics later deployed against Georgia and Moldova were first developed at scale. The annexation of Crimea and the war in Donbas were accompanied by an information operation whose core elements are now standard across the region: denial of direct state involvement ("little green men"), saturation of the information space with mutually contradictory versions of events (most notoriously around the downing of flight MH17), exploitation of language, religion, and historical memory as wedge issues, and the use of ostensibly local proxies to voice Kremlin positions. The response infrastructure that now defines Ukrainian resilience also dates from this period: StopFake was founded within weeks of the annexation in March 2014, and the years 2014–2021 saw the gradual construction of a regulatory perimeter, including broadcast bans on Russian channels and the 2017 blocking of Russian social media platforms. Two features of the pre-2022 period matter for the comparative argument of this report. First, Russian operations were still predominantly persuasive in intent: they sought to convince audiences of specific claims, such as the illegitimacy of the post-Maidan government or the "civil war" framing of Donbas. Second, Ukraine's countermeasures were largely reactive and fact-checking-centred, a model whose limits became apparent as the volume of manipulation grew.

2022–2023: industrialisation under full-scale war

The full-scale invasion transformed both the scale and the function of Russian FIMI. According to the first EEAS FIMI Threat Report, 60 of the 100 incidents analysed in 2022 were motivated by attempts to strengthen or justify the armed aggression against Ukraine[1]. The information campaign became an integrated component of military operations, and three developments from this period proved formative.

The first was the arrival of synthetic media as an operational weapon. The crude deepfake of President Zelensky calling on Ukrainian forces to surrender, seeded in March 2022 alongside the hacking of a national broadcaster's ticker, failed within hours, but it established the template of combining a cyber intrusion with synthetic content, what the Institute for Innovative Governance framework paper calls a hybrid FIMI incident, in which the cyber and informational components function as a single mechanism[2].

The second was industrial-scale impersonation. Operation Doppelgänger produced cloned versions of at least 17 major Western outlets, including Le Monde, The Washington Post, The Guardian, and Bild, complete with lookalike domains, and was managed through dedicated software coordinating profiles, content production, and target selection[3]. The impersonation playbook later reappeared almost unchanged in Moldova, where Storm-1516 and Matryoshka built fake local news sites and fabricated BBC, DW, and Euronews reports (see Part V).

1 EEAS, 1st Report on Foreign Information Manipulation and Interference Threats, February 2023.
2 Countering AI-Enabled Cyber Threats and FIMI: A Cross-Government Framework for Ukraine's Public Sector, Institute of Innovative Governance.
3 Ibid

The third was the convergence of FIMI with cyber operations: hack-and-leak operations against officials, phishing campaigns impersonating ministries and state services, and attacks on the databases underpinning public trust in digital government. The 2025 episode in which a file purporting to be a leaked Diia database circulated online illustrates the reputational mechanics: regardless of the technical reality, the state was forced into defensive communication about the security of its flagship digital infrastructure.

2023–2025: from persuasion to exhaustion, and the routinisation of AI

From late 2023, Ukrainian analysts documented a strategic shift in Russian tactics that this report treats as the single most important lesson for Georgia and Moldova: the move from mass persuasion to information exhaustion. The objective of most campaigns is no longer to make audiences believe specific Russian claims, but to compel them to doubt any message from any source, including official ones[4]. Exhaustion is cheaper than persuasion, more resistant to fact-checking, and corrosive precisely where democracies are most vulnerable: in the baseline trust that makes institutional communication possible at all.

This shift coincided with the routinisation of generative AI across every stage of the FIMI cycle. Mapping conducted for the Institute for Innovative Governance framework paper identifies four distinct modes, each documented in the Ukrainian theatre:

Content generation. Deepfakes of military and political figures became recurrent rather than exceptional: fabricated appeals attributed to the 117th Territorial Defence Brigade[5] calling on General Zaluzhnyi to remove the government; an AI-edited photograph of schoolchildren deployed during the February 2024 change of military command to seed coup narratives; a viral AI-generated video of a "mass retreat from Pokrovsk"[6] debunked by the Center for Countering Disinformation in March 2025 by its visual artefacts ("floating" stretchers, anatomically impossible movement). Texty.org.ua's analysis of mobilisation-themed videos found that 45 percent of 268 analysed recordings combined harmful narratives with calls to action designed to harvest personal data, showing how AI-generated disinformation and phishing now operate as a single funnel[7].

Amplification infrastructure. The Center for Countering Disinformation assesses that roughly 67 percent of comments in the Ukrainian segment of Telegram are generated by pro-Russian bots[8]. A 2025 OpenMinds and DFRLab study of Telegram channels serving occupied territories identified at least 3,600 bot accounts that produced more than 316,000 comments on 69 topics in a week and a half, roughly one comment every 36 seconds[9]. The same architecture was exported: on the eve of Moldova's elections, around 500 bots operated in the Moldovan segment of Telegram, achieving comment uniqueness of 95 percent, a level of variation only feasible with generative text models.

Targeting and social engineering. AI-assisted profiling is used to identify vulnerable groups, with military personnel and their families singled out for tailored disinformation, blackmail, and threats. Real-time deepfakes crossed from theory to practice years ago: the fake Klitschko video calls with the mayors of Berlin, Madrid, and Vienna in 2022, and the 25-minute real-time deepfake of Petro Poroshenko used against fighters of the International Legion, demonstrated that live impersonation of trusted figures can extract information and shape decisions before verification is possible.

Attacks on the information layer of AI itself. The Pravda/Portal Kombat network floods the open web with low-quality republished propaganda in dozens of languages, not primarily for human readers but to contaminate the retrieval base of large language models, a technique now termed LLM grooming[10]. NewsGuard documented chatbots repeating Storm-1516 narratives about France,

4 Ibid
5 https://www.tiktok.com/@ukrglass/video/7335361313985547538?_r=1&_t=8jsFXVzJtry
6 https://uatv.ua/uk/oborona-pokrovska-tryvaye-u-tspd-sprostuvaly-shi-video-rosiyan-z-fejkamy-pro-vidstup-zsu/
7 https://texty.org.ua/projects/116211/shtuchnyj-intelekt-i-tiktok-yak-vidomyx-zhurnalistok-peretvoryuyut-na-fejky/
8 https://www.ukrinform.ua/rubric-society/4068504-v-ukrainskomu-telegrami-67-komentariv-e-robotou-rosijskih-botoferm-cpd.html
9 https://www.openminds.ltd/reports/digital-occupation-pro-russian-bot-networks-target-ukraines-occupied-territories-on-telegram
10 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5461315&__cf_chl_f_tk=lBR1_Y9vvC_TixIHLEh_KjrnhnRlpX6BztFvv4TaP-do-1783095016-1.0.1.1-88Z7D1PY3KT_T1Vg6oh9ay.cvzPYdpabk80YFAQVDHs

and an August 2025 Texty.org.ua audit of 27 LLMs found reliability on Ukraine-related questions degraded sharply outside English[11]. For electoral contexts, the implication is direct: as voters increasingly consult AI assistants, the assistants themselves become a contested surface.

The trajectory, in short, runs from persuasion (2014), through industrialisation and cyber convergence (2022), to exhaustion and AI routinisation (2023–2025). Georgia and Moldova in 2025 encountered the mature version of this system, without the decade of adaptation Ukraine had undergone.

Lessons from Ukrainian Resistance

The most transferable finding from Ukraine is architectural. Ukrainian resilience does not rest on one strong counter-disinformation agency; it rests on a networked model combining government analytical units, domestically built technology platforms, investigative media, and civil society fact-checkers. Military and strategic communications structures work with AI monitoring platforms developed by Ukrainian companies (Osavul, LetsData, Mantis Analytics); newsrooms such as Texty.org.ua and fact-checking organisations including VoxUkraine, Detector Media, and StopFake use the same class of tools for verification and documentation; state bodies use them to prepare communication decisions. The framework paper identifies three mechanisms through which this architecture produces resilience: it accelerates innovation through rapid feedback between developers and end users; it distributes verification capacity across many societal nodes rather than concentrating it in one institution; and it shortens the detection-to-response cycle, cutting into the adversary's window of surprise[12].

Crucially, the model remains human-centric. AI tools generate alerts, cluster narratives, and detect coordinated inauthentic behaviour, but attribution, public response, and legal assessment remain with authorised human actors. This matters for transfer: what Georgia and Moldova would be importing is not a piece of software but a division of labour.

Government responses

On the institutional side, Ukraine built two specialised bodies, the Center for Countering Disinformation under the NSDC and the Center for Strategic Communications and Information Security under the Ministry of Culture, alongside the pre-existing security, cyber, and regulatory agencies. Their practical record includes rapid public debunking of high-impact fakes (the Pokrovsk video, the Zaluzhnyi coup narratives), documentation of adversary TTPs, and increasingly sophisticated coordination with platforms and international partners.

Regulatory measures included media registration requirements and aggressor-state ownership bans under the Law on Media, criminalisation of specific propaganda categories, and targeted sanctions against FIMI actors and resources. The Ukrainian experience with sanctions is instructive in both directions: they proved effective against traditional broadcast infrastructure but structurally too slow for the online environment, where sanctioned outlets reappear as clones within days, a dynamic Moldova has already encountered with the Sputnik Moldova ecosystem, whose "2.0" channels feature prominently in post-ban monitoring data (see Part V)[13].

An honest account must also register the limits, because they are as instructive as the successes. Ukraine's Information Security and Cybersecurity Strategies both expired in 2025 without timely replacement; interagency response remains largely ad hoc, without a unified incident taxonomy or standard operating procedures; and the state has itself described the resulting condition as "managed chaos", in which institutions spend resources on consequences rather than on systematic counteraction. Ukrainian resilience, in other words, is real but under-institutionalised: societal capacity has outrun governance architecture. Georgia and Moldova should copy the capacity and preempt the institutionalisation gap rather than replicate it.

Civil society, independent media, and OSINT

Ukraine's civil sector functions as the distributed sensor network of

11 https://texty.org.ua/projects/115548/sho-dumaye-shi-pro-ukrayinu-doslidzhennya-uperedzhen-velykyh-movnyh-modelej/
12 Countering AI-Enabled Cyber Threats and FIMI: A Cross-Government Framework for Ukraine's Public Sector, Institute of Innovative Governance.
13 https://hcss.nl/wp-content/uploads/2025/07/Policy-Brief-FIMI-in-Focus-HCSS-2025.pdf

the model: the Institute of Mass Information, Detector Media, StopFake, VoxUkraine, Molfar, and dozens of smaller organisations monitor dissemination channels, document incidents, and feed both public debunks and confidential signals to state bodies. Investigative OSINT practice, honed on war documentation, transfers directly to FIMI attribution: reverse image search exposed the doctored Zaluzhnyi schoolchildren photo; digital tracing linked bot networks to their coordinating infrastructure; metadata and provenance analysis underpin most successful attributions.

Two features distinguish the Ukrainian civil sector's role from a generic "support civil society" recommendation. First, it possesses independent analytical legitimacy: debunks from Detector Media or Texty carry credibility with audiences that distrust government communication, which is precisely the audience exhaustion campaigns target. Second, it is integrated into response workflows rather than parallel to them, functioning as what the framework paper describes as an extra verification layer for complex cases and an amplifier of trust in public communications.

Media literacy and prebunking

Ukraine invested early in shifting from debunking (reactive fact-checking after a narrative spreads) toward prebunking (inoculating audiences against manipulation techniques before specific fakes appear). The national educational platform Diia. Education carries courses on disinformation recognition, cyber hygiene, phishing, and AI literacy aimed at both civil servants and the general public.[14] The strategic logic follows the evidence on the illusory truth effect: once the space is saturated, corrections struggle, so the cheaper intervention is upstream. Ukrainian practice also generated a set of debunking disciplines directly relevant to electoral contexts: refute only major and influential fakes to avoid amplification; lead with the accurate statement rather than restating the fake; respond infrastructurally (through platform escalation against coordinated networks) rather than item by item[15].

Platform cooperation

Ukraine's engagement with platforms evolved from ad hoc contact toward structured escalation, using established channels to request removal of coordinated networks, cloned resources, and specific high-harm content. The experience yields a sober lesson: platform response is meaningful but slow, inconsistent across companies, and weakest in non-English languages, which is why the framework paper's central recommendation is a designated national coordination point with pre-agreed, DSA-aligned crisis protocols for vulnerable periods, rather than reliance on personal contacts and goodwill[16]. Moldova's 2025 experience, where authorities secured removal of some 100,000 fake TikTok accounts yet saw Operation Undercut reconstitute its networks within 24 hours of takedown, confirms both halves of that lesson[17].

Transferable Lessons for Georgia and Moldova

Five elements of the Ukrainian experience are, in this report's assessment, directly adaptable.

The networked sensor model. Building distributed monitoring capacity across government, civil society, and technology partners does not require wartime conditions, large budgets, or new legislation. Moldova has already moved partway there: WatchDog.MD, local fact-checkers, and international monitoring during the 2025 elections functioned as exactly this kind of network. The gap is formalisation: standing signal-sharing arrangements, agreed escalation procedures, and joint exercises.

Rapid-response protocols for vulnerable periods. Ukraine's core procedural lesson is that election periods, like major security incidents, need pre-authorised response tracks with defined roles, timelines, and platform escalation channels agreed in advance. The Floreşti drone case in Moldova (see Part V), where a fabricated narrative occupied the information space

14 https://cdn.osce.org/sites/default/files/f/documents/f/e/596911.pdf
15 https://www.village.com.ua/village/life/mediahramotnist/338591-voxcheck-ya-doslidzhuiu-rosiisku-propahandu
16 https://digital-strategy.ec.europa.eu/en/policies/digital-services-act
17 Théodore Donguy, "Operation Matryoshka: Russia's direct intrusion into Moldova's parliamentary elections," New Eastern Europe, 10 October 2025, https://neweasterneurope.eu/2025/10/10/operation-matryoshka-russias-direct-intrusion-into-moldovas-parliamentary-elections/; G7 Rapid Response Mechanism, Joint Monitoring of 2025 Moldovan Parliamentary Elections, https://international.canada.ca/en/global-affairs/corporate/reports/rapid-response-mechanism/news/2025-moldovan-election

unchallenged for an entire evening because it was seeded after working hours, is a textbook illustration of what the absence of such a protocol costs.

Prebunking around predictable events. Elections are the most predictable vulnerable period there is. Russian TTPs are stable enough (impersonation of trusted media, fabricated corruption "investigations", diaspora-focused fraud claims, staged-incident conspiracies) that audiences can be inoculated against the techniques months in advance, without needing to anticipate specific fakes.

A common analytical language. Adopting the FIMI framework, the ABCDE and DISARM methodologies, and standardised incident documentation costs little and yields compatibility with EEAS reporting, the G7 RRM, FIMI-ISAC, and donor-funded monitoring, multiplying the value of every locally documented incident[18]. For two EU candidate states, this is also an accession investment.

Treating FIMI and cyber as one continuum. Moldova's 2025 experience (over 1,000 cyberattacks on state systems alongside the information campaign) replicates the Ukrainian pattern; response structures that separate the two will systematically miss hybrid incidents such as hack-and-leak operations and phishing built on impersonation of state institutions.

What cannot be replicated

Three foundations of Ukrainian resilience do not transfer, and pretending otherwise would mislead policymakers.

First, the clarity of existential threat. Full-scale war produced a societal consensus about the adversary that suppresses the domestic political incentive to borrow Kremlin narratives for partisan gain. In both Georgia and Moldova, significant domestic political forces profit from amplifying those narratives, which means the "whole-of-society" model has to be built without the whole society, and in Georgia, as discussed below, without the state.

Second, the legal perimeter. Ukraine's bans on Russian platforms, broadcasters, and affiliated media rest on a legal basis (armed aggression by the sanctioned state) and a degree of public acceptance that neither Georgia nor Moldova can assume. Moldova's more surgical measures, such as the deregistration of the Victory bloc over illicit financing, point to the realistic alternative: enforcement targeted at behaviour (financing, coordination, impersonation) rather than at content or entire platforms.

Third, the scale of international integration. Ukraine's counter-FIMI capability is embedded in the Tallinn Mechanism, NATO StratCom cooperation, the UK-Ukraine 100 Year Partnership, and prospective integration into FIMI-ISAC and the EU Rapid Alert System. Moldova received a meaningful fraction of comparable attention in 2025, including EU Hybrid Rapid Response Team support; Georgia, under its current government, is moving in the opposite direction, with the UK cancelling its electoral-observation grant programme in 2025 amid official hostility.[19]

The deepest limit on transfer is not resources but the position of the state itself. The Ukrainian model presumes a government that wants to counter Russian FIMI. That assumption holds in Moldova, holds only partially in Ukraine's own contested pre-2022 politics, and does not hold in Georgia in 2025.

In Moldova, the state is a willing counter-actor with capacity constraints: a small country facing what its experts assessed as the largest foreign electoral interference operation on record, spending roughly two percent of GDP-equivalent to defend against it.[20] The Ukrainian lessons apply nearly wholesale, with adaptations for Moldova's specific vulnerabilities: the Romanian/Russian linguistic divide that Russian operations exploit through language-segmented channels, the weight of the diaspora vote and its

18 https://www.disinformationindex.org/research/2024-10-21-fimi-isac-collective-findings-report-on-2024-european-elections/

19 EUvsDisinfo, "Russian scripts, Georgian voices: How disinformation targets the country's Western allies: the US, EU, and UK in Georgia," August 2025, https://euvsdisinfo.eu/russian-scripts-georgian-voices-how-disinformation-targets-the-countrys-western-allies-the-us-eu-and-uk-in-georgia/

20 Théodore Donguy, "Operation Matryoshka: Russia's direct intrusion into Moldova's parliamentary elections," New Eastern Europe, 10 October 2025, https://neweasterneurope.eu/2025/10/10/operation-matryoshka-russias-direct-intrusion-into-moldovas-parliamentary-elections/; G7 Rapid Response Mechanism, Joint Monitoring of 2025 Moldovan Parliamentary Elections, https://international.canada.ca/en/global-affairs/corporate/reports/rapid-response-mechanism/news/2025-moldovan-election

exposure to targeted fraud narratives, the unregulated online media space, and the Transnistrian parallel information ecosystem documented in this report's monitoring data.

In Georgia, the ruling party's convergence with Kremlin messaging inverts the model. During the 2024–2025 electoral cycle, statements by Russia's SVR alleging Western coup plots were rebroadcast within hours by government-aligned broadcasters, and senior officials accused the EU and UK of interference in terms indistinguishable from Russian narratives. Where the state is an amplifier rather than a counter-actor, the transferable unit is not the interagency protocol but the civil-society layer of the Ukrainian model: independent monitoring, OSINT documentation, international signal-sharing, and audience-level inoculation. Yet exactly that layer is under legal pressure from foreign-agent-style legislation, and local watchdogs boycotted observation of the October 2025 municipal elections altogether[21]. The honest conclusion is that in captured-state conditions, the Ukrainian experience transfers mainly as documentation practice, preserving an evidentiary record for future accountability, and as support for exiled and surviving independent media, not as a national resilience framework.

This three-way distinction (counter-actor, bystander, amplifier) is proposed here as the organising lens for the comparative analysis in Part VI: the same Russian toolkit produces different outcomes depending less on the sophistication of the attack than on which side of the information conflict the target state's own government stands.

21 Sopo Gelava, "Suspicious websites amplify narratives from sanctioned Russian entities targeting Georgia," DFRLab, 28 November 2025, https://dfrlab.org/2025/11/28/suspicious-websites-amplify-narratives-from-sanctioned-russian-entities-targeting-georgia/; Emma Woollacott, "EU Hits Back Over Georgian Election Misinformation," Forbes, 6 October 2025.

Part III
Country Case Study: Georgia

Scale and strategic context

Russian information manipulation surrounding Georgia's 4 October 2025 municipal elections developed within a political environment already shaped by the disputed 2024 parliamentary elections, prolonged anti-government protests, increasing restrictions on civil society and a sharp deterioration in relations between the Georgian government and its Western partners. Unlike Moldova, where the principal confrontation was between foreign interference networks and a government attempting to defend the electoral process, the Georgian case was characterised by extensive convergence between Russian strategic narratives and the messaging of domestic political and government-aligned actors[22].

This convergence complicates attribution. Not every anti-Western statement circulated by Georgian politicians or media outlets can be classified as a Russian-directed operation. Nevertheless, foreign information manipulation does not require direct control over every amplifier. Russian actors can introduce or reinforce narratives that are subsequently adopted, localised and legitimised by domestic actors pursuing their own political objectives. The result is a form of narrative laundering in which foreign strategic interests become embedded in apparently domestic political debate.[23]

The 2025 municipal elections took place under highly restrictive conditions. Most major opposition parties boycotted the vote, domestic watchdog organisations did not conduct observation, and Georgia's late invitation to the OSCE Office for Democratic Institutions and Human Rights made meaningful international observation impossible. Georgian Dream subsequently claimed more than 80 per cent of the nationwide vote and victory across all municipalities.[24]

The information campaign surrounding the elections was therefore not primarily aimed at persuading undecided voters between competing electoral programmes. Its broader function was to legitimise the governing party's political position, portray domestic opposition and civil society as instruments of foreign powers, and pre-emptively discredit protests or international criticism as components of a Western-sponsored coup attempt.

In this context, Russian FIMI operated less as a separate external campaign than as part of a mutually reinforcing ecosystem. Russian intelligence statements and state-aligned media supplied claims about Western interference, while Georgian officials, pro-government broadcasters and associated online networks repeated or adapted similar arguments for domestic audiences.[25]

Dominant narratives

The most prominent narrative during the 2025 electoral cycle alleged that Western governments were attempting to organise a coup, revolution or violent change of government in Georgia. This framing drew on the

22 ISFED, "Propaganda and Information Operations in Georgia," 2025.
https://isfed.ge/eng/sotsialuri-mediis-monitoringi/propaganda-da-sainformatsio-manipulatsiebi-saqartveloshi

23 OSCE Office for Democratic Institutions and Human Rights, "Invitation from Georgia less than a month before elections makes meaningful observation impossible: ODIHR statement," 9 September 2025, https://odihr.osce.org/odihr/elections/597267

24 Media Development Foundation, "Disinformation and Discrediting Campaigns against Media and Journalists," 4 May 2026.
https://mdfgeorgia.ge/en/case/disinformation-and-discrediting-campaigns-against-media-and-journalists/

25 Venice Commission, "Georgia–Opinion on the Amendments to the Organic Law 'Election Code of Georgia', Pertaining to Local Elections," CDL-AD(2025)016, 15 March 2025, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2025)016-e

established Kremlin concept of "colour revolutions," according to which popular protests and democratic movements in post-Soviet states are not authentic domestic developments but externally organised regime-change operations.

The narrative was used preemptively. Before the municipal elections, Russia's Foreign Intelligence Service and other Kremlin-linked sources claimed that Western actors, particularly the United Kingdom, were preparing destabilisation, supporting radical opposition groups and financing organisations that would challenge the electoral result. A grant announced by the British Embassy to support domestic election observation was presented as evidence of a British operation to remove the Georgian government. Russian Duma member Andrei Lugovoi reinforced the claim through a documentary titled Georgian Front, which depicted Western engagement with civil society as part of a coordinated effort to provoke unrest.

This framing served several purposes simultaneously. It delegitimised independent election observation, presented international assistance as covert political interference and created a justification for restrictive action against protesters and civil society organisations. It also allowed any post-election mobilisation to be dismissed in advance as foreign-directed rather than as a response to domestic political grievances.[26]

A second major narrative portrayed the European Union, the United States and other Western partners as seeking to draw Georgia into a war with Russia. This "second front" narrative had circulated since the beginning of Russia's full-scale invasion of Ukraine but remained central during the 2025 electoral period. According to this framing, Western governments were dissatisfied with Georgia's refusal to confront Russia and were therefore supporting opposition forces willing to open a new battlefield in Abkhazia or South Ossetia.

The unresolved territorial conflicts provided this narrative with significant emotional power. Memories of the 2008 war were used to suggest that stronger alignment with the EU, NATO or Ukraine would expose Georgia to renewed military confrontation. The governing party's claim to be preserving peace was consequently contrasted with an opposition allegedly willing to sacrifice national security on behalf of external actors.

Russian-linked websites reinforced this argument immediately before the municipal elections. One article published by the SVR-linked New Eastern Outlook and republished by The Intel Drop used the arrest of two Ukrainian nationals allegedly carrying explosives to claim that Ukraine and its Western allies were organising election-related provocations in Georgia. Other publications portrayed former President Salome Zourabichvili as a Western operative and alleged that European and American actors intended to reactivate the conflicts in Abkhazia and South Ossetia.

A third recurring narrative presented Western support for civil society, media and election monitoring as an attack on Georgian sovereignty. Foreign-funded organisations were accused of serving external political interests, organising unrest and acting outside democratic accountability. This narrative aligned closely with the justification used for legislation targeting organisations receiving foreign funding.

The manipulation lies not in the factual observation that Georgian organisations receive international assistance, which many do transparently, but in the systematic portrayal of such assistance as evidence of subversion. Foreign funding was treated as proof that organisations lacked legitimate domestic constituencies, while their criticism of the government was framed as the execution of instructions from Brussels, Washington or London.

A fourth narrative sought to reverse accusations of foreign interference by portraying the West, rather than Russia, as the principal external manipulator of Georgian politics. This created false equivalence between covert Russian influence operations and transparent diplomatic, financial or electoral assistance provided by democratic partners. EU criticism of electoral conditions was framed as an attempt to dictate political outcomes, while statements by Russian officials were reproduced as legitimate warnings about Western destabilisation.[27] This inversion was strategically useful because it blurred the meaning of foreign interference. If all external en-

26 European External Action Service, "Statement by High Representative/Vice-President Kallas and Commissioner for Enlargement Kos on Georgia," 5 October 2025, https://www.eeas.europa.eu/node/456882

27 ISFED, "Advertised Campaign Led by Russia against Pro-European Protest."

gagement is portrayed as equivalent, evidence of Russian manipulation loses its significance and Georgian citizens are encouraged to view international observation, civil society support and covert hostile influence as indistinguishable forms of geopolitical competition.

A fifth narrative legitimised the electoral process and government position by portraying criticism of the elections as fabricated, politically motivated or externally coordinated. Where credible domestic and international observation was limited, government-aligned media could selectively highlight favourable foreign voices and present them as representative international assessments.

This tactic continued a pattern documented after the 2024 parliamentary elections, when Georgian Dream-aligned broadcasters promoted statements from politically biased or inadequately qualified foreign observers. These individuals were repeatedly described simply as "international observers," while their affiliations and records were often omitted. Their positive comments were then amplified through television, websites and Facebook as evidence that the elections met democratic standards.

The significance of this tactic goes beyond the accuracy of individual statements. It creates a parallel system of validation designed to neutralise criticism from established monitoring organisations. Rather than directly disproving documented irregularities, the information ecosystem produces alternative "international" endorsements and invites audiences to treat all assessments as politically motivated.

Key platforms and channels

Facebook remained the central platform for domestic political communication in Georgia. Government-aligned broadcasters, political actors, commentators and online pages used it to disseminate television clips, political statements, visual cards and emotionally framed messages. DFRLab assessments of the regional information environment identified Facebook as the dominant platform in Georgia and documented the use of coordinated advertising and inauthentic amplification by both domestic and foreign actors.[28]

The platform's importance reflects the continuing interaction between television and social media. Major broadcasters produce the initial content, which is then repackaged into short video clips, headlines and quote cards for Facebook. This allows television narratives to circulate beyond scheduled broadcasts and acquire additional visibility through engagement-driven algorithms.

Government-aligned television outlets, particularly TV Imedi and Rustavi 2, played an important amplification role. Their coverage did not necessarily rely on demonstrably false content in every instance. More often, manipulation occurred through selective framing, repetition, omission of context and the promotion of actors whose statements supported the government's narrative.

The amplification of biased foreign observers after the 2024 parliamentary elections illustrates this method. TV Imedi and Rustavi 2 highlighted positive statements, repeatedly emphasised the speakers' foreign nationality and "international observer" status, and provided limited information about their credentials. The corresponding Facebook posts received thousands of reactions and shares, demonstrating how traditional media authority and social-platform amplification reinforced one another.

Russian and foreign-language websites served a different function. Their direct reach among Georgian voters was likely more limited, but they provided an external source layer from which narratives could be republished, cited or introduced into broader debate. DFRLab identified English-, French- and Polish-language websites that laundered content from sanctioned Russian organisations and targeted Georgia with claims about Western coup attempts and election destabilisation.[29]

The Intel Drop was particularly active, publishing 21 Georgia-related articles between January and October 2025.

https://isfed.ge/eng/sotsialuri-mediis-monitoringi/rusetidan-martuli-dareklamebuli-kampania-proevropuli-protestis-tsinaaghmdeg

28 International Society for Fair Elections and Democracy, "First Interim Report on Social Media Monitoring," 2024 Parliamentary Elections, https://isfed.ge/eng/2024-saparlamento/sotsialuri-mediis-monitoringis-pirveli-shualeduri-angarishi-27-agvisto-20-seqtemberi.

29 International Society for Fair Elections and Democracy, "Propaganda and Information Operations in Georgia," 2025, https://isfed.ge/eng/sotsialuri-mediis-monitoringi/propaganda-da-sainformatsio-manipulatsiebi-saqartveloshi

Much of its content originated from sanctioned Russian propaganda entities, including New Eastern Outlook, an organisation associated with Russia's Foreign Intelligence Service, and South Front. Publication intensified around the October elections and focused heavily on claims of Western infiltration, Ukrainian provocations and externally organised unrest.

This redistribution model provided several advantages. It obscured the original source, allowed content from sanctioned Russian entities to reach audiences through nominally separate websites and created the appearance that similar conclusions were being reached by multiple foreign outlets. The use of English and other European languages also made the content potentially useful for influencing international audiences and for reimporting Russian narratives into Georgian debate with an appearance of external validation.[30]

RuTube and Russian audiovisual channels were used to host longer propaganda products, such as the Georgian Front documentary. Telegram also remained relevant for Russian-language distribution and communication among highly politicised audiences, although the Georgian domestic political environment was less Telegram-centred than the Moldovan or Ukrainian cases.

YouTube and other video platforms provided durable hosting for political interviews, documentaries and broadcast segments that could then be redistributed through Facebook and websites. X was more relevant to international discourse, diplomatic messaging and the amplification of claims to foreign audiences than to mass domestic reach.

The platform structure in Georgia was therefore comparatively concentrated. Whereas Moldova's 2025 interference campaign relied on a large multiplatform ecosystem involving TikTok, Telegram, Facebook, X, cloned websites and extensive bot activity, Georgia's political information environment remained strongly anchored in the combination of television and Facebook. This increased the importance of domestic media ownership, editorial alignment and the relationship between governing-party communication and broadcast coverage.

Pro-Russian actors and amplification networks

The Georgian case requires careful differentiation between actors directly connected to Russia, actors with ideological or organisational links to pro-Russian networks, and domestic actors who amplify Russian narratives without evidence of direct coordination.

At the external level, Russian state bodies and intelligence-linked entities provided strategic narratives. Statements by the Russian Foreign Intelligence Service alleging Western coup preparations served as authoritative narrative anchors. Russian officials and state-aligned commentators then repeated these claims, while outlets linked to sanctioned organisations produced supporting articles and audiovisual material.[31]

The New Eastern Outlook network was an important content originator. DFRLab found that Georgia-related articles published by The Intel Drop frequently originated from New Eastern Outlook and South Front, both connected to wider Russian propaganda infrastructure. The content was then redistributed through additional foreign-language websites, creating a laundering chain between sanctioned originators and nominally separate amplifiers.[32]

Within Georgia, pro-Russian or strongly anti-Western political and media actors functioned as localisers. Some openly advocated closer relations with Moscow or promoted traditional Kremlin positions. Others did not present themselves as pro-Russian but repeatedly framed the EU, the United States, NATO and Western-supported civil society as threats to sovereignty, peace or national identity.

The most consequential amplification, however, came from the convergence between these narratives and the communication of the ruling Georgian Dream party and its aligned media ecosystem. Georgian Dream officials repeatedly accused Western actors of attempting to organise revolutions, interfere in elections or pressure Georgia into war. Govern-

30 Sopo Gelava, "Suspicious Websites Amplify Narratives from Sanctioned Russian Entities Targeting Georgia," Digital Forensic Research Lab, 28 November 2025, https://dfrlab.org/2025/11/28/suspicious-websites-amplify-narratives-from-sanctioned-russian-entities-targeting-georgia/

31 International Society for Fair Elections and Democracy, "Russian Disinformation Campaign Targeting Salome Zurabishvili," 2025, https://isfed.ge/eng/sotsialuri-mediis-monitoringi/rusuli-dezinformatsiuli-kampania-salome-zurabishvilis-tsinaaghmdeg

32 Sopo Gelava, "Suspicious Websites Amplify Narratives from Sanctioned Russian Entities Targeting Georgia," Digital Forensic Research Lab, 28 November 2025, https://dfrlab.org/2025/11/28/suspicious-websites-amplify-narratives-from-sanctioned-russian-entities-targeting-georgia/

ment-aligned broadcasters reproduced these claims and provided extensive airtime to commentators and foreign figures who reinforced them.[33]

This convergence does not prove that all domestic messaging was centrally directed by Russia. Its strategic effect was nevertheless favourable to the Kremlin. It normalised Russian interpretations of democratic protest, reduced public trust in the EU and Western governments, and shifted the political debate away from Russian occupation and toward alleged Western interference.

The laundering process typically followed one of several paths. In the first, a Russian official or intelligence agency issued an allegation that was subsequently reported by Georgian media and repeated by domestic politicians. In the second, a Russian-linked website published a fabricated or manipulative story that was redistributed through secondary foreign sites and social platforms. In the third, a Georgian political actor independently used a narrative already established in Russian propaganda, giving it local legitimacy without any visible external intervention.

Government-aligned television stations and their Facebook pages were especially important because they connected elite political messaging with mass audiences. Unlike anonymous bot accounts, established broadcasters carry institutional familiarity and can present politically motivated narratives as ordinary news reporting.

A secondary amplification layer consisted of ideologically aligned foreign politicians, commentators and purported election observers. Their statements were useful because they could be presented as independent international validation. In the aftermath of the 2024 elections, government-aligned Georgian media selectively promoted individuals from European and other countries whose positive assessments supported the official narrative, despite questions regarding their impartiality and professional credentials.

The same underlying tactic remained relevant in 2025, particularly because credible international and domestic observation was limited. In the absence of authoritative monitoring, favourable statements from sympathetic foreign actors could be given disproportionate weight.

Use of AI and automated tools

The publicly documented use of generative AI in Georgia's 2025 electoral information environment appears more limited than in Moldova. There were no comparably well-documented large-scale campaigns involving deepfakes of national leaders, industrial production of synthetic news reports or extensive AI-generated comment networks.[34] This does not mean that AI was absent. Generative tools had already become widely accessible and could have been used in routine content production, translation, image creation or text variation without producing visible forensic indicators. However, the available evidence does not support the conclusion that synthetic media was the defining feature of Russian FIMI in Georgia's municipal elections.

Automation and coordinated amplification were more significant than high-profile deepfakes. DFRLab identified coordinated advertising and inauthentic amplification on Facebook, the country's dominant political platform. These techniques can artificially increase the visibility of political content, create the appearance of widespread support and direct messages toward selected audiences.

The structure of the Georgian campaign also reduced the need for technically sophisticated synthetic content. Where government officials, major broadcasters and established political figures were already communicating narratives aligned with Russian strategic interests, fabricated impersonations were less necessary. Authentic statements by real domestic actors could achieve greater credibility and reach than an externally produced deepfake.[35]

This is an important comparative finding. AI-enabled manipulation is often treated as the principal emerging FIMI threat, but Georgia demonstrates that institutional and political

33 International Society for Fair Elections and Democracy, "Fake Accounts Supporting the Central Election Commission on Facebook," 2024/2025, https://isfed.ge/eng/sotsialuri-mediis-monitoringi/tseskos-mkhardamcheri-trolebis-moqmedeba-feisbuqze

34 International Society for Fair Elections and Democracy, "Propaganda and Information Operations in Georgia," 2025.

35 International Society for Fair Elections and Democracy, "Fake Accounts Supporting the Central Election Commission on Facebook," 2024/2025

capture can be more consequential than technological sophistication. A low-tech narrative repeated by trusted domestic actors may have greater impact than a highly sophisticated synthetic video distributed by anonymous accounts.[36]

Nevertheless, future Georgian elections are likely to face growing AI-related risks. Synthetic audio or video could be used to fabricate statements by opposition leaders, activists, diplomats or election observers. AI-generated content may also assist rapid translation and localisation of Russian narratives into Georgian and other relevant languages.

Automated engagement represents an additional concern. Generative models make it easier to produce varied comments and posts that evade detection based on repeated wording. On Facebook, such activity could be combined with coordinated pages, paid advertising and domestic political networks to simulate organic public support.[37]

The weakening of independent fact-checking also increases vulnerability. Meta's 2025 policy changes concerning third-party fact-checking were themselves used by political actors to attack and delegitimise Georgian researchers and monitoring organisations. Reduced access to platform data and fewer reliable moderation mechanisms may make it harder to distinguish genuine public engagement from coordinated activity.

Assessment

Five conclusions follow from the Georgian case.

First, Russian FIMI in Georgia relied less on overwhelming the electorate with large quantities of visibly foreign content than on the domestic adoption of Russian strategic narratives. The decisive mechanism was narrative convergence. Claims originating from Russian officials or propaganda networks gained political significance because they were repeated and legitimised by Georgian actors with much greater domestic reach.

Second, the dominant objective was not simply to influence municipal voting choices. It was to redefine the political conflict as a struggle between a sovereign government defending peace and foreign-supported actors seeking revolution, war and external control. This framing delegitimised opposition parties, civil society, independent media and Western criticism simultaneously.

Third, the fear of war was the strongest strategic vulnerability. The conflicts in Abkhazia and South Ossetia and the memory of 2008 enabled hostile narratives to equate European and Euro-Atlantic integration with renewed military confrontation. The "second front" narrative transformed accommodation with Russia from a geopolitical choice into an alleged necessity for national survival.

Fourth, television and Facebook formed the core amplification infrastructure. Russian-linked websites and audiovisual products supplied content and external validation, but domestic broadcasters and political actors provided the scale, familiarity and authority required to shape mainstream debate.

Fifth, Georgia demonstrates that technological sophistication is not the principal determinant of FIMI effectiveness. Compared with Moldova, the documented use of AI-generated content was limited. Yet the political effect may have been equally serious because narratives compatible with Russian interests were embedded in the domestic governing and media environment.

The central resilience problem in Georgia is therefore not only the detection and removal of foreign networks. It is the erosion of the distinction between foreign manipulation and official political communication. Where state institutions and government-aligned media reproduce the same narratives as the external aggressor, a conventional whole-of-government counter-FIMI model cannot function.

Under these conditions, resilience depends primarily on protecting independent media, civil society monitors, investigative researchers and international documentation mechanisms. Their task is not merely to debunk individual falsehoods but to trace how narratives originate, move across foreign and domestic networks, and become normalised within mainstream political discourse.

36 Venice Commission, "Georgia–Opinion on the Law on the Registration of Foreign Agents, the Amendments to the Law on Grants and Other Laws Relating to 'Foreign Influence'," CDL-AD(2025)034, 10 October 2025, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2025)034-e

37 Sopo Gelava, "Suspicious Websites Amplify Narratives from Sanctioned Russian Entities Targeting Georgia," DFRLab, 28 November 2025.

Part IV
Country Case Study: Moldova

Scale and strategic context

The parliamentary elections of 28 September 2025 were the most heavily targeted electoral process in Moldova's history and, by several assessments, one of the most intensive foreign interference operations ever documented against a single country. The election determined whether the Party of Action and Solidarity (PAS) would retain the majority needed to sustain Moldova's EU accession course, and the Kremlin treated it accordingly: as a decisive battle over the country's geopolitical orientation, fought primarily in the information space.

The scale is captured in several independent datasets. The 4th EEAS Report on FIMI Threats, covering 2025, recorded 540 FIMI incidents globally and identified Moldova as one of the most targeted countries worldwide, behind only Ukraine and France, with electoral interference as the dominant vector[38]. The G7 Rapid Response Mechanism, which conducted joint monitoring of the Moldovan information space in consultation with the government, documented over 450 pieces of FIMI content targeting the parliamentary elections and attributed the coordinated activity with high confidence to four known Russian state-aligned campaigns: Operation Overload (Matryoshka), Operation Undercut, Storm-1516, and Portal Kombat. [39]Moldovan public policy expert Andrei Curararu estimated total Russian spending on the interference effort at roughly EUR 300 million, equivalent to about two percent of Moldova's GDP, describing it as the largest foreign electoral interference operation ever recorded. The think tank WatchDog.MD assessed that the volume of manipulative content targeting Moldova exceeded by a factor of five what had been observed around the two most recent US presidential elections combined.[40]

The pressure was not limited to the information domain. Prime Minister Dorin Recean reported more than 1,000 cyberattacks against state systems in 2025, and authorities removed approximately 100,000 fake TikTok accounts spreading election-related disinformation.[41] TikTok separately confirmed the removal of a network of at least 6,790 accounts working to discredit the pro-European leadership.[42] BBC and Ziarul de Gardă investigations documented the parallel human infrastructure: covert networks linked to fugitive oligarch Ilan Shor that paid Moldovan citizens to produce and share pro-Russian content, coordinated through closed Telegram groups, generating posts viewed millions of times.[43]

Despite this pressure, PAS secured 55 of 101 seats, and the election was assessed by international observers as sound, though seriously marred by foreign interference.[44] The Moldo-

38 EEAS, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards, March 2026, https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

39 G7 Rapid Response Mechanism, Joint Monitoring of 2025 Moldovan Parliamentary Elections, https://international.canada.ca/en/global-affairs/corporate/reports/rapid-response-mechanism/news/2025-moldovan-election

40 Théodore Donguy, "Operation Matryoshka: Russia's direct intrusion into Moldova's parliamentary elections," New Eastern Europe, 10 October 2025, https://neweasterneurope.eu/2025/10/10/operation-matryoshka-russias-direct-intrusion-into-moldovas-parliamentary-elections/

41 Ibid

42 OSCE/ODIHR International Election Observation Mission, Republic of Moldova, Parliamentary Elections, 28 September 2025, Statement of Preliminary Findings and Conclusions.

43 AFP, "Russia-linked disinfo campaign targets Moldovan election," 24 September 2025, https://www.france24.com/en/live-news/20250924-russia-linked-disinfo-campaign-targets-moldovan-election

44 OSCE/ODIHR International Election Observation Mission, Republic of Moldova, Parliamentary Elections, 28 September 2025, Statement of Preliminary Findings and Conclusions.

van case is therefore doubly instructive: it demonstrates both the unprecedented intensity that Russian electoral FIMI has reached and the fact that a coordinated whole-of-society response can absorb it. It also demonstrates something less comforting, examined in the final part of this section: the operation did not end on election day.

The operational ecosystem

Four distinct but complementary Russian campaigns structured the interference effort, each with a recognisable signature.

Operation Overload / Matryoshka specialises in impersonation and saturation. NewsGuard documented 39 fabricated stories targeting Moldova between mid-April and mid-July 2025 alone, produced as fake video news reports and articles mimicking 23 legitimate media outlets, including the BBC and purported Bellingcat investigations; in the entire preceding year the campaign had not targeted Moldova at all.[45] The pivot began within days of parliament setting the election date in April 2025, an indication of centralised tasking rather than organic drift. A characteristic Overload technique is emailing fabricated content directly to fact-checkers and newsrooms, a deliberate resource-exhaustion tactic aimed at overwhelming the verification capacity of the defending side. Typical narratives accused President Maia Sandu and her entourage of corruption, embezzlement, drug addiction, and mental illness, with the top five false claims gaining nearly 1.5 million views on Telegram between April and July.[46]

Storm-1516 followed its established playbook of seeding fabricated stories on cloned or inauthentic "local news" websites and producing likely AI-generated videos, which were then amplified through networks of X accounts, some of them verified. Its Moldova-related output focused on discrediting Sandu and PAS and on framing NATO as a threat to the country.[47]

Operation Undercut, linked to the sanctioned Social Design Agency structures, produced localised video content with AI-generated voiceovers and imagery, dressed up with screenshots of mainstream media and infographics to simulate credibility. Its defining feature in the Moldovan campaign was resilience: when its dedicated X network was removed on 22 September, days before the vote, a replacement network was active within 24 hours.[48]

Portal Kombat (the "Pravda" network) functioned as a redistribution layer, translating content from Russian state media and Kremlin-affiliated Telegram channels and republishing it across dozens of websites posing as local outlets.[49]

These external operations rested on a domestic proxy layer: the Shor-linked paid-influencer networks, Kremlin-aligned Telegram ecosystems (Sputnik Moldova and its clones, Gagauz-focused channels, Transnistrian outlets), and politically aligned commentators who translated strategic narratives into locally resonant grievances. This division of labour, with foreign infrastructure producing content and local intermediaries supplying authenticity and reach, is consistent with the proxy architecture described in the conceptual framework of this report.

AI-enabled manipulation

Moldova in 2025 offers one of the clearest documented cases to date of generative AI moving from the margins of an influence operation to its production core. Across the EEAS monitoring perimeter, 27 percent of all FIMI incidents recorded in 2025 involved artificial intelligence, whether AI-generated text, synthetic audio, or manipulated video, and the EEAS assessed that these tools had shifted from experimental to routine deployment.[50] The Moldovan campaign illustrated each of these uses. The most visible incidents were

45 NewsGuard, "Russia's Matryoshka Propaganda Machine Picks New Target, Pushing 39 False Claims Against Moldova Over Past Three Months," July 2025, https://www.newsguardtech.com/special-reports/russia-matryoshka-propaganda-moldova/

46 NewsGuard, "Russia's Matryoshka Propaganda Machine Picks New Target, Pushing 39 False Claims Against Moldova Over Past Three Months," July 2025, https://www.newsguardtech.com/special-reports/russia-matryoshka-propaganda-moldova/

47 G7 Rapid Response Mechanism, Joint Monitoring of 2025 Moldovan Parliamentary Elections, https://international.canada.ca/en/global-affairs/corporate/reports/rapid-response-mechanism/news/2025-moldovan-election

48 Ibid

49 Recorded Future (Insikt Group), Russian Influence Assets Converge on Moldovan Elections, September 2025, https://www.recordedfuture.com/research/russian-influence-assets-converge-on-moldovan-elections

50 EEAS, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards, March 2026, https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

deepfakes of President Sandu. Weeks before the vote, a mocking video created with the commercial tool Luma AI portrayed her rapping in Russian about her own ineffectiveness; investigators at The Insider and the Antibot4Navalny collective attributed it to the Matryoshka operation.[51] Recorded Future's Insikt Group documented a companion technique: deepfakes of government spokesperson Daniel Vodă, built by repurposing authentic press footage and overlaying AI-generated audio, designed to create a closed loop in which fabricated "official statements" appeared to confirm earlier fabricated news items.[52] Fabricated video news reports impersonating Euronews, Deutsche Welle, and the BBC carried AI-generated voiceovers and falsified graphics, including invented approval-rating charts attributed to legitimate statistics portals.[53]

Monitoring data collected for this project (LetsData M-Mind)[54] captured a further stage in this evolution: the fusion of AI-generated content with automated amplification into a single hybrid tactic. Between 24 and 29 September 2025, spanning election day itself, an AI-generated YouTube "satire" video attacking Sandu and Western support for Moldova was promoted across 25 pro-Russian, Russian-language Telegram channels by a network of 65 bot accounts, which produced 80 posts and 5,310 comments. Individual bots posted up to four comments per minute, with up to ten bots converging on a single thread, and the comments themselves were AI-generated, echoing the video's themes and redirecting audiences to YouTube. The narratives followed the standard strategic repertoire: the West imposes external control, Sandu enforces authoritarian justice, EU ties bring moral corruption, Moldova is being turned into a "new trench" of the war. Two features of this incident deserve emphasis. First, the satirical framing functioned as narrative laundering, allowing overtly political content to evade both platform moderation and audience scepticism. Second, the source channel itself had negligible organic reach (68 subscribers); the operation's entire footprint was manufactured, demonstrating how cheaply AI content plus botnet distribution can now simulate a public conversation.

The strategic logic of AI use in Moldova was less about persuading voters of specific falsehoods than about volume, plausibility, and cost. Generative tools allowed the operations to produce localised content in Romanian, Russian, and Gagauz at a tempo that manual production could not sustain, and to keep fact-checkers permanently on the defensive. Even crude fakes served the "firehose" function described earlier in this report: saturating the environment until audiences disengage from verification altogether.

After the vote: pivoting to institutional delegitimisation

A central finding of this research, drawn from post-election monitoring data (LetsData M-Mind, October to December 2025), is that the defeat of Kremlin-aligned forces at the ballot box did not end the operation. It changed its target. Having failed to swing the vote, the same actor ecosystem redirected its output from electoral persuasion to the delegitimisation of the institutions the election had produced, in effect contesting the result retroactively and pre-positioning grievance narratives for future cycles.[55]

Several coordinated incidents from this period illustrate the pattern.

Post-election integrity attacks. On 5 November, the Facebook page Democrația Acasă published an anecdotal, single-source claim that overseas electoral staff had received cash bribes in envelopes. One post, corroborated by nothing, reached roughly 97,000 views with over 700 shares, exploiting the diaspora's decisive electoral weight to seed durable doubt about the overseas vote.[56]

51 Euronews, "Online disinformation intensifies ahead of Moldovan parliamentary elections," 3 September 2025, https://www.euronews.com/my-europe/2025/09/03/online-disinformation-intensifies-ahead-of-moldovan-parliamentary-elections; The Insider / Antibot4Navalny attribution as reported therein.

52 Recorded Future (Insikt Group), Russian Influence Assets Converge on Moldovan Elections, September 2025, https://www.recordedfuture.com/research/russian-influence-assets-converge-on-moldovan-elections

53 Recorded Future (Insikt Group), Russian Influence Assets Converge on Moldovan Elections, September 2025, https://www.recordedfuture.com/research/russian-influence-assets-converge-on-moldovan-elections

54 https://letsdata.net/

55 Project monitoring data: LetsData M-Mind intelligence subscription, incident reports and weekly information space overviews, Moldova, September–December 2025. Incident metrics cited in the text (post counts, actor counts, views, shares, timing) are drawn from this dataset.

56 https://letsdata.net/resources/case-studies

Manufactured minority-persecution campaigns. On 13 November, the Sputnik Moldova ecosystem (including its post-ban clone channels) ran a tightly coordinated campaign alleging that two Russian-aligned MPs, Lashchenova and Petrovich, had been excluded and mistreated during parliamentary debates. Monitoring identified 45 posts built from roughly 15 template texts, published by 22 actors within minutes of each other, reaching about 38,500 views. The same week, the government's termination of the agreement on Russian cultural centres triggered a larger outrage wave: 172 posts across Telegram, Facebook, Instagram, and YouTube, some 172,000 views, framing the closure of the Russian House in Chișinău as "russophobic" repression dictated by Brussels. Both campaigns worked the same seam: recasting routine institutional decisions as ethnic persecution in order to polarise Russian-speaking audiences against the state.

Real-time conspiracy seeding around security incidents. When a Russian Gerbera drone crashed in Florești district on 25 November, malign channels launched two mutually inconsistent conspiracies within hours: that the drone was Ukrainian with false Russian markings, and that it had been "lying on the roof for two weeks," proving a staged provocation. The second claim originated in a single villager's joking remark to a local outlet at around 17:00; by 18:40 it had been converted into an assertive claim by a major malign channel, and between 18:46 and 20:35 an identical text block cascaded through more than 15 channels. Notably, elements of the staged-incident narrative were then recycled by neutral and mainstream-adjacent outlets, giving the fabrication secondary validation. The after-hours timing, outside newsroom and institutional working hours, allowed the narrative to occupy the information space uncontested overnight, a tactic that presupposes pre-planned exploitation of breaking security events.

Official Russian framing as narrative anchor. On 27 and 28 November, 25 actors across Telegram, Facebook, and Instagram amplified statements by Russian MFA spokesperson Maria Zakharova claiming that Moldova fabricates the "Russian threat," is militarising under EU and NATO pressure, and is destroying CIS ties to justify integration. A seized weapons truck at the Romanian border in September was repurposed within this storyline as "evidence" of staged anti-Russian provocations, showing how discrete incidents are stitched into a cumulative delegitimisation narrative over months.

Taken together, these incidents show volumes that are individually modest compared with the pre-election peak, but a targeting logic that is arguably more corrosive: each campaign attacks a different pillar of institutional trust (electoral administration, parliament, cultural policy, the judiciary, the security sector), and the ecosystem demonstrates persistent, disciplined coordination long after the electoral trigger has passed.

The Transnistrian dimension

The unrecognised Transnistrian region functioned throughout 2025 as both an amplifier and a mirror of the anti-Chișinău campaign. Monitoring of Transnistrian channels shows a stable narrative architecture: the self-proclaimed authorities as competent providers of stability and social care; Moldova as a "fascist," NATO-militarised, economically failing state persecuting Russian speakers and erasing Soviet memory; and Ukraine as corrupt, violent, and on the verge of collapse.

The so-called elections of 30 November 2025 in the region concentrated these dynamics. In the preceding week, four Transnistrian channels synchronously recycled an identical statement by Russian MP Sergey Mironov framing "self-determination through honest, free elections" as the region's right, appropriating democratic vocabulary to normalise separation. Between 26 and 27 November, 19 channels published 31 near-identical posts accusing Moldovan security structures of sabotaging the vote through intimidation and blackmail, complete with appeals to the OSCE to simulate due process. Around the vote itself, coverage combined saturation messaging on turnout and civic duty, preemptive attribution of any disruption to Chișinău, and endorsements by Russian politicians presented as neutral international observers, in one case validation by the "foreign ministry" of South Ossetia, another unrecognised entity. The contrast drawn was explicit: orderly Transnistrian elections against alleged Moldovan "falsifications." For Chișinău, the practical effect is a parallel information space in which Moldovan sovereignty is contested by default and every electoral cycle on either bank becomes an occasion to harden separation.

Assessment

Five conclusions follow from the Moldovan case.

First, the objective of the 2025 operation was systemic rather than electoral in the narrow sense. As Oxford's Corneliu Bjola observed of the campaign, the aim was not to shift a marginal number of votes but to erode confidence in the democratic process itself.[57] The post-election pivot to institutional delegitimisation confirms this reading empirically.

Second, AI has changed the economics of interference more than its content. The narratives deployed against Moldova in 2025 were largely traditional; what was new was the cost structure. Deepfakes, synthetic voiceovers, AI-written comments, and cloned news sites allowed a saturation-level campaign to be run against a country of 2.4 million at industrial tempo, and the EEAS finding that over a quarter of all 2025 FIMI incidents involved AI indicates that Moldova is the template, not the exception.[58]

Third, the operations displayed engineered resilience. Undercut's 24-hour network reconstitution after takedown, Sputnik Moldova's numbered clone channels, and the after-hours exploitation of the Florești incident all point to adversary planning that assumes and prices in defensive countermeasures.

Fourth, effectiveness ultimately hinged on the domestic layer. Foreign-produced content achieved scale, but its credibility depended on local proxies: paid influencers, aligned politicians, regional identity entrepreneurs in Gagauzia and Transnistria. This is where Moldova's countermeasures (deregistration of Shor-linked electoral blocs, sanctions enforcement, platform escalation channels) had the most measurable effect, and where the country remains most exposed.

Fifth, Moldova's experience converges with Ukraine's core lesson: interference of this intensity cannot be fact-checked away item by item. What limited its impact was the combination of institutional preparedness, civil society monitoring capacity, platform cooperation secured in advance, and a population partially inoculated by a decade of exposure. These are the elements examined comparatively in the following chapter.

57 AFP, "Russia-linked disinfo campaign targets Moldovan election," 24 September 2025, https://www.france24.com/en/live-news/20250924-russia-linked-disinfo-campaign-targets-moldovan-election

58 EEAS, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards, March 2026, https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

Part V
Comparative analysis

Comparative Insights: Georgia vs Moldova vs Ukraine

The cases of Georgia, Moldova and Ukraine demonstrate that Russian Foreign Information Manipulation and Interference is not a collection of isolated disinformation campaigns, but a persistent regional system of influence. Across all three countries, Russia relies on a relatively stable repertoire of narratives, operational methods and amplification infrastructures. These include the portrayal of European integration as a loss of sovereignty, claims that Western governments are controlling domestic political institutions, attacks on the legitimacy of elections, and the exploitation of linguistic, religious, regional and historical divisions.

At the same time, the comparative analysis shows that the effect of Russian FIMI depends not only on the sophistication or scale of the hostile operation. It is also shaped by the political and institutional environment into which it is introduced. The same narrative can remain marginal where institutions respond rapidly and credible independent media retain public trust, but become dominant where political actors, government-aligned media or state institutions reproduce and legitimise it.[59]

The central comparative distinction is therefore the role played by the state. In Ukraine, the state functions primarily as a coordinator of resistance against Russian information operations. In Moldova, it acts as a willing counter-actor, although one constrained by limited administrative capacity, fragmented media consumption and significant linguistic and regional vulnerabilities. In Georgia, by contrast, parts of the governing and government-aligned information ecosystem have increasingly operated as amplifiers of narratives that overlap with Russian strategic messaging. This distinction substantially changes what democratic resilience can mean in each national context.

Similarities in Russian tactics

Russian operations in all three countries combine externally produced content with domestic distribution networks. The foreign layer supplies narratives, technical infrastructure, fabricated media products and strategic direction. The domestic layer provides cultural familiarity, political relevance and perceived authenticity.

This division of labour is essential to the success of contemporary FIMI. Content originating directly from Russian state media may be easily recognised as propaganda, particularly among audiences already sceptical of the Kremlin. The same claim becomes more persuasive when voiced by a local politician, journalist, commentator, religious figure, influencer or apparently independent media outlet. Russia therefore does not need to control the entire information environment. It needs access to a sufficient number of local intermediaries capable of translating strategic narratives into domestic political language.

A second similarity concerns the shift from promoting a single alternative reality to generating confusion and exhaustion. Across the three countries, Russian operations increasingly seek to make verification appear impossible. Contradictory claims are circulated in parallel, not because

59 European External Action Service, 4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats, March 2026, https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

all are expected to be believed, but because their coexistence weakens confidence in any authoritative account.

This was particularly visible in the Moldovan information response to the Russian drone crash in Florești district. Malign channels simultaneously claimed that the drone was Ukrainian and falsely marked as Russian, and that it had been planted as part of a staged provocation. The inconsistency did not weaken the campaign because the objective was not to establish a coherent explanation. It was to prevent the public from accepting the official account with confidence.

The same logic has been documented extensively in Ukraine, including around military operations, alleged mobilisation abuses, fabricated government leaks and attacks on digital public infrastructure. In Georgia, the strategy has frequently taken the form of competing allegations of foreign interference. Documented concerns about Russian influence are answered with claims that the European Union, the United States, international organisations and civil society are themselves manipulating elections and political protests. The result is a deliberate flattening of distinctions between democratic support, public diplomacy, election observation and covert foreign interference.[60]

A third common feature is the use of trusted brands and institutional identities. Impersonation has become one of the most effective techniques because it bypasses the need to build credibility from the ground up. Russian-linked operations have cloned media outlets, fabricated reports attributed to recognised broadcasters and fact-checking organisations, and produced false statements presented as coming from public institutions.

Differences in national vulnerability

Although Russian tactics are broadly transferable, the vulnerabilities they exploit differ substantially.

Ukraine's principal vulnerability is the prolonged pressure of war. Russian operations target military morale, mobilisation, trust in political and military leadership, relations between soldiers and civilians, refugee communities, and confidence in international support. The adversary can connect information manipulation directly to battlefield developments, casualties, energy disruption and social fatigue. This gives Russian narratives a continuous supply of emotionally powerful material.

At the same time, Ukraine possesses the clearest societal understanding of Russia as an aggressor. This limits the political space available to openly pro-Russian actors and increases public receptiveness to counter-disinformation measures. Ukraine's vulnerability is therefore not primarily ambiguity about the external threat. It is exhaustion, the enormous volume of hostile content and the risk that prolonged crisis conditions gradually weaken confidence in institutions.

Moldova's vulnerability is more closely linked to institutional scale, linguistic segmentation, economic insecurity and unresolved territorial fragmentation. The country has a relatively small public administration confronting an influence operation supported by the resources of a much larger state. Romanian-speaking and Russian-speaking audiences often consume different media, while Gagauzia and Transnistria possess distinctive political and information environments. These divisions allow hostile actors to tailor different messages to different communities.

The Moldovan diaspora while a strong actor for Moldova's democracy and development can also be seen as vulnerability. Because overseas voters can influence close elections, hostile actors have an incentive to spread claims about manipulated polling stations, fraudulent ballots, government pressure and preferential treatment of diaspora voters. These narratives can delegitimise results even when they fail to reduce turnout or change voting behaviour.

Georgia's most important vulnerability is political polarisation combined with the erosion of institutional consensus regarding the country's Euro-Atlantic orientation. Russian FIMI benefits from an environment in which anti-Western narratives are not confined to marginal actors but

60 European External Action Service, 2025 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference, 24 June 2026, https://www.eeas.europa.eu/eeas/2025-report-eeas-activities-counter-foreign-information-manipulation-interference-fimi_en

are incorporated into mainstream political competition.

The unresolved conflicts in Abkhazia and South Ossetia provide Russia with permanent sources of pressure. Fear of renewed war can be used to frame any stronger Western alignment as reckless or dangerous. The "second front" narrative has been particularly effective because it connects geopolitical choice with immediate physical insecurity. Rather than presenting Russia as desirable, the narrative presents accommodation with Russia as the only realistic way to preserve peace.[61]

Georgia also faces growing pressure on the independent institutions that would ordinarily detect and counter information manipulation. Civil society organisations, watchdogs, investigative journalists and election observers have been portrayed as foreign agents or political actors. This weakens their credibility, complicates their access to funding and makes their monitoring work more difficult. The vulnerability is therefore not only exposure to hostile narratives but the deliberate weakening of the domestic actors capable of challenging them.

The role of institutions and civil society

The three cases show that institutional alignment is more important than institutional size alone.

Ukraine has developed the most extensive counter-FIMI ecosystem. Government bodies, security institutions, strategic communication units, independent media, fact-checkers, technology companies and civil society organisations operate within a partially coordinated network. This system is not free of duplication, gaps or legal controversy, but it provides multiple detection and response points.

A false narrative may be identified by a monitoring company, investigated by an independent newsroom, assessed by a public authority, escalated to a digital platform and then addressed through public communication. The strength of the system lies in this redundancy. No single institution needs to identify and resolve every incident.[62]

Moldova has moved toward a similar networked model, particularly during the 2024 and 2025 electoral cycles. Public institutions cooperated with civil society monitors, international partners and digital platforms. Authorities acted against illicit financing networks, requested the removal of coordinated accounts and worked with external monitoring mechanisms. Independent organisations contributed fact-checking, investigative reporting and analysis of pro-Russian networks.

Nevertheless, Moldova's capacity remains concentrated among a relatively small number of specialised actors. This creates sustainability risks. A prolonged saturation campaign can overwhelm fact-checkers and public communication teams, particularly when hostile actors deliberately submit fabricated material to newsrooms or launch incidents outside normal working hours. Moldova therefore requires not only greater expertise but wider distribution of that expertise across regional media, local authorities, schools, election bodies and community organisations.

In Georgia, civil society and independent media remain the principal sources of counter-FIMI capacity, but they operate in an increasingly restrictive environment. The absence of a state-led counter-disinformation consensus means that civil society cannot rely on access to government information, coordinated public communication or unified platform escalation channels. In some cases, the state itself is part of the problem being monitored.

This creates a different model of resilience. Rather than a whole-of-government or whole-of-society framework, the immediate priority becomes the preservation of independent analytical capacity. Georgian organisations need secure funding, legal support, digital protection, access to international verification networks and mechanisms for documenting coordinated manipulation. Their role is not limited to correcting false claims.

61 Digital Forensic Research Lab, "Foreign and Domestic: Information Manipulation during Elections in Georgia, Moldova, Armenia, and Azerbaijan," 31 March 2026.

62 Andrei Rusu, Andrei Curăraru and Eugen Muravschi, "The Russian Disinformation Network in Moldova: Anatomy of a Social Media Operation," WatchDog.MD, 14 August 2025.
https://watchdog.md/en/studies/208525/reteaua-rusa-de-dezinformare-in-moldova-anatomia-unei-operatiuni-pe-retelele-de-socializare/

They also preserve evidence of how narratives move between Russian sources, domestic political actors and government-aligned media.

International partnerships consequently have different functions in the three countries. In Ukraine, they supplement and connect a strong domestic ecosystem. In Moldova, they provide surge capacity, specialist expertise and technical support that a small state cannot generate alone. In Georgia, they may serve as a protective external infrastructure for civil society and independent media when domestic institutional cooperation is unavailable.

Effectiveness of countermeasures

The comparative evidence suggests that no single countermeasure is sufficient. The most effective responses combine institutional preparation, credible communication, platform cooperation, financial investigation, independent verification and public resilience.[63]

Fact-checking remains necessary but has clear limitations. It is most effective when a false claim is specific, high-impact and still limited in reach. It is less effective against high-volume campaigns designed to create general distrust. Repeating every false claim can also amplify it, while slow corrections rarely reach all audiences exposed to the original content.

Ukraine's experience demonstrates the value of selective debunking combined with broader narrative and infrastructure responses. Rather than addressing every individual post, institutions can identify recurring manipulation techniques, expose coordinated networks and provide the public with advance warning about predictable campaign themes.[64]

Moldova applied elements of this model in 2025. The removal of fake accounts, exposure of paid influencer networks and action against illicit political financing reduced the operational freedom of pro-Russian actors. The election result indicated that interference did not achieve its central strategic goal of reversing the country's European trajectory.

However, the post-election campaigns show why electoral success should not be equated with the defeat of FIMI. The operation pivoted from influencing voter choice to delegitimising the institutions produced by the election. Claims about diaspora fraud, minority persecution, parliamentary exclusion and staged security incidents continued to erode trust. Resilience must therefore extend beyond election day.

Platform takedowns also had mixed results. Moldova secured the removal of substantial numbers of accounts, but some networks were rebuilt within 24 hours. This illustrates the difference between account-level enforcement and infrastructure-level disruption. Removing individual accounts may reduce immediate reach but does not dismantle the coordinating actors, content production systems, financial incentives or alternative channels behind them.

Ukraine has faced the same problem with cloned websites and sanctioned media brands. Once one outlet is blocked, a new domain, Telegram channel or social media identity may appear almost immediately. Sustainable disruption requires coordinated action against networks rather than isolated content, including domain registrars, advertising services, payment systems and the entities managing the distribution infrastructure.[65]

Legal restrictions can be effective when narrowly tied to demonstrable harmful behaviour, such as illicit foreign financing, covert coordination, impersonation, cybercrime or undisclosed political advertising. They become more problematic when they rely on broad definitions of disinformation or national security that can also be used against legitimate journalism and political opposition.

This distinction is particularly important in Georgia. Measures officially presented as protecting sovereignty from foreign influence may in practice weaken the civil society and media organisations best equipped to identify Russian manipulation. Counter-FIMI policy must therefore be assessed not only by its declared

63 European Board for Digital Services, Report on the European Elections–Digital Services Act and Code of Practice on Disinformation, 29 July 2024, https://digital-strategy.ec.europa.eu/en/library/european-board-digital-services-publishes-post-election-report-eu-elections

64 European Commission, Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes, 26 April 2024, https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes

65 VoxUkraine, "Disinformation about Ukraine in Russian and Pro-Russian Telegram Channels."
https://narratives.voxukraine.org/en.html

purpose but by its institutional effect. A measure that reduces transparency, independent oversight or pluralism may increase vulnerability even when justified in the language of national resilience.

Overall, the cases support five comparative conclusions.

First, Russian FIMI is most effective when its narratives are adopted by domestic political actors. Direct foreign propaganda is less influential than locally legitimised manipulation.

Second, the position of the state is decisive. A state can be a counter-actor, a passive bystander or an amplifier. Technical assistance alone cannot compensate for the absence of political will.

Third, FIMI operations increasingly seek institutional exhaustion rather than immediate persuasion. Measuring success only through changes in voting behaviour misses their longer-term effects on trust, participation and democratic legitimacy.

Fourth, effective resilience is networked. Governments, civil society, independent media, researchers, election authorities and platforms each possess only part of the necessary information and capability.

Fifth, the defensive cycle must continue after elections. Post-electoral delegitimisation is not an after-effect of the campaign but an integral phase of it.

Part VI
Emerging Trends Ahead of Future Elections

The 2025 electoral cycles demonstrate that Russian information operations are entering a new phase characterised by lower production costs, faster adaptation, deeper localisation and greater integration between online and offline influence.[66]

The strategic narratives themselves are not necessarily new. Claims about Western control, national decline, cultural threat, corruption, war and electoral fraud have circulated for years. What is changing is the speed and scale at which these narratives can be produced, adapted and distributed.

AI-generated and synthetic content

Generative artificial intelligence is reducing the cost of producing convincing text, audio, images and video in multiple languages. This enables hostile actors to generate large quantities of localised content without maintaining extensive teams of native speakers, editors and video producers.

The Moldovan election illustrated this transition particularly clearly. AI-generated voiceovers, fabricated news reports, synthetic videos and automated comments were integrated into coordinated campaigns. Content could be adapted for Romanian-speaking, Russian-speaking and regional audiences while maintaining a consistent strategic narrative.

Future elections are likely to encounter a growing number of fabricated statements attributed to candidates, election officials, journalists and foreign leaders. Synthetic audio may be particularly disruptive because it is cheaper to produce than high-quality video and can be distributed rapidly through messaging applications. A short audio recording released shortly before voting could falsely suggest that a candidate admitted to corruption, planned electoral fraud or made a controversial private statement.[67]

The most dangerous incidents may combine synthetic content with cyber intrusion or impersonation. A fabricated video becomes more credible when uploaded to a compromised media account, displayed on a hacked website or distributed from an official-looking institutional channel. This convergence reduces the time available for verification and increases the likelihood that mainstream outlets will reproduce the material before its authenticity is established.

At the same time, the growing public awareness of deepfakes creates the opposite risk: authentic evidence may be dismissed as AI-generated. Political actors can exploit uncertainty by claiming that genuine recordings, documents or images are synthetic. This “liar’s dividend” may ultimately be more damaging than individual deepfakes because it weakens the evidentiary value of all digital content.[68]

Responses will therefore need to focus not only on detecting manipulation but on establishing trusted systems of provenance, authentication and rapid verification. Election bodies, political parties, media or-

66 European External Action Service, 4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats, March 2026.
67 European Commission, Guidelines for Providers of VLOPs and VLOSEs on the Mitigation of Systemic Risks for Electoral Processes, 26 April 2024.
68 Robert Chesney and Danielle Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,” California Law Review, Vol. 107, No. 6, 2019, pp. 1753–1820, https://californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security

ganisations and public authorities should prepare procedures for confirming or denying disputed content within hours rather than days.

Automated amplification and synthetic engagement

AI is also transforming amplification. Bot networks no longer need to repeat identical messages that can be detected through simple text matching. Generative models can produce thousands of semantically similar but linguistically distinct comments, creating the appearance of organic public reaction.

This was visible in the Moldovan Telegram ecosystem, where automated accounts generated varied comments, redirected users toward external content and simulated broad agreement with anti-government narratives. Similar techniques have been used in Ukraine to create the impression of mass dissatisfaction with mobilisation, military leadership and public institutions.

Synthetic engagement affects public perception even when users do not believe the underlying claim. Large numbers of comments, shares and reactions function as social proof. They can make marginal positions appear mainstream, intimidate journalists or activists, and influence editorial decisions by creating the impression that a particular issue is dominating public debate.

Future detection systems will therefore need to assess behavioural coordination rather than only content similarity. Timing, account creation patterns, posting frequency, shared links, interaction structures and cross-platform movement may provide stronger indicators than the wording of individual posts.

Micro-targeting and audience segmentation

Russian campaigns are likely to become increasingly segmented. Rather than disseminating one national narrative, operators can tailor different messages to narrow groups based on language, region, age, economic status, religious identity, political preference or media consumption pattern.[69]

In Moldova, one campaign can simultaneously tell pro-European voters that the government is failing to deliver reform, Russian-speaking communities that they face cultural repression, Gagauz audiences that autonomy is under threat, and diaspora voters that the election process is manipulated. These narratives may contradict one another, but they are delivered to audiences unlikely to compare them directly.

In Georgia, urban liberal audiences may be targeted with cynicism about the effectiveness of European support, while conservative or rural audiences receive narratives about cultural values, foreign-funded activism and the risk of war. In Ukraine, military families, refugees, residents of frontline regions and citizens affected by mobilisation can each be targeted with distinct emotional triggers.

The availability of commercially collected behavioural data, leaked databases and platform advertising tools may increase the precision of such targeting. Even where foreign actors cannot directly purchase political advertisements, domestic proxies can perform the same function. Closed messaging groups and influencer networks further reduce transparency because outside researchers may not see the content being delivered.[70]

Election monitoring will therefore need to move beyond nationally visible media. Researchers must examine regional channels, private or semi-private communities, minority-language spaces, influencer networks and political advertising repositories. Civil society organisations should also develop partnerships with community-level actors who can identify narratives circulating outside mainstream monitoring systems.

Platform governance gaps

Platform governance remains weakest precisely where hostile actors are most active: smaller language markets, messaging applications, short-form video platforms and rapidly changing networks of cloned accounts.[71]

69 European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, Version 2.0, 13 April 2021, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-082020-targeting-social-media-users_en

70 NATO Strategic Communications Centre of Excellence, Social Media Manipulation Reports and related research on coordinated inauthentic behaviour, https://stratcomcoe.org/publications

71 European Commission, “Guidelines under the Digital Services Act–Electoral Processes,” updated 2026, https://digital-strategy.ec.europa.eu/en/policies/dsa-guidelines

Content moderation in Georgian, Romanian, Russian, Ukrainian and Gagauz remains inconsistent. Automated moderation systems often perform less effectively outside major global languages, while human review teams may lack cultural and political context. Satire, coded language and local references can be used to avoid enforcement.

Telegram presents a particular challenge because of its combination of public channels, private groups, weak transparency and limited cooperation with researchers and authorities. TikTok offers enormous reach and algorithmic amplification but can be difficult to monitor systematically. YouTube provides a durable hosting environment for videos that are then promoted through other platforms. X remains useful for creating the appearance of international visibility and for laundering fabricated stories through networks of verified or apparently credible accounts.[72]

Operations increasingly distribute different components of the same campaign across platforms. A fake story may originate on a cloned website, be summarised in a Telegram post, converted into a short TikTok video, amplified through X accounts and discussed in AI-generated YouTube comments. Removing one component leaves the wider system intact.

Future platform cooperation should therefore be organised around incidents and networks rather than individual posts. A designated national coordination mechanism should be able to provide platforms with structured evidence showing how accounts, websites and content assets are connected. Platforms should, in turn, provide sufficiently detailed information about enforcement actions to allow national authorities and researchers to understand whether the underlying network has been disrupted.

Hybrid online and offline influence

Online manipulation is increasingly connected to offline political activity. Paid influencers, organised protests, vote-buying schemes, political financing, cultural organisations, religious networks and local community structures can all serve as distribution channels.

Moldova's experience with Shor-linked networks showed how financial incentives can transform ordinary citizens into participants in a coordinated information operation. Individuals may be paid to post content, administer groups, attend protests or recruit others. The resulting activity appears local and spontaneous even when its organisation and financing are external.

Georgia demonstrates a different form of hybridity, in which government rhetoric, legislation, political mobilisation and media narratives reinforce one another. Online claims about foreign agents or Western interference can prepare public opinion for restrictive measures against civil society. Those measures then reduce the capacity of independent actors to expose future manipulation.

Ukraine illustrates the most extreme integration of information activity with military and cyber operations. False claims may support battlefield objectives, undermine mobilisation, collect personal data or prepare targets for phishing and recruitment attempts.

These cases suggest that election-security structures should include financial intelligence, cybersecurity, law enforcement, media regulators and civil society monitors. A campaign cannot be fully understood if each institution examines only its own component.

Post-election delegitimisation as a permanent phase

A further trend is the extension of electoral interference beyond the campaign period. When preferred actors lose, hostile networks do not necessarily disengage. They shift from influencing voter choice to disputing the legitimacy of the result and obstructing the institutions that follow from it.[73]

The Moldovan post-election monitoring provides a clear example. Narratives about diaspora fraud, persecution of Russian-speaking politicians, manipulation by Brussels and staged security incidents continued after the vote. Each cam-

72 European Board for Digital Services, Report on the European Elections–Digital Services Act and Code of Practice on Disinformation, 29 July 2024.

73 European Commission, Guidelines for Providers of VLOPs and VLOSEs on the Mitigation of Systemic Risks for Electoral Processes, 26 April 2024.

paign targeted a separate institution, but together they promoted the conclusion that the new parliamentary majority lacked legitimate authority.

Comparable tactics are visible in Georgia, where allegations of Western interference are used to delegitimise opposition mobilisation, civil society monitoring and international criticism. In Ukraine, elections have been postponed under martial law, but similar narratives target the legitimacy of political leadership and imply that the absence of voting makes the state inherently authoritarian.

Future resilience planning should therefore cover the entire electoral cycle: candidate selection, campaigning, voting, counting, government formation, post-election protests and the first months of the new administration. Monitoring capacities that are dismantled immediately after election day leave institutions exposed during a period when hostile actors may be seeking to turn political disappointment into sustained distrust.

The information layer of artificial intelligence

An emerging longer-term risk is the manipulation of the information sources used by AI assistants and search systems. Networks such as Portal Kombat publish large volumes of repetitive, multilingual content across apparently independent websites. While much of this material attracts limited direct readership, it may influence the datasets and retrieval systems used by generative AI tools.

As citizens increasingly use chatbots to obtain information about elections, candidates, wars and international organisations, hostile actors may attempt to ensure that manipulated narratives appear repeatedly in the underlying information environment. This could cause AI systems to reproduce false claims, present fringe narratives as widely reported, or cite inauthentic websites as legitimate sources.[74]

Smaller language environments may be particularly vulnerable because fewer high-quality sources are available to outweigh coordinated propaganda. Georgian, Romanian and Ukrainian responses generated by AI systems may be less reliable than English-language outputs, especially on politically contested topics.

Countering this threat will require investment in authoritative local-language public information, open datasets, high-quality journalism and systematic exposure of coordinated propaganda networks. Governments and civil society should also regularly test major AI systems on election-related questions in relevant languages to identify recurring errors or contaminated sources.

74 European External Action Service, 4th EEAS Annual Report on FIMI Threats, March 2026.

Part VII Recommendations and conclusions

Policy recommendations

The cases of Georgia, Moldova and Ukraine demonstrate that Russian Foreign Information Manipulation and Interference cannot be addressed through isolated communication campaigns or short-term electoral support. It is a persistent form of hybrid interference combining information manipulation with cyber operations, covert financing, political proxies, economic pressure and efforts to weaken independent institutions.

The European Union already possesses an increasingly comprehensive policy framework in this area. The European Democracy Shield, the EU Rapid Alert System, the Digital Services Act, the European Cooperation Network on Elections and the EEAS FIMI methodology provide important foundations for detecting and responding to information manipulation. The establishment of the European Centre for Democratic Resilience offers an additional opportunity to connect EU institutions, Member States and civil society.

However, the experience of the 2025 elections shows that existing instruments must be applied more systematically beyond the EU's borders, particularly in candidate countries exposed to sustained Russian interference. Moldova, Georgia and Ukraine should not be treated merely as recipients of external assistance. They are part of the wider European democratic and information-security environment. Manipulation techniques tested in these countries are frequently redeployed against EU Member States, while hostile networks operate across national borders and digital platforms.

EU action should therefore pursue the following reinforcing objectives:

EU support should move from temporary election-observation and crisis-response missions toward permanent electoral-resilience partnerships with Moldova, Georgia and Ukraine. These partnerships should operate throughout the electoral cycle rather than being activated only shortly before voting.

Establish permanent EU election-resilience partnerships with candidate countries

Each partnership should bring together the relevant EU Delegation, the EEAS, the European Commission, national election authorities, cybersecurity bodies, strategic communication institutions, civil society monitors, independent media and digital-platform representatives. The objective should be to develop a shared operational picture, identify predictable vulnerabilities and agree response procedures before a crisis occurs.

The partnerships should include:

- joint risk assessments conducted at least twelve months before major elections;
- national maps of vulnerable audiences, information channels and proxy networks;
- pre-agreed procedures for escalating high-risk incidents to digital platforms;
- secure channels for exchanging evidence concerning coordinated campaigns;
- simulation exercises covering deepfakes, cyber-enabled leaks, political-financing scandals and attacks on electoral infrastructure;
- post-election monitoring extending through government formation and the first months of the new administration.

The EU's existing Rapid Alert System facilitates information exchange among EU institutions and Member States. Its benefits should be extended more consistently to candidate countries through structured partner arrangements, while respecting requirements for security, attribution and sensitive information.

Moldova should be prioritised for a fully developed partnership because of the demonstrated scale of Russian interference and the country's willingness to cooperate. Ukraine should be integrated as both a beneficiary and a provider of expertise, particularly in monitoring, cyber-FIMI convergence and rapid public communication.

In Georgia, cooperation with state authorities should be conditional on genuine institutional commitment to electoral integrity, pluralism and independent oversight. Where this commitment is absent, the EU should redirect support toward election monitors, independent media, researchers, professional associations and civil society organisations rather than suspending resilience assistance altogether.

Differentiate EU support according to the role of the national government

The comparative findings show that the same model of technical assistance cannot be applied uniformly. The EU should distinguish between governments acting as counter-actors, governments with limited capacity and governments or governing ecosystems that amplify hostile narratives.

In Moldova, the government has demonstrated political willingness to counter Russian interference but faces major capacity constraints. EU assistance should therefore focus on increasing institutional depth, regional reach, linguistic coverage and operational sustainability. Moldova requires not only centralised expertise in Chișinău but also trained local authorities, regional journalists, community organisations and public communicators capable of responding in Romanian, Russian and Gagauz.

In Ukraine, EU assistance should support the institutionalisation of a highly developed but sometimes fragmented resilience ecosystem. Priority should be given to common incident taxonomies, interagency procedures, secure information exchange, long-term funding and the integration of Ukrainian expertise into European mechanisms.

In Georgia, EU policy should avoid treating government institutions as neutral partners where evidence indicates that official actors are reproducing narratives aligned with Russian strategic interests or restricting independent watchdogs. Funding or technical cooperation involving public authorities should be accompanied by measurable conditions relating to media freedom, civil-society participation, electoral transparency and the protection of independent monitoring.

This differentiation is essential because resources intended to strengthen resilience could otherwise reinforce institutions that contribute to information manipulation or use counter-disinformation language to suppress criticism.

Integrate FIMI resilience more firmly into the EU accession process

The ability to resist foreign interference should be treated as a practical component of democratic preparedness for EU membership. It intersects with the rule of law, electoral integrity, media freedom, cybersecurity, public administration and alignment with the EU's Common Foreign and Security Policy.

The Commission should incorporate clearer FIMI-related benchmarks into annual enlargement assessments. These benchmarks should evaluate not only the existence of strategies or institutions, but also their operational independence, effectiveness and respect for fundamental rights.

Relevant indicators could include:

- the existence of transparent coordination mechanisms for electoral threats;
- the independence and capacity of election-management bodies;
- enforcement against illicit foreign and political financing;
- transparency of political advertising and campaign expenditure;
- access to public information for independent media and civil society;
- protection of journalists, researchers and election observers;
- cooperation with platforms during electoral periods;
- public reporting on major FIMI incidents;
- safeguards preventing counter-disinformation powers from being used against legitimate political speech.

For Moldova and Ukraine, progress in these areas should unlock additional technical assistance, participation in EU networks and access to specialised funding. For Georgia, deterioration in media freedom, civic space or election monitoring should have direct consequences within the accession and financial-assistance framework.

Conditionality should be targeted and reversible. The EU should avoid measures that punish the wider population or weaken pro-democratic actors. Where government-level assistance is suspended or reduced, corresponding support to independent media, municipalities, universities and civil society should increase.

Extend the practical reach of the Digital Services Act to candidate-country elections

The Digital Services Act requires very large online platforms and search engines to assess and mitigate systemic risks, including risks to electoral processes. The Commission's election guidelines recommend election-specific risk mitigation, cooperation with authorities and civil society, incident-response mechanisms, measures addressing generative AI and post-election reviews.

Although Moldova and Georgia are not EU Member States, the platforms used in their elections are largely the same platforms operating within the EU. Campaigns targeting candidate countries can also reach EU-based diaspora communities, use infrastructure hosted in the Union and form part of broader cross-border influence operations.

The Commission should therefore encourage designated platforms to apply DSA-equivalent election-integrity measures voluntarily and consistently in candidate countries.

This should include:

- country-specific risk assessments ahead of elections;
- adequately staffed moderation teams with relevant language expertise;
- direct escalation channels for election authorities and trusted civil-society organisations;
- monitoring of coordinated inauthentic behaviour across borders;
- preservation and controlled access to data for independent researchers;
- transparency concerning political advertising, influencers and paid content;
- rapid action against impersonation of media, election bodies and public officials;
- post-election assessments covering network reconstitution and institutional-delegitimisation campaigns.

The EU should make platform participation in these arrangements a recurring component of high-level dialogue under the Democracy Shield and the European Centre for Democratic Resilience.

Particular attention should be given to smaller languages and regional information environments. Platforms should be required, or strongly encouraged where EU law does not directly apply, to demonstrate that their moderation, risk-assessment and crisis-response capacity is effective in Romanian, Georgian, Ukrainian, Russian and relevant minority languages.

The EU should also evaluate platforms on their ability to disrupt networks rather than merely remove individual accounts. Moldova's experience showed that takedowns can be followed by rapid network reconstruction. Enforcement metrics should therefore include the persistence of the disruption, the removal of coordinating assets and whether the same operators are able to reappear under new identities.

Create a standing EU rapid-support mechanism for high-risk elections

The EU should establish a deployable electoral-resilience support capacity for candidate countries and other vulnerable partners. This could build on the European Democracy Shield, the European Centre for Democratic Resilience, EEAS FIMI expertise, EU Hybrid Rapid Response Teams and existing election-cooperation mechanisms. The Democracy Shield already promotes a society-wide approach connecting information integrity, resilient institutions, free elections and independent media.

The mechanism should be available several months before an election and remain active during the post-election period. It should not replace national responsibility, but provide temporary surge capacity in areas where smaller administrations can be overwhelmed.

Deployable support could include:

- multilingual monitoring analysts;
- open-source intelligence and network-analysis specialists;
- forensic support for suspected deepfakes and synthetic audio;
- cybersecurity experts able to assess hybrid cyber-FIMI incidents;
- legal experts on political financing and platform regulation;
- strategic communication advisers;
- secure technical infrastructure;
- assistance in documenting evidence for sanctions or criminal investigations.

The mechanism should include a twenty-four-hour contact point during the most sensitive electoral period. The Moldovan Florești incident demonstrated how quickly fabricated explanations can dominate the information environment when institutions and newsrooms are operating outside normal working hours.

The EU should develop clear activation criteria based on threat assessments, requests from national authorities or credible warnings from election observers and civil society. In politically captured environments, support should be deliverable to independent election-monitoring coalitions without requiring full cooperation from the national government.

Provide long-term core funding for independent media and civil society

Independent media, fact-checkers, investigative journalists and monitoring organisations function as democratic security infrastructure. Yet EU support is often delivered through short projects tied to individual elections, specific activities or donor visibility requirements.

This model is poorly suited to confronting persistent and adaptive influence operations. Organisations need stable staff, secure technology, regional networks, legal protection and the capacity to monitor between elections. Project-based funding can create gaps precisely when hostile networks are regrouping and developing new tactics.

The EU should establish multiannual funding windows for organisations working on information integrity, investigative journalism, election observation, media literacy and digital rights. Funding should cover institutional costs, cybersecurity, staff retention, legal assistance and emergency relocation where necessary.

In Moldova, support should prioritise regional and minority-language media, including outlets serving Russian-speaking and Gagauz audiences. The objective should not be to replace one form of propaganda with pro-EU messaging, but to expand access to credible, locally relevant reporting on public services, economics, identity and international relations.

In Georgia, support should include legal-defence funds, cybersecurity assistance, alternative funding channels and mechanisms to protect organisations facing politically motivated restrictions. The EU should also support exiled Georgian journalists and media outlets where continued domestic operation becomes impossible.

In Ukraine, assistance should reinforce the long-term sustainability of organisations that have developed advanced monitoring, fact-checking and open-source intelligence capabilities under wartime conditions.

Support should be distributed transparently and through multiple intermediaries to reduce the risk that the closure or targeting of one organisation disrupts the wider resilience ecosystem.

Strengthen enforcement against the financial and operational infrastructure of FIMI

The EU should focus more strongly on the infrastructure enabling foreign interference. Removing content after publication is less effective than disrupting the financing, coordination, distribution and technical services behind sustained campaigns.

EU institutions and Member States should improve cooperation in identifying:

- companies financing or managing influence operations;
- advertising and payment services used by sanctioned actors;
- domain registrars and hosting providers supporting cloned media sites;
- intermediaries facilitating covert political funding;
- individuals recruiting and paying domestic influencers;
- organisations involved in coordinated impersonation or cyber-enabled manipulation;
- assets and networks linked to already sanctioned Russian entities.

The EEAS already supports attribution, international coordination and restrictive measures against actors responsible for FIMI and destabilising activities. These instruments should be applied more rapidly and connected more systematically to evidence collected by partner-country institutions and independent researchers.

Sanctions should target clearly attributable behaviour and operational support rather than broad categories of speech. Potential measures could include asset freezes, travel restrictions, prohibitions on providing advertising or hosting services, and restrictions on companies demonstrably supporting covert influence operations.

The EU should also assist Moldova, Georgia and Ukraine in strengthening financial-investigation capacity. Illicit political financing, paid influencer networks and organised mobilisation should be examined as part of the same interference ecosystem rather than as unrelated electoral offences.

Evidence-sharing arrangements should be developed so that information gathered by civil society can, subject to verification and procedural safeguards, contribute to administrative, sanctions or criminal processes.

Treat cyber operations and FIMI as a single operational continuum

The EU's institutional response still risks separating information manipulation, cybersecurity, political financing and physical security into different policy communities. Russian operations deliberately cross these boundaries.

A hacked account can distribute a deepfake. A phishing campaign can use a fabricated government notice. A leaked database can be manipulated to undermine trust in state institutions. A cyberattack on election infrastructure can be accompanied by narratives claiming that the authorities are concealing fraud.

EU-supported assessments and exercises should therefore examine complete hybrid incidents rather than treating the information and technical components separately.

The EU should promote joint national structures or coordination cells involving:

- election-management authorities;
- cybersecurity agencies and computer-emergency-response teams;
- law enforcement;
- financial intelligence;
- strategic communication institutions;
- media regulators;
- data-protection authorities;
- independent technical experts and civil society monitors.

Common incident-reporting formats should capture both the technical and informational dimensions of an operation. This would facilitate comparison across countries and strengthen compatibility with EEAS FIMI reporting and European cybersecurity mechanisms.

Moldova should receive continued support through the EU Partnership Mission and other instruments aimed at strengthening resilience against hybrid threats. The mission's experience could also inform lighter, civilian technical arrangements for other candidate and partner countries.

Develop an EU framework for AI-enabled electoral interference

The 2025 elections demonstrated that generative AI has become a routine component of influence operations. EU policy should address not only high-quality deepfakes but the full range of AI-enabled manipulation: automated text production, synthetic voiceovers, cloned news reporting, bot-generated comments, multilingual localisation and the contamination of AI retrieval systems.

The EU should develop a dedicated protocol for AI-related electoral incidents under the Democracy Shield and DSA election framework.

This should clarify:

- how disputed audio and video can be rapidly authenticated;
- which institutions are responsible for public confirmation;
- how platforms should label, restrict or preserve synthetic content;
- how evidence should be shared with journalists and election bodies;
- how AI-generated content used for satire or impersonation should be assessed;
- how to respond when authentic material is falsely dismissed as AI-generated.

Political parties and election candidates should be encouraged to register official digital channels and provide authenticated reference material that can assist rapid verification. Election authorities should establish public channels where disputed content can be submitted and assessed.

The EU should also support regular testing of major AI assistants in Georgian, Romanian, Ukrainian, Russian and minority languages. These audits should examine whether systems repeat known FIMI narratives, cite cloned websites or provide materially different answers across languages.

Where systemic weaknesses are identified, the Commission should engage AI providers and search platforms to improve source quality, provenance and the visibility of authoritative local-language information.

Invest in prebunking, media literacy and trusted local communication

Public-awareness programmes should move beyond general messages advising citizens to “check the source.” Many contemporary operations imitate trusted sources, employ authentic footage or use domestic intermediaries. Citizens need to understand the techniques through which manipulation operates.

EU-funded programmes should focus on prebunking predictable tactics before election periods.

These include:

- impersonation of public broadcasters and international media;
- fake recordings released immediately before voting;
- allegations of diaspora fraud;
- claims that Western partners plan to provoke war;
- fabricated corruption investigations;
- paid influencer networks;
- coordinated efforts to portray minority communities as persecuted;
- contradictory conspiracy theories around security incidents.

Prebunking should explain the method rather than repeat every anticipated false claim. It should also direct citizens toward trusted verification channels and explain what public authorities will do when a suspected incident occurs.

Programmes should be tailored to specific audiences and delivered through credible local messengers. EU-branded communication alone may not reach audiences sceptical of European integration and can sometimes reinforce narratives of external control.

In Moldova, trusted local journalists, teachers, religious and community figures should be included, particularly in Gagauzia and Russian-speaking communities. In Georgia, independent cultural figures, regional media, professional associations and community leaders may have greater credibility than official institutions. In Ukraine, programmes should continue to address the specific vulnerabilities of military families, displaced persons, refugees and frontline communities.

Media literacy should be integrated into education and professional training, but it should not be used as a substitute for platform accountability or institutional action. Citizens cannot reasonably be expected to individually verify an industrial volume of sophisticated manipulation.

Protect electoral observation and democratic documentation

Election observation is itself increasingly targeted by FIMI. Domestic and international observers are portrayed as foreign agents, opposition activists or instruments of external interference. Weakening observers allows manipulation, campaign-finance violations and institutional abuse to proceed with less scrutiny.

The EU should treat the preservation of credible observation capacity as a strategic priority.

Support should include:

- multiannual funding for domestic monitoring organisations;
- legal and physical protection;
- cybersecurity and secure data storage;
- training in documenting online interference;
- tools for preserving digital evidence;
- rapid international publication of credible findings;
- coordination between traditional election observers and FIMI analysts.

In Georgia, where parts of civil society withdrew from or were constrained in their observation role, the EU should invest in alternative documentation structures, including regional networks, independent researchers and diaspora-based expertise.

Observation reports should systematically include information manipulation, digital campaigning, online advertising, misuse of public resources and attacks on journalists. At the same time, observers should distinguish foreign interference from legitimate partisan communication and avoid making attribution claims that exceed the available evidence.

Improve EU strategic communication without reproducing propaganda practices

The EU needs to communicate more effectively about its policies, assistance and enlargement process, but it should not imitate the manipulative methods it seeks to counter. Strategic communication must remain transparent, factual and open to criticism.

EU institutions and delegations should respond more rapidly when major false claims concern EU policies, military cooperation, accession requirements or financial assistance. Delayed responses allow narratives to consolidate and be repeated by domestic political actors.

Communication should provide concrete, locally relevant information. Abstract messages about European values are less effective than explanations of how accession, trade, infrastructure funding, energy support or regulatory reform affect people’s daily lives.

At the same time, the EU should avoid framing every criticism of European integration as Russian disinformation. Domestic grievances may be genuine even when foreign actors exploit them. Labelling legitimate concerns as manipulation can damage EU credibility and strengthen claims that Brussels seeks to suppress dissent.

The appropriate response is to distinguish between the underlying issue, which may require policy attention, and the manipulative behaviour used to exploit it.

Establish measurable objectives and evaluate impact

EU counter-FIMI initiatives should be evaluated against outcomes rather than activity levels. The number of workshops, fact-checks, communication products or accounts removed does not by itself indicate whether democratic resilience has improved.

Relevant indicators should include:

- the time between detection and coordinated response;
- the number of institutions using common reporting procedures;
- platform response times during electoral incidents;
- the persistence of networks after enforcement;
- the reach of credible local-language information;
- public awareness of manipulation techniques;
- the financial sustainability of independent monitoring organisations;
- the ability of regional and minority-language media to participate in verification networks;
- public trust in election administration;
- whether hostile narratives migrate successfully from fringe channels into mainstream political discourse.

Evaluation should also consider unintended effects. A counter-disinformation measure may remove harmful content but reduce transparency. A public debunk may inadvertently amplify a marginal claim. Support to a government institution may weaken independent oversight if the institution uses its authority selectively.

Independent evaluators and local civil society should therefore participate in assessments of EU-funded programmes.

Strategic Priorities by Country

Moldova

EU engagement with Moldova should focus on consolidating the resilience demonstrated during the 2025 parliamentary elections and converting temporary crisis arrangements into permanent national capacity. Moldova remains exposed to sustained Russian pressure through covert political financing, paid influencer networks, linguistic segmentation, Gagauz and Transnistrian information ecosystems, cyber operations and repeated efforts to delegitimise pro-European institutions. EU support should therefore continue throughout the electoral cycle and not end once voting or government formation is complete.

Priority should be given to strengthening the Centre for Strategic Communication and Countering Disinformation and its links with the Central Electoral Commission, cybersecurity bodies, financial intelligence, law enforcement, independent media and civil society monitors. These actors should use common incident-reporting standards, secure information-sharing channels and twenty-four-hour escalation procedures during sensitive periods. Regular simulations should test responses to deepfakes, hacked accounts, fabricated leaks, vote-buying allegations, diaspora-fraud narratives and security incidents exploited outside normal working hours.

The EU should expand credible information and monitoring capacity beyond Chișinău. Multiannual support is needed for regional, Russian-language and Gagauz media, local journalists, community organisations and public communicators able to address everyday concerns without relying on polarising geopolitical messaging. Cooperation with platforms should include permanent Moldovan- and Russian-language contact points, transparency on political advertising and stronger disruption of networks that rapidly reconstitute after takedowns.

Finally, EU assistance should target the financial and organisational infrastructure of interference. This includes support for investigations into illicit political funding, payments to influencers, coordinated mobilisation and links between domestic proxies and sanctioned Russian actors. Moldova should also be progressively integrated into EU and Member State FIMI, election-security and hybrid-threat networks, both as a beneficiary and as a source of operational lessons from the 2024–2025 electoral cycles.

Georgia

EU policy toward Georgia should place the preservation of independent democratic infrastructure at its centre. The principal challenge is not only foreign manipulation, but the convergence between Kremlin-compatible narratives and the communication of domestic governing and government-aligned actors. Where state institutions portray civil society, independent media, election observers and Western partners as agents of destabilisation, conventional government-led counter-FIMI assistance risks strengthening the very structures that contribute to democratic erosion.

Government-level cooperation should therefore be conditional on measurable commitments to media freedom, electoral transparency, independent observation, access to public information and meaningful participation by civil society. EU accession reporting and financial assistance should assess whether state institutions act as counter-actors, passive bystanders or amplifiers of hostile narratives. Where safeguards are not met, assistance should be redirected toward independent media, watchdogs, researchers, universities, professional associations, regional organisations and municipalities rather than withdrawn from Georgian society altogether.

The EU should provide multiannual core funding, legal defence, cybersecurity assistance, secure data storage and emergency support for organisations documenting manipulation and electoral abuses. Particular attention should be given to regional and Georgian-language reporting, monitoring of television–Facebook amplification, preservation of digital evidence and analysis of how narratives move from Russian intelligence-linked or sanctioned sources into mainstream domestic discourse. Support should also extend to exiled journalists and organisations if continued operation inside Georgia becomes impossible.

Strategic communication should address the fear-based narratives most relevant to the Georgian context, especially claims that European integration will provoke war or create a "second front". Responses should be factual, locally grounded and delivered through credible Georgian messengers rather than framed as external counter-propaganda. The EU should maintain visible engagement with Georgian citizens, students, journalists, local communities and businesses even when political relations with the government deteriorate, thereby avoiding the perception that Europe is disengaging from the country as a whole.

Ukraine

The EU should recognise Ukraine not only as the principal target of Russian information warfare, but also as a leading source of operational expertise. Ukrainian public institutions, technology companies, investigative media and civil society organisations have developed advanced capabilities in narrative monitoring, open-source investigation, bot-network detection, rapid verification and the analysis of combined cyber and information incidents. These capabilities should be integrated into European training, exercises, research networks and the future work of the European Centre for Democratic Resilience.

EU support should help institutionalise Ukraine's networked resilience model. Priorities include renewed national information-security and cybersecurity strategies, a common FIMI incident taxonomy, formal interagency procedures, secure signal-sharing and clearer divisions of responsibility among strategic communication, security, cyber, regulatory and law-enforcement bodies. Assistance should preserve the human-centred character of the system: AI can identify anomalies and cluster narratives, but attribution, legal assessment and public response must remain subject to authorised human judgement and democratic oversight.

Long-term support is also required for independent media, fact-checkers, OSINT organisations and Ukrainian monitoring technology providers operating under wartime pressure. Funding should cover institutional sustainability, staff retention, cybersecurity, access to data and cooperation with platforms, rather than only short-term communication projects. The EU should facilitate partnerships through which Ukrainian tools and practices can be adapted for Moldova, Member States and other vulnerable partners.

At the same time, the transfer of Ukrainian experience must distinguish between wartime and peacetime measures. Restrictions justified by armed aggression cannot automatically be replicated in candidate countries or EU Member States. The EU should draw on Ukraine's operational strengths–rapid detection, distributed verification, prebunking and cyber-FIMI integration–while retaining proportionate legal safeguards, media pluralism and fundamental-rights protections. Ukraine's future integration into EU democratic-resilience structures should therefore be reciprocal: Europe supports Ukrainian capacity, while Ukrainian expertise strengthens Europe's collective defence against FIMI.

Ballots Under Pressure:

Russian Information Manipulation in 2025 Elections in Georgia and Moldova