EPIS Thinktank

ARTIFICIAL INTELLIGENCE & CYBERSECURITY

Hana Popelisova & Edoardo Barca

Reflexive Control Russian AI and Hybrid Warfare

How the digital domain is defining post-contemporary warfare in Eastern Europe

About the Authors:

Hanka Popelisova

Hanka holds an MSc in Political Science from the University of Amsterdam and a BA in International Studies from Leiden University. Coming from Slovakia, she is passionate about Central and Eastern Europe, EU enlargement, the Eastern Partnership, and the Western Balkans. She has experience from several think tanks in this field and enjoys contributing to debates on Europe’s future. Outside her mother tongue, she is fluent in English and German and proficient in French and Czech.

Edoardo Barca

Honors student in political science and IR in a franco italian degree. Specialized in economics of defence, game theory and arms racing in the european political climate. Passionate about european affairs and social issues of the EU. Wants to pursue an academic career in defence and strategic studies

About the publication:

3 Main Points:

How does Russia leverage AI and the digital domain to destabilise Eastern Europe's security architecture? Moscow utilises an automated ecosystem of generative AI, cyber-kinetic attacks, and domestic proxies to exploit societal fractures, inducing strategic paralysis in "in-between" states. To counter this, nations must move beyond technical fixes toward context-specific reforms that protect electoral integrity and rebuild institutional trust.

Highlight Sentence:

"By targeting the cognitive processes of both leadership and the general public, Moscow seeks to induce a strategic paralysis, ensuring opponents remain reactive and internally divided."

Definition:

Reflexive control is a Soviet strategy of conveying curated information to a target to manipulate their information filter, inducing them to make decisions that favour the initiator's interests.

Reflexive Control: Russian AI-Driven Hybrid Warfare in Eastern Europe

Scenario Setting

The contemporary European security architecture is navigating a profound transition, defined by the Russian Federation's shift from conventional conflict toward a multi-domain, hybrid offensive. As the conflict in Ukraine enters its fifth year of high-intensity attrition, the Kremlin has pivoted toward a Hybrid Escalation (Dixon & Beznosiuk, 2025) strategy. This operational doctrine is designed to compensate for military exhaustion by destabilising the European periphery, with a focus on the Western Balkans and the South Caucasus, where EU-NATO integration remains contested.

In this digital battlefield, Russia acts as a chaos agent, leveraging ethnic fault lines to maintain a permanent security vacuum. Central to this approach is a technical toolset of AI-driven disinformation and offensive cyber operations. By automating narrative amplification and exploiting infrastructure vulnerabilities, Moscow applies a Reflexive Control (Polyakova & Fried, 2019) strategy, deceiving opponents into making decisions that favor Russian strategic interests. This brief examines how this remix of Soviet-era measures and 21st-century technology facilitates a new style of guerrilla geopolitics, threatening democratic resilience and European sovereignty.

Russian Fundamentals for Hybrid, AI Warfare

Russian digital hybrid warfare is a sophisticated military-political doctrine that views modern conflict as a state of continuous confrontation. At its core lies a renewed concept of the Cold War’s Reflexive Control (de Goeij, 2023). This theory targets the information domain, conveying prepared data to an opponent to manipulate their decision-making process. In the Kremlin's view, the digital domain is the primary theatre for information confrontation (Duclos, 2021), where social stability and political legitimacy can be compromised without large-scale kinetic force. This doctrine assumes that the boundaries between peace and war must be permanently blurred, transforming critical services into a grey zone battlefield (Galeotti, 2022). By targeting the cognitive processes of both leadership and the general public, Moscow seeks to induce a strategic paralysis, ensuring opponents remain reactive and internally divided.

The Kremlin has transitioned from traditional propaganda to an automated ecosystem characterised by speed and scale. Fundamental to this is the deployment of generative AI to create high-volume, culturally nuanced content that mimics domestic actors (Propastop, 2025). OPFOR operatives utilise data mining to identify societal fault lines, tailoring messages to exploit specific cognitive biases. This is complemented by botnets on platforms like Telegram and X (formerly Twitter) that create an artificial consensus to isolate target populations. According to a Vigninum (2025) assessment, these tactics amplified narratives like the "Save Europe" Instagram trends of late 2024 and 2025. Foreign bot accounts exploited social unrest to create friction among pro-European stakeholders, weakening the PPE-SDP bloc during the 2024 EU Parliamentary elections and bolstering the far-right "Patriots" party, a group ideologically aligned with Russian interests regarding Ukraine and energy resilience. Simultaneously, Russia employs cyber-kinetic integration, where computer network attacks (CNA) are conducted in tandem with psychological operations. Multiple incidents investigated by CISA and the FBI (2024) have observed actors altering SSH[1] access keys and administrative credentials to lock out system administrators during ongoing attacks. In sabotage campaigns involving the WhisperGate and PathWiper malware, ransomware is often deployed as a front for permanent data destruction. Carried out by state-linked groups like APT29 ("Cozy Bear"), these operations target energy, media, and defence sectors to expose institutional vulnerability and reinforce counter-government unrest.

The scope of this approach is not the acquisition of physical territory but the permanent fragmentation of the Euro-Atlantic security architecture. In the Western Balkans and South Caucasus, the Kremlin aims to leverage structural vulnerabilities to create a permanent backdoor to the EU political landscape.

By ensuring these regions remain in a perpetual buffer state, Moscow effectively stalls their integration into Western ecosystems. This strategy seeks to systematically erode public trust in democratic institutions and the concept of

[1] Secure Shell. SSH protocols specify standards for operating network services securely between untrusted hosts over unsecured networks. Communications between a client and server using SSH are encrypted, so it is ideal for use on unsecure networks.

objective truth, aiming for what can be described as the civilisational erasure of the Western political model. Ultimately, this doctrine transforms target states into strategically paralysed entities no longer capable of mounting unified resistance to Moscow's geopolitical projections.

Moldova: A Polarised "In-Between" State

Moldova constitutes the most politically and socially polarised case in this comparison: an "in-between" state with deep societal cleavages, active electoral contestation, and the continued presence of Russian troops in Transnistria, making it particularly vulnerable to AI-amplified hybrid influence during democratic processes (Baltag & Eaglestone, 2025; Dvornikova, 2023).

This vulnerability is rooted in entrenched political, social, and identity-based divisions. Society remains split between supporters of European integration and groups nostalgic for the Soviet era, creating a contested information environment highly susceptible to misinformation (Dvornikova, 2023). Frequent shifts between pro-European and pro-Russian governments have weakened institutional resilience and reinforced domestic instability (Baltag & Eaglestone, 2025; Dvornikova, 2023). The breakaway region of Transnistria provides Moscow with a permanent foothold on Moldovan territory, while linguistic and cultural ties further facilitate the spread of pro-Russian narratives (Dvornikova, 2025). Economic hardship, inflation, corruption, and an underfunded education system increase public receptiveness to propaganda and disinformation (Baltag & Eaglestone, 2025).

AI-Enabled Hybrid Influence

In Moldova, AI-enabled cyber and information operations function as a force multiplier rather than a standalone threat. Since the early 2000s—and with greater intensity after February 2022—Russia has relied on asymmetric methods to exploit internal opposition, generate psychological pressure, and fracture societal cohesion without territorial conquest (Cebotari et al., 2025). Technological advances have blurred the origin and credibility of online information, complicating attribution and enhancing manipulation through bots, trolls, and coordinated networks that amplify emotionally charged and divisive content (Nistor & Stretea, 2025). AI-enhanced tools increase the speed, scale, and targeting precision of these campaigns, but their effectiveness depends on pre-existing political and informational fractures rather than technological novelty (Nistor & Stretea, 2025).

Rather than seeking outright territorial conquest, the Russian hybrid strategy aims to render the Moldovan state politically favourable to Moscow by confusing, dividing, and demobilising the population through sustained influence operations that challenge national identity and democratic reform trajectories (Cebotari et al., 2025).

Elections, Local Amplifiers, and Hybrid Pressure

Russian election interference in Moldova relies heavily on domestic proxy actors who embed hostile narratives into the electoral discourse. Russophile political parties and oligarchic networks—most notably those linked to Ilan Șor and his party—have mobilised public dissatisfaction during election periods, promoted anti-EU messaging, and portrayed President Maia Sandu as authoritarian and illegitimate (Baltag & Eaglestone, 2025; Dvornikova, 2023). Former political elites have reinforced these narratives through appearances in pro-Russian media, directly targeting the legitimacy of pro-European leadership during campaigns (Dvornikova, 2023).

These networks intensified their activities during the 2024 presidential election and the EU referendum. Russian-backed actors combined coordinated disinformation, cyber operations, illicit campaign financing, voter bribery, and intimidation tactics—including bomb threats at diaspora polling stations—to undermine pro-EU sentiment and suppress turnout (Mihailov et al., 2025). Targeting focused on politically vulnerable regions such as Transnistria, where regional grievances could be more easily exploited (Baltag & Eaglestone, 2025). Although President Sandu ultimately prevailed—largely due to diaspora mobilisation—the narrow referendum result demonstrated the depth of societal polarisation and the tangible impact of sustained, election-centred hybrid pressure (Baltag & Eaglestone, 2025; Mihailov et al., 2025).

Georgia: Elections between European Aspiration and Authoritarian Drift

Georgia represents the most geopolitically exposed case in this comparison. It combines a strongly pro-Western societal orientation with direct Russian military occupation, sustained hybrid pressure, and growing domestic political convergence with Kremlin narratives. This makes elections a critical arena for contestation over Georgia's Euro-Atlantic trajectory (Kakachia & Kakabadze, 2024).

Russia's hybrid influence in Georgia follows a layered strategy combining military coercion, political manipulation, economic leverage, and cyber and information operations. Georgia's long-standing aspirations for EU and NATO membership have positioned it as a priority target for Russian influence aimed at halting the Euro-Atlantic alignment and reasserting control in the South Caucasus (Kakachia & Kakabadze, 2024).

AI-Enabled Influence in the 2024 Parliamentary Elections

In the Georgian case, AI amplifies pre-existing hybrid tactics rather than constituting a distinct or independent threat. Russian hybrid warfare builds on established Soviet-era methods, updated through digital technologies in which cyber operations and disinformation accompany or substitute direct military action (Maisaia et al., 2020). AI-enabled tools enhance the speed, scale, and repetition of existing narratives, making election-related propaganda cheaper, faster, and harder to trace.

A defining feature of Russian influence during the 2024 parliamentary elections was its reliance on domestic political and media actors rather than overt Russian messaging. Pro-government and pro-Russian narratives circulated through sympathetic NGOs, media outlets, and political figures who questioned Western integration and promoted neutrality or accommodation with Moscow (Maisaia et al., 2020). This indirect strategy allowed Kremlin-aligned messaging to appear domestically rooted, increasing its credibility during the campaign.

Election-period narratives relied heavily on emotional framing. Campaign materials and public messaging juxtaposed images of destruction from the war in Ukraine with slogans such as “choose peace,” implicitly warning that political change or continued Western alignment could lead to war in Georgia (Gasparyan et al., 2024). Rather than engaging in substantive policy debate, these messages narrowed voter choice by linking opposition success to instability and insecurity.

Within this context, AI-enabled tools amplified—rather than created—these narratives. By increasing their frequency and reach across digital platforms, AI supported the rapid dissemination of fear-based messaging already promoted by domestic actors, reinforcing psychological pressure during a politically sensitive period (Maisaia et al., 2020).

Military Occupation as Background Coercion

Russia’s military presence in the occupied territories of Abkhazia and South Ossetia continued to shape the information environment of the 2024 elections. The presence of Russian forces—covering approximately 20 per cent of Georgian territory—served as a constant reminder of the risk of escalation and made warnings about war appear credible (Andruș & Ivan, 2025; Chikhladze et al., 2025).

Rather than being activated directly, this military pressure functioned as background coercion. It reinforced fear-based electoral narratives and discouraged political alternatives associated with confrontation or deeper Western alignment, thereby strengthening information and psychological operations during the electoral process (Chikhladze et al., 2025).

Bosnia and Herzegovina: Political Fragmentation and Exposure to External Pressure

Bosnia and Herzegovina (BiH) constitutes the most structurally vulnerable case in this comparison due to its fragmented constitutional architecture, entrenched ethnic divisions, and weak institutional capacity (Dolan, 2022). The post-Dayton governance system, based on entity-level veto powers and ethnic representation, produces chronic political paralysis and enables domestic elites to block state-level reforms (Dolan, 2022; Putină, 2024). This institutional dysfunction makes the political system more vulnerable to external hybrid interference, as slow and fragmented decision-making weakens coordinated security responses and undermines public trust in democratic institutions.

Russia exploits these structural weaknesses as part of a broader strategy to prevent BiH's Euro-Atlantic integration and preserve instability in the Western Balkans (Solik et al., 2022). Unlike in Moldova or Georgia, Moscow does not require high levels of direct engagement or technological sophistication in BiH. Instead, it leverages existing ethnic cleavages and elite capture—particularly within Republika Srpska (RS)—to obstruct reforms, delegitimise state institutions, and normalise separatist discourse (Mikac et al., 2022; Solik et al., 2022). The alignment between Russian strategic interests and RS leadership, especially Milorad Dodik, allows Moscow to exert disproportionate influence through political support, diplomatic backing, and information amplification rather than overt coercion (Ahić & Hodžić, 2022; Putină, 2024).

The country's media environment further amplifies these vulnerabilities. Low trust in domestic media, weak regulatory oversight, and strong partisan alignment enable disinformation to circulate through established television and print outlets rather than relying solely on social media manipulation (Putină, 2024). Russian state-linked outlets, most notably the Serbian-language version of Sputnik, act as indirect hubs for pro-Russian narratives, which are then recycled by local media and political actors (Putină, 2024). AI-enabled tools function primarily as accelerants within this ecosystem, increasing the speed, repetition, and reach of narratives that already resonate with polarised audiences, rather than introducing novel forms of influence (Mikac et al., 2022; Solik et al., 2022).

Elections as a Target of Russian Hybrid Pressure

Elections represent a central pressure point in Russia's hybrid strategy in BiH. Rather than attempting to shape nationwide electoral outcomes, Russian interference focuses on preserving favourable power structures at the entity level—particularly in RS—by reinforcing nationalist narratives, discrediting opposition candidates, and framing Western engagement as a threat to stability and identity (Putină, 2024). Information operations intensify during electoral periods, synchronising disinformation with political campaigning to protect elite allies and entrench institutional deadlock.

Ahead of the RS elections, Russian-aligned media and political actors consistently portray pro-reform candidates as Western proxies, while depicting EU and NATO integration as sources of economic decline and security risk (Solik et al., 2022). These narratives are emotionally framed around victimhood, sovereignty, and historical grievance, resonating strongly within an already polarised electorate. AI-enabled disinformation tools enhance these campaigns by automating content production and amplification across platforms, creating an artificial sense of consensus and marginalising moderate or pro-state positions (Dolan, 2022).

Crucially, Russia's objective is not to overturn public support for EU accession—which remains broadly positive at the societal level—but to sustain elite-level obstruction and political paralysis. By ensuring that elections reproduce the same veto players and nationalist leadership, Moscow maintains a low-cost mechanism to block institutional reform, weaken state cohesion, and keep BiH strategically stalled. The threat, therefore, lies less in electoral fraud than in the long-term erosion of democratic functionality through repeated manipulation of electoral narratives.

Bosnia and Herzegovina’s limited capacity to counter these threats exacerbates the risk (Mikac et al., 2022). The absence of a comprehensive national hybrid threat strategy, weak cybersecurity governance, and minimal coordination between state and entity-level institutions leave the country poorly prepared for AI-enhanced information and cyber operations. In this context, Russian hybrid activity acts as a force multiplier, embedding itself within BiH’s structural fragility and transforming elections from instruments of democratic accountability into recurring vectors of destabilisation (Ahić & Hodžić, 2022).

Final Observations: Strengthening Resilience Against External Pressures

For Georgia, Moldova, and BiH, political guidelines must prioritise resilience against hybrid interference while preserving democratic legitimacy. In Georgia, where societal support for Euro-Atlantic integration remains high but political polarisation is increasing, guidelines should focus on insulating electoral processes from disinformation and indirect proxy influence. Strengthening independent media oversight, improving transparency of party financing, and reinforcing strategic communication capacities are essential to counter fear-based narratives that link European integration with instability (Kakachia & Kakabadze).

Moldova requires a dual approach combining institutional reform with societal cohesion. Given its deep internal divisions and exposure to proxy political networks, political guidelines should support judicial independence, regulate campaign financing, and expand state capacity to detect and attribute foreign information manipulation. At the societal level, investment in media literacy and public trust-building measures is critical to reducing receptiveness to polarising narratives (Baltag & Eaglestone; Dvornikova).

In Bosnia and Herzegovina, the primary challenge lies in structural paralysis. Political guidelines should therefore target constitutional deadlock by reinforcing state-level coordination mechanisms and limiting the ability of entity-level elites to monopolise security and information policy. Supporting pluralistic media environments and independent regulatory bodies would reduce the dominance of ethnonationalist framing in political discourse (Dolan; Putină).

Overall, the three cases demonstrate that hybrid pressure exploits existing institutional weaknesses rather than creating them. Effective political guidelines must therefore be context-specific but united by a common objective: protecting electoral integrity, strengthening information resilience, and preventing elite capture. Without sustained political reform and coordinated strategic communication, external hybrid influence will continue to transform domestic political competition into a vector of long-term destabilisation rather than democratic accountability.

References

Ahić, J., & Hodžić, K. (2022). *The War in Ukraine and Challenges for the National Security of Bosnia and Herzegovina*. 61–80.

Baltag, D., & Eaglestone, A. (2025). Furthest away from Russia and ever closer to the EU? Moldova hedging its bets on alternating alignments and (differentiated) dis/integration. *European Security*, *34*(4), 624–645. https://doi.org/10.1080/09662839.2025.2583337

Cebotari, S., Coropcean, I., & Stejaru, S. (2025). *The Republic of Moldova in the Context of the Russian Federation Hybrid War*. *16*(1), 183–208.

CISA & FBI. (2024). Russian state-sponsored cyber actors use WhisperGate malware to target Ukrainian organizations. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

de Goeij, M. W. R. (2023). Reflexive control: Influencing strategic behavior. Parameters, 53(4), 119–131. https://press.armywarcollege.edu/parameters/vol53/iss4/14

Dixon, W., & Beznosiuk, M. (2025, December 19). Russia is losing – time for Putin's 2026 hybrid escalation. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/commentary/russia-losing-time-putins-2026-hybrid-escalation

Dolan, C. J. (2022). Hybrid Warfare in the Western Balkans: How Structural Vulnerability Attracts Maligned Powers and Hostile Influence. *SEEU Review*, *17*(1), 3–25. https://doi.org/10.2478/seeur-2022-0018

Duclos, M. (2021). The information confrontation: Russia's digital strategy in the European theater. Institut Montaigne. https://www.institutmontaigne.org/en/expressions/russias-national-security-strategy-2021-era-information-confrontation

Dvornikova, P. (2023). *Foreign Influence and Disinformation in Moldova* (No. 9). Peace & Security Monitor. https://peacehumanity.org/wp-content/uploads/2023/09/The-Peace-and-Security-Monitor-SEE-BSR-Issue-9.pdf#page=30.00

Galeotti, M. (2022). The weaponisation of everything: A field guide to the new way of war. Yale University Press.

Gasparyan, D., Wolkov, N., & Kagan, F. W. (2024). *Russia or the West: The Stakes in Georgia's Election*. *1*, 1–19.

Kakachia, K., & Kakabadze, S. (2024). Beyond Cyber and Disinformation: Russian Hybrid Warfare Tactics in Georgia. In *Russian Warfare and Influence: Small States in the Intersection Between East and West* (pp. 129–153). Bloomsbury Academic.

Maisaia, V., Guchua, A., & Zedelashvili, T. (2020). The cybersecurity of Georgia and threats from Russia. *Eastern Review*, *9*(1), 105–119. https://doi.org/10.18778/1427-9657.09.07

Mihailov, A., DeSisto, I., Pop-Eleches, G., Burmester, I., & Marandici, I. (2025). *Presidential Election and EU Referendum* (D. Baltag, J. M. Dollbaum, A. Eaglestone, E. Knott, I. Marandici, J. Perović, S. Suveica, & D. Ursprung, Eds.) [Application/pdf]. University of Fribourg/CH, the Research Centre for East European Studies at the University of Bremen, the Center for Security Studies (CSS) at ETH Zurich and the Center for Eastern European Studies (CEES) at the University of Zurich. https://doi.org/10.3929/ETHZ-B-000715250

Mikac, R., Mitrevska, M., & Smajić, M. (2022). Hybrid Threats and Counter-Hybrid Solutions: A Comparative Case Study Analysis of Croatia, North Macedonia, and Bosnia and Herzegovina. *Politics in Central Europe*, *18*(3), 375–395. https://doi.org/10.2478/pce-2022-0017

Ministry for Europe and Foreign Affairs. (2025, February 5). Foreign digital interference - Publication of the VIGINUM report on information manipulation. France

Diplomatie. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/foreign-digital-interference-publication-of-the-viginum-report-on-information

Nistor, R.-M., & Stretea, A.-I. (2025). Dismiss, distort, distract, dismay: The civil society in Moldova in the face of disinformation. *Civil Szemle*, *22*(1), 177–194. https://doi.org/10.62560/csz.2025.01.11

Polyakova, A., & Fried, D. (2019). Democratic defense against disinformation. Atlantic Council / CEPA. https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/

Propastop. (2025, April 29). Old wine in a new bottle 4: Reflexive control. https://www.propastop.org/en/2025/04/29/old-wine-in-a-new-bottle-4-reflexive-control/

Putină, N. (2024). *Strenghtening the Resilience of States Against Hybrid Threats—Lessons for the Republic of Moldova*. https://doi.org/10.5281/ZENODO.12719755

Solik, M., Graf, J., & Baar, V. (2022). *Hybrid Threats in the Western Balkans: A Case Study of Bosnia and Herzegovina*. *22*(1), 5–23.