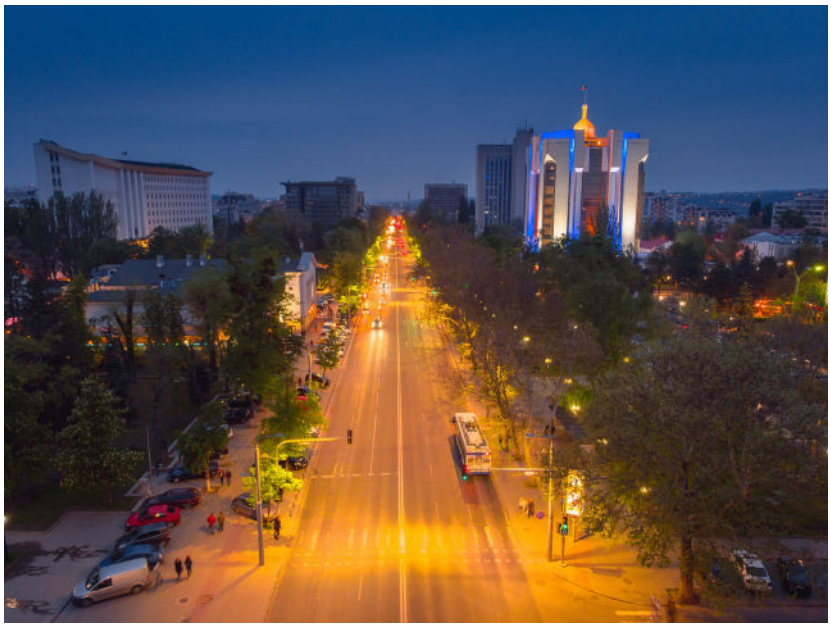
STUDY

Requested by the AFET committee

European Parliament

Challenges faced by the EU enlargement countries from Russian hybrid interference



Authors:
Levan KAKHISHVILI

European Parliament coordinator:
External Policies Analysis and Support Unit
Directorate-General for External Policies of the Union

PE 783.619 – July 2026

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
EXTERNAL POLICIES ANALYSIS AND SUPPORT UNIT

European Parliament

STUDY

Challenges faced by the EU enlargement countries from Russian hybrid interference

ABSTRACT

This paper analyses how Russia's hybrid interference targets European Union (EU) enlargement countries and how the EU responds, particularly with regard to its enlargement policy. It develops a precise, strategy-centred concept of 'hybrid interference' that distinguishes coordinated, multi-instrument campaigns against domestic democratic orders from broader notions of hybrid warfare, influence or leverage. On this basis, it maps recurring vulnerabilities across nine enlargement countries – Albania, Bosnia and Herzegovina, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, Serbia and Ukraine – and identifies six main instruments in Russia's toolkit: covert political financing; information operations; legal-constitutional obstruction via proxy elites; energy and economic leverage; cyber operations; and security-sector penetration with support for proxy violence. The empirical core combines a cross-country overview with a focused comparison of Moldova, Georgia and Serbia to show how these instruments are re-combined under different domestic alignments and conflict settings. The paper then examines the EU's evolving counter-strategy, from the 2016 Joint Framework, the Global Strategy and Strategic Compass to on-the-ground measures in enlargement countries, highlighting both progress in mainstreaming hybrid resilience into accession conditionality and persistent implementation gaps. It argues that EU tools are most effective where reform-oriented elites align with EU objectives, as in Moldova and least effective where domestic governments internalise Russia's authoritarian playbook, as in Georgia, or pursue ambiguous dual-track policies, as in Serbia. The concluding recommendations set out how the European Parliament can use its legislative, budgetary and scrutiny powers to embed democratic resilience and counter-hybrid measures at the heart of the enlargement process.

EP-EXPO/2023/OP/0001/AFET/LOT2/1/C/2
July 2026 – PE 783.619

EN

AUTHOR(S)

Dr Levan KAKHISHVILI, Postdoctoral Researcher, ETH Zurich, Switzerland

ACKNOWLEDGEMENTS

The author would like to thank the anonymous external reviewer for their insightful comments.

CONTRIBUTORS

Tomma FIEDLER, Project Assistant, Trans European Policy Studies Association (TEPSA), helped with the review process.

CONTRACTOR

Trans European Policy Studies Association (TEPSA), Belgium (Coordinator: Ana LELADZE, Project Officer)

CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Michal MALOVEC
Editorial assistance: Inge BRYS

To give feedback or obtain copies, please write to: mailto:exas@europarl.europa.eu.

PEER REVIEW

This study was subject to an external peer review.

VERSION(S)

Original: English

Manuscript completed in July 2026.

BIBLIOGRAPHIC REFERENCE FOR THIS PAPER

KAKHISHVILI, Levan. 2026. *Challenges faced by the EU enlargement countries from Russian hybrid interference*. Brussels: European Parliament, External Policies Analysis and Support Unit.

For in-text citations: Kakhishvili, 2026

Table of contents

List of abbreviations

CFSP	Common Foreign and Security Policy
CSDP	Common Security and Defence Policy
DDoS	Distributed denial of services
EEAS	European External Action Service
EPF	European Peace Facility
EU	European Union
EUGS	European Union Global Strategy
FIMI	Foreign information manipulation and interference
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
IPA	Instrument for Pre-accession Assistance
NATO	North Atlantic Treaty Organization
ODIHR	Office for Democratic Institutions and Human Rights
OSCE	Organization for Security and Co-operation in Europe
SIPRI	Stockholm International Peace Research Institute
USA	United States of America

List of figures and tables

Executive summary

How does Russia's hybrid interference target European Union (EU) enlargement countries? What instruments are used and what vulnerabilities are exploited? This paper explores these questions aiming at understanding hybrid interference as a strategy-centred concept in nine enlargement countries: Albania, Bosnia and Herzegovina, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, Serbia and Ukraine. Focusing on the European Parliament's role, the paper proposes a package of recommendations on the EU's response to Russian hybrid interference through its enlargement policy.

Existing debates among scholars and policy experts blur important distinctions between 'hybrid warfare', 'interference', 'influence' and 'leverage'. Hence, in designing countermeasures a precise definition of 'hybrid interference' is helpful. It is defined here as the coordinated use, under peacetime conditions, of at least two distinct instruments (from financial, informational, cyber, legal, economic or security-sector tools) by a foreign state or its proxies to reshape another state's domestic political order below the threshold of open armed conflict. Hybrid interference: targets elections, party systems, institutional rules and foreign-policy orientation; operates in a grey zone relying on deniability and legal ambiguity; and seeks identifiable psychological effects such as fear, dissatisfaction and nostalgia that induce segments of the population to demand political change aligned with the interferer's preferences. This definition of hybrid interference is applicable to empirical cases.

Hybrid interference seeks to produce psychological effects by exploiting the vulnerabilities of a target society within various political and economic systems. Across the nine enlargement countries seven such vulnerabilities can be identified: intense political polarisation and unstable coalition politics; unresolved ethnic, constitutional and status disputes; fragile and captured information ecosystems; institutional weakness and corruption; energy and economic dependence; security-sector and critical-infrastructure exposure; and the specific fragilities of electoral processes. These vulnerabilities form an interconnected ecosystem: polarisation and disputes feed information fragility; weak rule of law magnifies the impact of energy dependence and security penetration; while cyber and media weaknesses make elections a recurring point of leverage.

Against this background, Russia deploys a modular toolkit encompassing a range of instruments, among which six are particularly significant:

- Covert and illicit political financing tilts electoral competition, creates proxy parties and binds elites to Moscow through financial dependency, with Moldova providing the most sophisticated example.
- Information operations, increasingly laundered through local media and social-media networks, corrode information integrity and normalise pro-Kremlin narratives, with the EUvsDisinfo database showing that enlargement and neighbourhood countries are disproportionately targeted.
- Legal and constitutional obstruction via proxy elites appears in Bosnia and Herzegovina, Montenegro and above all, Georgia, where foreign-agent-style legislation has been imported from the Russian model.
- Energy, economic and oligarchic leverage is central in Serbia, Montenegro, Bosnia and Herzegovina, Moldova, Georgia and Ukraine.
- Cyber operations and technical sabotage accompany political crises and elections, notably in Georgia, Ukraine and Moldova.
- Finally, security-sector penetration and support for proxy violence are evident in the Montenegrin coup attempt, paramilitary structures in Republika Srpska, incidents in northern Kosovo and Russian-backed armed formations in Ukraine, Georgia and Moldova.

A focused comparison of Georgia, Moldova and Serbia illustrates how these instruments are recombined under different domestic alignments. Moldova has become a 'laboratory' for electoral interference, with

large-scale illicit financing, disinformation and cyberattacks concentrated around the 2024–2025 electoral cycles; yet a reform-oriented government has adopted 'militant democracy' tools, strengthened oversight and used EU support to maintain a pro-EU trajectory. Georgia has progressively internalised the Russian authoritarian playbook: the 'foreign influence' law, manipulation of elections and anti-Western narratives show how domestic elites can voluntarily adopt Moscow-style instruments, making Russia's operational footprint lighter while its strategic gains increase. Serbia functions as a regional hub for Russian geoeconomic, information and intelligence influence, particularly through energy ties, media platforms such as RT Balkans and long-standing security cooperation, even as it simultaneously seeks to preserve EU accession prospects and gradually diversify some dependencies. These three cases confirm that unresolved conflicts (Transnistria and Gagauzia; Abkhazia and South Ossetia; Kosovo and the wider 'Serb question') are central objects of manipulation.

Since 2016, the EU has moved from *ad hoc* reactions to a layered strategic framework. As the Union seeks to make hybrid threats governable, at the level of enlargement policy, hybrid-threat resilience has been integrated into accession and association frameworks, security and defence cooperation, political conditionality and financial instruments. However, the effectiveness of this response is uneven. The EU has placed hybrid threats at the centre of its strategic framework and developed a sophisticated toolbox but implementation remains fragmented; many tools are non-binding and enforcement in sensitive domains such as illicit finance, media regulation and party funding is often weak. On the ground, outcomes correlate strongly with domestic political will, the credibility of the enlargement perspective and the Union's ability to deploy instruments in an integrated and timely manner. Moldova demonstrates that EU support *can* significantly bolster resilience when domestic elites and civil society are committed to reform; Georgia shows that EU leverage is limited when ruling elites internalise the Russian model; Serbia illustrates the difficulties of using conditionality effectively in a context of strategic ambiguity and perceived enlargement fatigue.

Russian hybrid interference is neither new nor deterministic. It represents a structured challenge that must be addressed at the core of the EU's enlargement policy. To this end, the European Parliament could: establish a standing cross-committee task force on foreign interference; make 'hybrid interference and resilience' an explicit benchmark under Cluster 1 of the accession process; use its budgetary powers to ensure funding for independent media, civic space, cyber resilience and media literacy; support a regional disinformation rapid-response network and digital-forensics components in all election observation missions; promote criminalisation of key enabling activities of interference in national legislation; enforce political advertising transparency in enlargement countries; treat these countries as part of the EU's defensive perimeter in Foreign Information Manipulation and Interference as well as cyber planning; and ensure that democratic resilience becomes a visible, measurable budget priority. Only by hard-wiring counter-hybrid measures into the enlargement framework and by aligning strategic, legal, financial and societal instruments, can the EU safeguard both the integrity of its democratic order and the credibility of enlargement.

1 Introduction

Russia's foreign policy in the post-communist space is often described by Russian politicians as a reaction to behaviour by the West at large[1]. This behaviour in Russian discourse refers particularly to 'expansion' of the North Atlantic Treaty Organization (NATO) and European Union (EU), which is viewed by the Kremlin as the Western penetration into what Russia calls its 'near abroad', referring to Moscow's historically defined areas of strategic influence, in other words, its former Soviet republics. Keeping Western countries out of its 'near abroad' has traditionally been one of the two main pillars of Russian foreign policy in the post-Cold War era. The second, though, has been reinforcing its hierarchy of sovereignty in the region, with that of Russia at the top of the ladder[2]. Such a hierarchy can be established and maintained by three practical objectives: political integration projects, such as the Commonwealth of Independent States; military presence legitimised through the Collective Security Treaty Organization; and asymmetric economic interdependence, particularly within the Eurasian Economic Union. On these grounds, the idea of interference within the domestic affairs of former Soviet republics already had a strong presence in political discourse immediately after the Soviet Union was dissolved. According to the former Russian Foreign Minister, Andrei Kozyrev's September 1993 statement, 'Russia has a special right to intervene in the former Soviet republics to protect human rights, particularly those of ethnic minorities'[3].

It is against this background that Russia has been intensifying its efforts to prevent the Western Balkan countries and the Eastern Trio – Georgia, Moldova and Ukraine – from progressing on their paths towards EU integration. While the historical trajectories of former Soviet republics and Western Balkan states differ, Russia's contemporary approach to both regions is shaped by a common strategic logic of contesting Western political and security penetration into what it perceives as its wider sphere of influence. In the Western Balkans, this has translated less into claims of formal tutelage and more into efforts to exploit legacies of cultural and religious affinities as well as unresolved status questions in order to hinder Euro-Atlantic integration and preserve room for Russian political and security leverage. Accordingly, the overarching background of resisting perceived Western 'expansion' and maintaining a hierarchical regional order remains relevant in the Western Balkans, even though the historical bases of Russia's claims differ from those regarding the former Soviet space.

As enlargement countries advance in the context of Europeanisation and draw ever closer to EU membership, Russia increasingly engages in hybrid warfare tactics to interfere in their domestic affairs and halt their progress. In attempting to counter such interference, it is important to understand how exactly Russian hybrid warfare works in the context of EU enlargement. What instruments does Russia use to dissuade enlargement countries' national governments or EU decision-makers from believing that EU membership is a credible prospect? How does the EU respond to these tactics and what can be improved in its approach to alleviate the effects of Russian interference in the enlargement process? This paper investigates these questions by exploring nine enlargement countries and their domestic contexts: Albania, Bosnia and Herzegovina, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, Serbia and Ukraine. While Georgia, Moldova and Ukraine were formerly part of the Soviet Union, Western Balkan countries were not. This distinction may determine Russia's varied approach and intensity of engagement across the two geographic areas.

[1] T. Kastueva-Jean, 'Russia's Domestic Evolution: What Impact on Its Foreign Policy?', *Russie.Nei.Visions*, No 84, 2015.
[2] R. Deyermond, *Security and Sovereignty in the Former Soviet Union*, Lynne Rienner Publishers, London, 2008.
[3] M. B. Olcott et al., *Getting it Wrong: Regional Cooperation and the Commonwealth of Independent States*, Carnegie Foundation for International Peace, Washington DC, 1999.

The EU's response to hybrid interference rests on a layered strategic framework that since 2016 has been developed around three main pillars: the 2016 Joint Framework on countering hybrid threats[4]; the EU Global Strategy (EUGS)[5] and its Strategic Compass[6]; and a democracy- and information-space pillar built around the Foreign Information Manipulation and Interference (FIMI) toolbox, as well as the emerging European Democracy Shield[7]. Together, these instruments seek to transform hybrid threats from a diffuse risk into a governable policy field with dedicated capacities and procedures.

The 2016 Joint Framework on countering hybrid threats provides the conceptual and institutional baseline. It defines hybrid threats as a mixture of coercive and subversive activities that blend diplomatic, military, economic and technological methods 'below the threshold of formally declared warfare' and emphasise exploiting vulnerabilities and creating ambiguity. Hybrid activity is understood as targeting both state and societal resilience, thereby blurring internal-external security boundaries[8]. On this basis, the Joint Framework organises the EU response around four lines of action: improving awareness; building resilience; preventing, responding to and recovering from crises; and strengthening cooperation with NATO[9].

The EUGS[10] and its implementation reports extend this logic into a broader strategic framework that positions hybrid threats at the centre of the Union's ambition to act as a security provider. The first report highlights the need to connect internal and external security, integrate conflict-prevention, crisis response and resilience, treating disinformation, cyber operations and the weaponisation of interdependence as core security issues. Rather than viewing hybrid interference as a marginal or purely technical problem, the EUGS embeds it in a narrative about Europe's role of defending a rules-based order and protecting its citizens against diffuse, cross-border threats.

The Strategic Compass for Security and Defence[11] operationalises this framework over the next decade. It frames the strategic environment as one in which 'everything is weaponised' and where the EU faces 'hybrid tactics and intermediate dynamics of competition, intimidation and coercion', including disinformation, foreign interference, energy leverage and instrumentalised migration. Within its four strands – act, secure, invest, partner – hybrid threats occupy a central place under 'Secure'. This Compass commits the EU to enhancing resilience substantially and developing an EU Hybrid Toolbox.

Alongside these security-centred instruments, the EU has gradually built a democracy- and information-space pillar directed at protecting electoral integrity and public debate. This third pillar revolves around the development of the FIMI toolbox, systematic monitoring of foreign information manipulation in the European External Action Service (EEAS) and plans for a European Democracy Shield[12]. In practice, it is reflected in three trends: the routine inclusion of hybrid-threat and FIMI language in rule-of-law and enlargement reports; the use of external-action instruments (Neighbourhood, Development and International Cooperation Instrument-Global Europe, Instrument for Pre-accession Assistance III, the Reform and Growth Facility) to fund resilience-building in media, civil society and digital

[4] European Commission, Joint Communication on Joint Framework on countering hybrid threats: a European Union response, JOIN(2016) 18 final, 6 April 2016.
[5] EEAS, A Global Strategy for the European Union's Foreign and Security Policy, 15 December 2016.
[6] EEAS, A Strategic Compass for Security and Defence, 2022.
[7] European Commission, Joint Communication on European Democracy Shield: Empowering Strong and Resilient Democracies, JOIN(2025) 791 final, 12 November 2025.
[8] European Commission, Joint Communication on Joint Framework on countering hybrid threats: a European Union response, JOIN(2016) 18 final, 6 April 2016.
[9] European Commission, Joint Framework on countering hybrid threats, JOIN(2016) 18 final, 6 April 2016.
[10] EEAS, A Global Strategy for the European Union's Foreign and Security Policy, 15 December 2016.
[11] EEAS, A Strategic Compass for Security and Defence, 2022.
[12] European Commission, Joint Communication on European Democracy Shield: Empowering Strong and Resilient Democracies, JOIN(2025) 791 final, 12 November 2025.

governance; together with an emerging, though still incomplete, link between hybrid-threat concerns and the EU's policy of conditionality in relation to candidate countries.

This strategic framework is therefore comprehensive yet still in flux. It offers a multi-level toolbox that ranges from intelligence fusion and cyber defence to political conditionality and support for independent media. However, it also remains unevenly implemented, with some initiatives still in the process of translation from paper to practice. Furthermore, the EU operates in a rather volatile geopolitical environment, in which increasing friction with the United States of America (USA) as well as incremental expansion of economic influence from China and Türkiye do not necessarily align with the Union's strategic interests[13]. This context complicates EU engagement with the enlargement countries through the traditional policy of conditionality because the candidate countries may engage in so-called 'cross-conditionality' as there are a number of great powers willing to provide economic benefits to them[14].

Debates on Russia's response to EU enlargement frequently conflate 'hybrid war', 'interference', 'leverage' and 'influence', even though these concepts capture different degrees and forms of involvement. This report, therefore, begins by building a more precise conceptual apparatus, grounded in both scholarly literature and policy analysis, to distinguish between hybrid interference and other, less intrusive forms of Russian engagement. Such clarity is essential because Russia's political, military, economic and cultural footprint is highly uneven across the nine enlargement and neighbourhood countries studied here: in some cases, Moscow can plausibly be said to wage a sustained hybrid campaign, while in others its influence is marginal or in decline. On the basis of this conceptual review, the paper identifies and thematically categorises the main tactics through which Russia seeks to constrain Western penetration, not only by preserving political and economic dependence but also retaining a hegemonic role in what it still regards as its sphere of influence. These categories then serve as a lens for evaluating empirical evidence country by country.

Methodologically, this paper combines broad comparative coverage with in-depth qualitative inquiry. Desk research maps the context in each of the nine countries, surveys existing measures of Russian influence and classifies states according to their vulnerability to Moscow's efforts to drive a wedge between them and the EU. In this process, particular attention is paid to official documents, media coverage and public statements, which simultaneously reveal Russian tactics and EU responses. To capture these dynamics in a more nuanced way, 18 in-depth interviews have been conducted with researchers, experts and current or former decision-makers based in the EU and enlargement countries. Respondents were identified purposively through personal contacts and desk research. At least one respondent had expertise on at least one of the enlargement countries. Finally, the report complements the nine-country overview with a focused comparison of Moldova, Georgia and Serbia – three cases of high but divergent Russian leverage – to illuminate how hybrid interference operates under different domestic alignments and how EU policy can better support governments and societies seeking to escape Moscow's grip.

2 Conceptualisation of hybrid warfare in the context of EU enlargement: Conceptual apparatus

In recent years, discussions around Russian 'hybrid warfare' have intensified. The term became a catch-all label for a range of activities such as 'information warfare', 'political warfare', 'unconventional warfare',

[13] M. Bonomi et al., Foreign Interference of China, Russia and Turkey in the EU Enlargement Countries until 2035: Three Scenarios and Policy Implications, *InvigoratEU Project*, 2026.

[14] For a detailed discussion on cross-conditionality, see: F. Schimmelfennig, 'Geopolitical Enlargement', in J. Pollak and M. Jopp (eds), *The European Union's Geopolitics: The Lackluster World Power*, Springer, Cham, 2024, pp. 79-98.

'irregular warfare', 'subversive warfare' and so on[15]. In the literature, at least four partly overlapping conceptual families emerge:

- 'hybrid warfare/hybrid threats', used for almost any blend of military, irregular, informational, cyber and economic tools;
- 'political warfare/information operations/influence operations', targeting perceptions, legitimacy and behaviour below the threshold of open war;
- 'unrestricted/grey-zone/fourth-generation warfare', derived from Chinese and Western debates about conflict 'everywhere and always';
- 'resilience/militant democracy/democratic security', which supply normative frameworks for domestic responses to such interference.

This proliferation of partially interchangeable labels usually complicates debates, undermining the analytical and policy value of the concepts themselves.

Key problems associated to the concept of hybrid warfare, frequently acknowledged in the literature, include: vagueness of conceptual boundaries; conflation between different levels of warfare, such as strategy or tactics; normative content of the concept; and difficulties in measurement[16]. If any mix of instruments is deemed 'hybrid', the term ceases to discriminate between qualitatively different cases and becomes a catch-all label. At the same time, without clear distinctions across incompatible levels of analysis, these concepts are applied to: tactical force combinations on the battlefield; grand strategy; and peacetime interference in democratic politics. This generates a further normative distortion, in that calling election campaigns, covert financing or media capture 'warfare' blurs the line between war and peace in ways that democratic states are understandably reluctant to codify. Yet this still leaves them with no precise vocabulary for hostile activities that fall short of armed attack. Unsurprisingly, this conceptual overload makes rigorous measurement virtually impossible, since coding 'hybrid' incidents or comparing intensities across countries becomes arbitrary. This has led various authors either to call for abandoning 'hybrid warfare' as an overarching label in favour of more precise notions such as strategy and political warfare, or to confine 'hybrid warfare' strictly to battlefield phenomena while adopting different terminology for domestic interference in democracies[17].

This conceptual proliferation often displays the same underlying pattern – the integrated use of military and non-military instruments to shape another actor's political choices below the threshold of open war. For the purposes of studying interventions in domestic political orders, a narrower, strategy-centred concept of 'hybrid interference' is therefore more useful and measurable than the broader and increasingly amorphous language of 'hybrid warfare'.

Scholarly literature grounded in traditional academic disciplines, such as strategic studies, for example, uses hybrid warfare to describe a specific type of warfare characteristic of contemporary armed conflicts. Popularised by Frank G. Hoffman[18], hybrid warfare was introduced to describe a specific way of waging

---

[15] M. Caliskan and P. A. Cramers, 'What Do You Mean by Hybrid Warfare? A Content Analysis on the Media Coverage of Hybrid Warfare Concept', *Horizon Insights*, Vol 1, No 4, 2018, pp. 23–36.

[16] See M. Caliskan, 'Hybrid warfare through the lens of strategic theory', *Defense & Security Analysis*, Vol 35, No 1, 2019, pp. 40–58.

[17] M. Caliskan, 'Hybrid warfare through the lens of strategic theory', *Defense & Security Analysis*, Vol 35, No 1, 2019, pp. 40–58; R. Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies*, Vol 29, No 1, 2019, pp. 141–163.

[18] F. G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, 2007; F. G. Hoffman, 'Hybrid Warfare and Challenges', *Joint Force Quarterly*, No 52, 2009, pp. 34–39; F. G. Hoffman, 'Hybrid vs. Compound War, The Janus Choice: Defining Today's Multifaceted Conflicts', *Armed Forces Journal,* 2009; F. G. Hoffman, '"Hybrid Threats": Neither Omnipotent nor Unbeatable', *Orbis*, Vol 54, No 3, 2010, pp. 441–455; F. G. Hoffman, 'On Not-So-New Warfare: Political Warfare vs Hybrid Threats', *War on the Rocks*, 28 July 2014.

war, characterised by three interlocking features: deliberate shifts in the centre of gravity to non-military domains; sustained operations in the grey zones between war and peace, domestic and external, state and non-state; as well as the creative orchestration of diverse civilian and military means. According to this reading, war is 'inherently hybrid' but 'hybrid warfare in the narrower sense' exists only when these tendencies become strategically central, as in Russia's Crimea and Donbas campaigns. However, 'hybrid warfare' has ballooned into a catch-all label encompassing guerrillas and regular forces, terrorism, cyber-attacks, propaganda, criminality, 'fourth-generation warfare', 'unrestricted warfare' and 'political warfare'. Hence, almost any contemporary conflict can be described as hybrid[19]. The term has become so broad that it often loses analytical sharpness: most wars display hybrid features, so the adjective adds little beyond signalling current Western anxieties[20]. Others have argued that the supposedly novel labels merely rediscover the enduring logic of grand strategy from Clausewitzian strategic theory: the integration of military, economic, informational and diplomatic means in pursuit of political ends[21].

Consequently, it is necessary to move beyond 'warfare' language when addressing domestic political orders. The use of 'hybrid threats' or 'hybrid interference' is more appropriate in capturing Russian practices directed at democratic institutions, *inter alia*: illicit political financing, election manipulation, disinformation, cyber-attacks, energy leverage and the mobilisation of oligarchic networks[22]. In the context of EU enlargement countries rather than open war, 'hybrid' denotes a toolkit not only for keeping target states in a grey zone between war and peace but also for obstructing reform and EU accession. This approach reserves 'hybrid warfare' for actual modes of war, while adopting 'hybrid interference' as a focused, strategy-centred concept for analysing and contesting hostile state practices that target democratic processes in peacetime.

Hybrid interference occurs when a foreign state or its proxies deliberately coordinate at least two distinct types of instruments (for example, financial, informational, cyber, legal, economic or security-sector tools) over time to influence another state's domestic political decision-making, public opinion and institutional rules. It takes place under formal peacetime conditions and below the threshold of an open, attributable armed attack, explicitly or implicitly seeking to reshape the psychological environment – for instance by cultivating fear, dissatisfaction, distrust or nostalgia – so as to generate internal demands for political change.

On this basis, hybrid interference can be specified through a set of necessary attributes that together distinguish it from ordinary influence or diplomacy:

- Firstly, it presupposes external agency: the initiation, direction or decisive enablement of activity by a foreign state apparatus, including its intelligence services, state-owned enterprises or state-linked oligarchic networks.
- Secondly, the targets are domestic political structures and processes rather than battlefield outcomes: elections and party competition, coalition dynamics, constitutional and institutional reforms, foreign-policy orientation (such as EU or NATO membership) and the perceived legitimacy of core democratic institutions.
- Thirdly, hybrid interference requires multi-tool orchestration. At least two distinct categories of instruments must be deployed in a mutually reinforcing way, for example: illicit political financing combined with media capture; cyber-attacks coordinated with disinformation campaigns; or energy leverage paired with legal and institutional capture.

---

[19] R. Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies*, Vol 29, No 1, 2019, pp. 141–163.

[20] R. Johnson, 'Hybrid War and Its Countermeasures', *Small Wars & Insurgencies*, Vol 29, No 1, 2019, pp. 141–163.

[21] M. Caliskan, 'Hybrid warfare through the lens of strategic theory', *Defense & Security Analysis*, Vol 35, No 1, 2019, pp. 40–58.

[22] L. Pitaval, 'The shadow of the bear: The role of Russian interference and hybrid warfare in the 2024 elections in Georgia and Moldova and their impact on EU accession prospects'. *Relações Internacionais*, 2025, pp. 40–52.

- Fourthly, it operates in a grey-zone environment: formally in peacetime, heavily reliant on deniability and proxies, exploiting legal ambiguity and calibrated carefully to stay below thresholds that would trigger collective-defence obligations or overt military retaliation.
- Fifthly, such campaigns seek identifiable psychological effects on the target society: deliberately cultivated fear (of war, chaos, economic collapse or abandonment), chronic dissatisfaction, distrust, nihilism, as well as cynicism toward institutions, elections and media, together with nostalgia or identitarian longing for a supposedly more legitimate past order (for instance, the Soviet Union or 'traditional' values). The strategic aim is to make these diffuse sentiments strong enough that segments of the public themselves, without necessarily recognising an external hand, demand political change by voting for 'pro-interferer' parties, tolerating democratic backsliding or resisting EU-aligned reforms.
- Finally, there must be a demonstrable direction of effect: even if outcomes are not fully controlled, empirical evidence should show that these operations systematically shift incentives and perceptions for domestic actors, for example by altering resource asymmetries, reshaping media agendas or reframing key issues, in ways that align with the foreign actor's preferences. Only when all these conditions are met does coordinated external action qualify as hybrid interference in the sense defined above.

3 Patterns of Russian interference: Exploiting the vulnerabilities across the Western Balkan countries and the Eastern neighbourhood

Russia's ability to conduct hybrid interference in the Western Balkans and Eastern Partnership countries rests on a recurrent set of seven main structural vulnerabilities. The first and most pervasive weakness is intense political polarisation combined with fragile coalition politics, which makes it difficult to sustain stable, pro-reform majorities, creating repeated opportunities for obstruction and spoiler behaviour. Furthermore, factional competition and low trust in political institutions allow external actors to amplify grievances and block policy continuity.

This is closely linked to a second subset of sensitivities, namely unresolved ethnic, constitutional and status disputes, which provide Russia with ready-made narratives and local partners. Disputes over the constitutional set-up of Bosnia and Herzegovina, the status of Kosovo, the position of Republika Srpska, identity and language issues in North Macedonia, as well as the territorial integrity of Georgia and Moldova, generate contested sovereignties that Moscow can frame as needing its protection or mediation. In Ukraine, the combination of earlier 'frozen conflict' arrangements and Russia's full-scale invasion underscores how territorial pressure can evolve from hybrid interference into open war, while still retaining grey-zone elements in occupied and frontline regions.

A third cluster of vulnerabilities concerns information ecosystems and societal trust. Information ecosystems have three constituting elements: (1) physical infrastructure, such as information technologies, tools and media; (2) actors that produce, consume, curate and/or share information; (3) complex and adaptive sets of social relationships through which information is exchanged and interpreted[23]. In this context, information becomes an important resource and controlling it, for example, how it is produced or interpreted, can be a source of influence. Trust, on the other hand, can be viewed as an intentional construct implying that an individual or a group is willing to depend or rely on another actor with a feeling of relative

[23] Internews, Why information matters: A foundation for resilience, May 2015.

security[24]. These intentions can be determined by the trustor's traits of personality; beliefs that the trustee is competent, benevolent, has integrity and is predictable in their behaviour; and by institutional frameworks that are stable and provide transparent guarantees, rules, regulations and procedures[25]. Consequently, by influencing information flows as well as public perceptions of political institutions, it is possible to disrupt otherwise social relationships and destabilise communities.

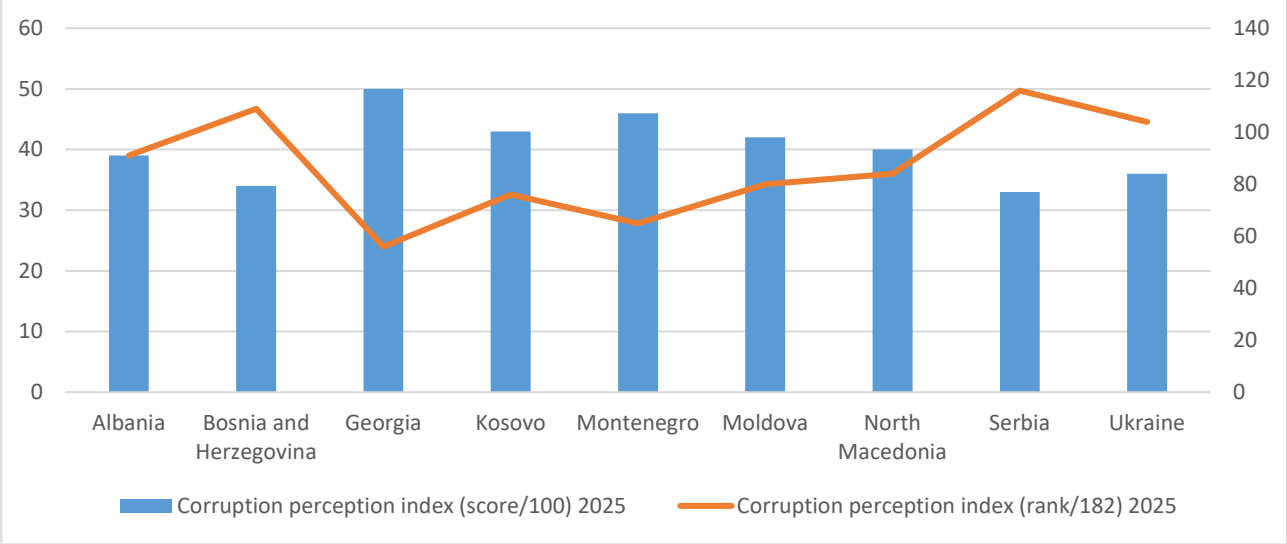
In almost all of the countries examined – Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia, Georgia, Moldova and Ukraine – media systems are fragmented, regulatory authorities are fragile or politicised and social media plays a major agenda-setting role. This makes them highly exposed to disinformation, conspiracy narratives and Russian state or proxy outlets, which can operate via local television channels, online portals, Telegram networks and church-linked or oligarch-owned media. In Georgia and Moldova, Russian information operations have directly targeted elections and referendums, combining social-media campaigns with covert funding and the mobilisation of proxy parties and oligarch networks. In the Western Balkans, pro-Russian narratives rely on local grievances, anti-Western sentiment and conspiracy theories, while religious and cultural affinity channels, such as the Orthodox Church, Slavic solidarity, or traditional values discourse, amplify Moscow's messaging. Low trust in institutions, high perceptions of corruption and repeated disappointments with reforms further increase societal receptivity to such narratives in all nine countries, whilst undermining the EU enlargement process from within candidate countries.

Institutional weakness and corruption form a fourth core area of vulnerability. Weak rule of law, clientelist networks and limited enforcement capacity create conditions within which Russian state and non-state actors can buy influence, capture regulators and launder money. Figure 1 shows the values of Transparency International's Corruption Perception Index[26] across the nine enlargement countries, along with their rank in the index. The data shows that some countries, such as Georgia, outperform EU Member States such as Greece, Malta, Slovakia, Croatia, Romania, Bulgaria and Hungary in terms of perceived corruption in the country. However, this should not necessarily be interpreted as evidence of strong institutional resilience in Georgia but rather as an indication that the listed EU Member States may also remain vulnerable to hybrid interference.

Bosnia and Herzegovina, Serbia, Montenegro, Moldova, Georgia and Kosovo are particularly exposed but Albania and North Macedonia also struggle with politicised administrations and incomplete anti-corruption reforms. In Georgia and Moldova, oligarchic structures have repeatedly acted as conduits for Russian leverage, while Georgian legislation facilitating tax-free offshore fund transfers increases the risk of sanctions circumvention[27]. In Bosnia and Herzegovina, institutional fragmentation and competing centres of authority – especially the Republika Srpska entity's leadership – open space for selective implementation of EU sanctions and for direct deals with Russian state bodies[28]. Across the Western Balkans, state capture and politicisation of regulators, including media and election commissions, facilitate both domestic and foreign manipulation of democratic processes.

[24] See D. H. McKnight and N. L. Cherrany, 'Trust and Distrust Definitions: One Bite at a Time', in R. Falcone et al (eds), *Trust in Cyber-societies,* Springer-Verlag, Berlin Heidelberg, 2001, pp. 27-54.
[25] D. H. McKnight and N. L. Cherrany, 'Trust and Distrust Definitions: One Bite at a Time', 2001, pp. 27-54.
[26] Transparency International, 'Corruption Perception Index', webpage, nd.
[27] European Commission, Georgia 2025 Report: Accompanying document to 2025 Communication on EU enlargement policy, SWD(2025) 757 final, 4 November 2025.
[28] European Commission, Georgia 2025 Report, SWD(2025) 757 final, 4 November 2025.

Figure 1: Corruption perception index in nine enlargement countries



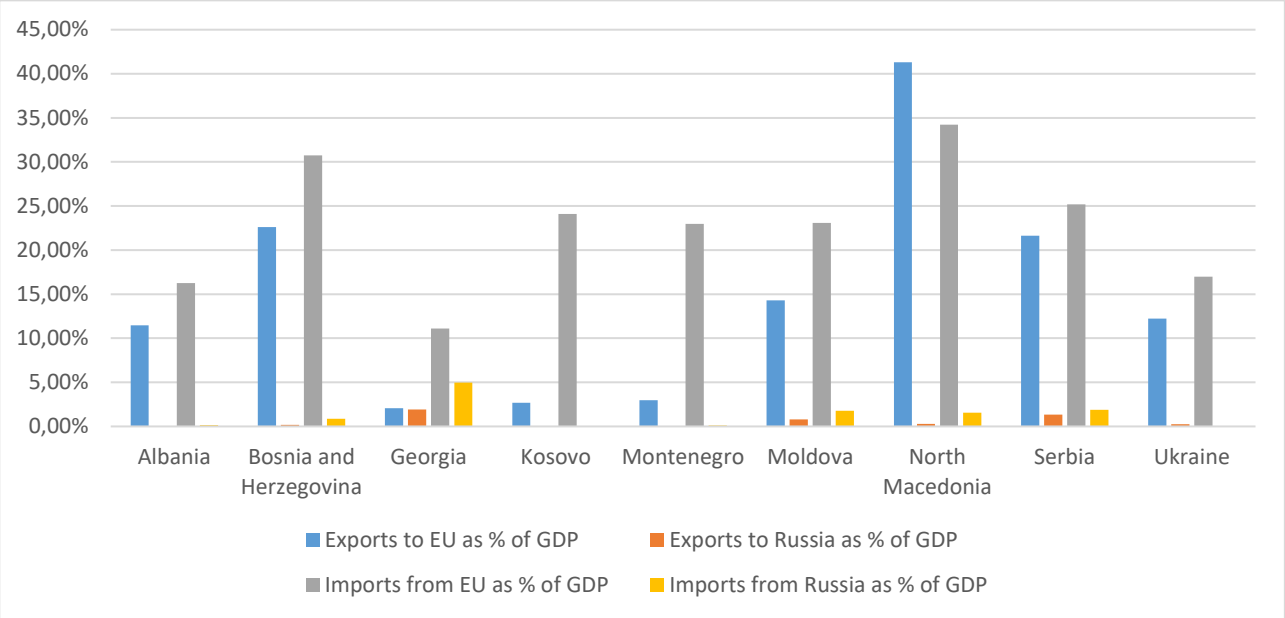
Source: Author's compilation based on Transparency International data (higher scores indicate less corrupt countries, higher ranks indicate more corrupt countries).

As a fifth set of weaknesses, Russian leverage also exploits economic and energy dependencies. Despite some diversification, Serbia, Bosnia and Herzegovina, Montenegro, North Macedonia, Moldova and Georgia have until recently relied heavily on Russian gas, oil or electricity supplies, as well as on Russian companies and financing in strategic sectors. This dependence creates coercive pressure points that can be used to shape regulatory decisions, delay alignment with EU energy rules or fuel price-based discontent. In Moldova and Georgia, energy vulnerability has historically been intertwined with the presence of Russian troops or peacekeepers in separatist territories, linking economic and hard-security pressure. While Ukraine has drastically reduced direct energy dependence since 2014, Russia continues to weaponise infrastructure and trade routes, including attacks on energy facilities and grain-export corridors, with knock-on socio-economic effects.

In terms of trade with Russia and the EU, Georgia seems to be the most dependent on Russian trade, with shares of exports and imports in the national economy being comparable to figures for the EU[29]. In all other cases, the EU is the dominant trade partner (see Figure 2).

[29] International Monetary Fund, 'International Trade in Goods (by partner country) (IMTS)', webpage, nd; World Bank, 'GDP (current US$)', webpage, nd.

Figure 2: Significance of trade with Russia and the EU for the nine enlargement countries



Source: Author's compilation based on International Monetary Fund and World Bank data.

A sixth set of vulnerabilities comprises security-sector and intelligence penetration, together with cyber and critical-infrastructure exposure. Serbia, Bosnia and Herzegovina, Montenegro, North Macedonia, Georgia and Moldova have all inherited or developed ties between parts of their security establishments and Russian services, ranging from formal cooperation agreements to informal networks involving former officers, paramilitaries and criminal groups. Across these countries, the most problematic links to Russian state structures concern intelligence cooperation, military ties and overlapping paramilitary-criminal networks. In military terms, Serbia is the clear outlier in the Western Balkans: it is the only country in the region to have a formal strategic partnership and military-cooperation agreements with Russia covering joint exercises such as 'Slavic Brotherhood', regular participation in Collective Security Treaty Organization drills, strategic information-sharing and arms sales, as well as parallel defence cooperation and significant arms purchases from China[30]. By contrast, the other Western Balkan states either belong to NATO or rely mainly on the USA, EU Member States and, to a lesser extent, Türkiye for military assistance and arms supplies, any cooperation with Russia and China being limited to *ad hoc* or low-intensity engagements (see Table 1 for data on arms imports by country).

Table 1: Volume of transfers of major arms (imports) by country, 2022-2025

Note: Figures are in millions of Stockholm International Peace Research Institute (SIPRI) Trend-Indicator Values. A '0' indicates that the volume of deliveries is between 0 and 0.5 million SIPRI Trend-Indicator Value. An empty field indicates that no deliveries have been identified.

Country	Supplier	2022	2023	2024	2025	Sum total years	% of total
Albania	Italy				20	20	32 %
	Bulgaria			19		19	30 %
	Türkiye			14	2	16	27 %
	United States		1	5	1	7	11 %
Bosnia and Herzegovina	Türkiye				1	1	100 %
Georgia	Türkiye			14		14	80 %

[30] M. Vulović, 'Western Balkan Foreign and Security Ties with External Actors', *SWP Comment* 2023/C 08, 9 February 2023.

	United States	2				2	14 %
	Poland		0	1		1	5.80 %
Kosovo	Türkiye	1	14			15	65.00 %
	United States				8	8	35.00 %
Moldova	France		10			10	48 %
	Israel				5	5	22 %
	Poland			4		4	17 %
	Germany		3			3	13 %
Montenegro	United States	2		6	1	8	92 %
	Germany				1	1	8.00 %
North Macedonia	United States	1	5	1	5	12	77 %
	Türkiye				4	4	23 %
Serbia	China	157	278	75	75	585	70 %
	France	5	13	56	40	114	14 %
	Cyprus		40			40	4.70 %
	Germany		3	10	13	27	3.20 %
	Spain		25			25	3.00 %
	Hungary			11		11	1.30 %
	Israel				10	10	1.20 %
	Denmark		8			8	0.90 %
	Belgium		1	3	3	6	0.70 %
	Russia				5	5	0.60 %
	United States	2		1	0	3	0.40 %
	Canada		3			3	0.40 %
Ukraine	United States	879	1834	2778	582	6074	41 %
	Germany	303	579	730	472	2084	14 %
	Poland	704	542	130	28	1405	9.50 %
	United Kingdom	265	156	158	116	695	4.70 %
	France	37	168	223	190	618	4.20 %
	Netherlands	59	26	84	273	443	3.00 %
	Czechia	153	93	147	30	423	2.80 %
	Canada	32	165	83	100	380	2.60 %
	Norway	17	55	130	136	337	2.30 %
	Denmark	32		143	80	256	1.70 %
	Slovakia	71	154		9	234	1.60 %
	Türkiye	181	23	16		220	1.50 %
	Jordan	2		216		218	1.50 %
	Italy	32	79	52	45	208	1.40 %
	Sweden	1	79	56	57	193	1.30 %
	Romania	1	1	123		125	0.80 %
	Australia	16	7	6	78	107	0.70 %
	Croatia	4	39	53		96	0.60 %
	Belgium	18	20	19	40	96	0.60 %
	Morocco	21	47	26		94	0.60 %

	Spain	12	25	56		93	0.60 %
	North Macedonia	31	59			90	0.60 %
	Qatar		54	20	2	76	0.50 %
	Portugal	2	8	37	1	47	0.30 %
	Slovenia	38	2	3		44	0.30 %
	Finland	2	20		15	36	0.20 %
	Greece	7	7	20	2	36	0.20 %
	South Korea	11	11	11		32	0.20 %
	Estonia	9	13	2		24	0.20 %
	Lithuania	12	8	3		23	0.20 %
	Latvia	10	7		1	18	0.10 %
	Bulgaria			14		14	0.10 %
	Unknown supplier(s)		9			9	0.10 %
	Ireland				7	7	0.00 %
	Bosnia-Herzegovina		6			6	0.00 %
	Montenegro	4				4	0.00 %
	United Arab Emirates	1	0	0		2	0.00 %

Source: SIPRI Arms Transfers Database[31].

However, issues related to intelligence cooperation are more concerning. For instance, in North Macedonia, leaked counter-intelligence documents show that Russian operatives, often working jointly with Serbian counterparts, conducted a long-term effort not only to recruit serving and former security personnel but also to cultivate assets in media and politics in order to derail NATO and EU integration[32]. Similar analyses point to unusually close cooperation between Russian agencies and Serbian intelligence services, described as operating on an almost 'open-book' basis that goes well beyond standard liaison practices and can be leveraged in relation to neighbouring Bosnia and Herzegovina and Montenegro[33]. Military links – including joint exercises, training activities and arms cooperation with Serbia and, indirectly, with security structures in Republika Srpska – further expand Russian access to sensitive intelligence and build personal networks within defence establishments[34].

In parallel, the role of informal networks in which former officers, nationalist paramilitaries and organised crime groups interface with Russian actors remains significant. For example, a loose ecosystem of proxy groups, Orthodox networks and oligarch-funded organisations that promote pro-Russian, ultra-nationalist and anti-Western narratives while maintaining plausible deniability has high potential to channel Russian influence. These actors form locally embedded networks that can be rapidly mobilised to support Kremlin objectives, including intimidation, protest and potential paramilitary training[35]. Included here are: biker clubs such as the Night Wolves; far-right formations, for example Serbian Honour and Narodne Patrole, as

[31] SIPRI, 'Arms Transfers Database', webpage, nd.
[32] A. Belford et al., 'Leaked Documents Show Russian, Serbian Attempts to Meddle in Macedonia', *Organized Crime and Corruption Reporting Project*, 4 June 2017.
[33] E. Vasilj, 'Russia's hybrid warfare and geoeconomics in Southeast Europe', *Defence24.com,* 12 November 2025.
[34] W. Zweers et al., Little substance, considerable impact: Russian Sources of Influence in Serbia, Bosnia and Herzegovina, and Montenegro, *Clingendael*, August 2023.
[35] W. Zweers et al., Little substance, considerable impact, *Clingendael*, August 2023.

well as Cossack and Orthodox structures; along with entities linked to figures like Konstantin Malofeev and facilities including the 'Humanitarian Centre' in Niš.

These links can facilitate access to sensitive information, impede reforms or sabotage pro-Western policy shifts. At the same time, all nine states face growing exposure to cyber intrusions against government institutions, media, civil society organisations and election infrastructure. EU and national reports highlight repeated cyber-attacks and Distributed Denial of Services (DDoS) campaigns linked to Russian actors, often synchronised with disinformation pushes and domestic political crises[36]. The limited resources and fragmented mandates of cybersecurity agencies in much of the region compound this vulnerability.

Finally, electoral processes *per se* are a critical point of weakness. Elections, referenda and major protest cycles offer high-value opportunities for hybrid interference, combining covert financing, media manipulation, strategic leaks, cyber-attacks and on-the-ground agitation. In Georgia and Moldova, recent electoral cycles have seen extensive attempts to distort competition and polarise public debate, including the use of Artificial Intelligence-driven bots and cross-platform campaigns, such as Facebook or Telegram, linked to Russian interests[37]. In Serbia, Montenegro, North Macedonia and Bosnia and Herzegovina, politicised electoral commissions, media capture and weak enforcement of campaign-finance rules leave elections vulnerable to both domestic and external manipulation. Even in Albania and Kosovo, where governments are strongly pro-EU, limited media pluralism, online disinformation and low trust in institutions create openings that hostile actors can exploit to depress turnout, discredit results or delegitimise pro-reform forces. Ukraine, under conditions of war, faces the most extreme form of electoral and institutional vulnerability, as Russian military and information operations directly target state capacity and the basic conditions for democratic competition.

All these vulnerabilities can be exploited by state and non-state actors from Russia. When hybrid interference can be traced to formal state institutions, it is rather straightforward to react to it. However, non-state actors without a clearly identifiable formal mandate whose interests and goals broadly align with those of the Kremlin can operate with varying degrees of autonomy and further complicate the patterns of interference and ensures a degree of plausible deniability for Moscow. For example, Wagner Group, as a private military company, was dismissed by Russian officials between 2011 and 2021 but by the end of 2021, the legality of private military companies was confirmed by Russian Foreign Minister, Sergey Lavrov, for the first time[38]. In 2022, Wagner Group was actively recruiting in Russian prisons and started playing an important role in the war against Ukraine but an open competition for power manifested in the 'march of justice' by Yevgeniy Prigozhin, a founder of Wagner Group, marked the beginning of the fall of the group[39]. Prigozhin was eventually killed in a plane crash in August 2023 but his legacy lives on as the Kremlin has effectively absorbed not only Wagner Group through Africa Corps, with closer connections to the state than its predecessor[40] but also 'troll farms' – notorious for interfering in the 2016 US presidential elections[41] – through the Internet Research Agency[42]. According to some reports, Prigozhin controlled about 15 000

---

[36] See A. Morson, 'DDoS Attacks on Moldova's September 2025 Elections: Real-Time Cybersecurity Analysis', *Mazebolt*, 29 September 2025; Defence Forces of Ukraine, 'In 2025, SSU Cyber Specialists Repelled More Than 3,000 Enemy Cyberattacks on Ukrainian Systems', *Armyinform*, 27 January 2026; C. Bômont and B. Zorić, Shared threats, shared resilience: Integrating enlargement partners in EU digital and cyber security, *EU Institute for Security Studies*, May 2026.

[37] See, V. Olari and E. T. Brooking, 'Cross-platform campaign sows anti-Europe division in Moldova', *DFRLab*, 26 March 2025; EEAS, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards, March 2026.

[38] K. P. Larsen, The rise and fall of the Wagner Group: Russia is seeking control over its 'private' military companies, *Danish Institute for International Studies*, January 2025.

[39] K. P. Larsen, The rise and fall of the Wagner Group, *Danish Institute for International Studies*, January 2025.

[40] K. P. Larsen, The rise and fall of the Wagner Group, *Danish Institute for International Studies*, January 2025.

[41] M. Markelov, 'I investigated millions of tweets from the Kremlin's "troll factory" and discovered classic propaganda techniques reimagined for the social media age', *The Conversation*, 1 October 2024.

[42] S. Poliakoff, 'Trolls Behind the Mask of Journalists: How Yevgeny Prigozhin's Patriot Media Group Was Organized', *Problems of Post-Communism*, Vol 72, No 5, 2025, pp. 416–428.

accounts in VK – a Russian social media platform – most of which started working against him around May 2023[43]. As Prigozhin's 'march of justice' and public confrontation with the Russian Ministry of Defence was triggered by the lack of success of the Russian military in the war in Ukraine, the dynamics of the war can lead to tighter control of the domestic realm in Russia. This may refer to political competition within the Russian elite as well as tighter control of the information space and citizens' access to and use of social media. Consequently, various types of actors and their varying interests in propagating Russian hybrid interference, together with the internal political dynamics and the developments in the war in Ukraine, can all affect the Russian strategy of exploiting vulnerabilities of the EU enlargement countries.

Taken together, these vulnerabilities form an interconnected ecosystem rather than separate risk categories. Political polarisation and unresolved status disputes feed information-space fragility; weak institutions and corruption magnify the impact of energy dependence and security-sector penetration; cyber- and media-system weaknesses make elections a recurring point of leverage. Russia's hybrid interference strategy systematically exploits these linkages, not only seeking to keep the Western Balkans and Eastern candidates in a grey zone between consolidation and destabilisation but also to slow or derail their path towards the EU[44].

4 Russian hybrid interference: Exploring the tactics - discussion of individual instruments and their use in empirical context

Russian hybrid interference in EU enlargement countries is best understood not as a set of country-specific episodes but as a repeatable toolkit of instruments that can be combined and adapted across contexts. Each instrument of leverage targets specific vulnerabilities – from party finance and media ecosystems to energy dependence and security-sector gaps – and is redeployed in different configurations not only in the six Western Balkan states but also in Georgia, Moldova and Ukraine. This section treats those instruments as main units of analysis and illustrates their use across all nine countries.

4.1 Covert and illicit political financing

One of Russia's most potent tools is simply pouring money into the target country in a covert or illicit manner for political purposes. Such financing is designed to tilt electoral competition, create proxy parties and widen the resource gap between pro-Russian and pro-EU forces in order to undermine the process of EU integration. In Moldova, this instrument has reached a high level of sophistication. Networks linked to fugitive oligarch Ilan Shor channelled large sums into vote-buying, mobilisation and media support not only around the 2024 presidential election and EU accession referendum but also ahead of the 2025 parliamentary elections, using shell companies, cash couriers and increasingly cryptocurrency rails to move money via Russian state-owned Promsvyazbank and encrypted apps such as TAITO[45]. Moldovan authorities seized substantial amounts of cash from couriers returning from meetings with Shor in Moscow and later traced millions of euros through crypto wallets, showing how illicit finance underpinned efforts to purchase around 300 000 votes in a small political market[46].

---

[43] P. Sauer and J. Burke, '"He lived by the troll, he dies by the troll": Putin takes on Prigozhin's business empire', *The Guardian*, 5 July 2023.

[44] I. Burmester, 'Soft Hegemony in the Shared Neighbourhood: How the European Union and Russia Co-opted Moldovan and Armenian Societies between 2000 and 2021', *Europe-Asia Studies*, Vol 77, No 3, 2025, pp. 389–414; K. Kakachia and B. Lebanidze, 'Can small states reshape their regional identities? Examining Georgia's cognitive dissonance between South Caucasus and Eastern Europe', *Nationalities Papers*, 2025, pp. 1–15.

[45] A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

[46] A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, February 2026; L. Pitaval, 'The shadow of the bear: The role of Russian interference and hybrid warfare in the 2024 elections in Georgia and Moldova and their impact on EU accession prospects', *Relações Internacionais*, 2025, pp. 40–52.

Similar patterns appear in Montenegro, albeit on a smaller and more opaque scale. Investigative reporting and regional think-tank work have documented Russian or Russia-linked funds entering Montenegro's party system via offshore structures, energy and real-estate deals, together with support for groups opposing NATO and EU integration[47]. In Bosnia and Herzegovina, covert and illicit finances flow through longstanding ties between Russian actors and party-linked business networks in Republika Srpska, providing resources for maintaining patronage networks and enabling media capture without always leaving a clear evidentiary trail. Serbia, with its dense economic and energy connections to Russia, has likewise seen recurrent concerns about opaque funding of pro-Russian parties, associations and media, even if direct attribution is often politically contested.

Even in countries where Russia has less political traction, this financing tool still appears in a more opportunistic form. For instance, in Albania, reports from 2018 and 2019 document attempts to establish covert influence channels and penetrate administrative structures, rather than build full-blown proxy parties[48]. In North Macedonia and Kosovo, donor opacity around pro-Russian and/or anti-Western media outlets, political movements and civil-society-type organisations amplifying pro-Russian messaging and anti-Western narratives has raised concerns about indirect financial support via regional networks centred on Serbia[49]. However, Ukraine shows the most intensive manifestation of this pattern: Russian intelligence and oligarchic networks used party financing, business leverage and local intermediaries to sustain pro-Kremlin political projects, illustrated by the cases of Dmitry Firtash and Viktor Yanukovich[50], in the years before and after 2014, even as open war escalated[51].

Across these cases, covert political finance works by altering incentives and capacities within domestic politics rather than through overt diplomatic pressure. It reduces parties' reliance on domestic fundraising, creates asymmetries in campaign resources and binds key actors to Moscow through financial dependency. The Moldovan experience demonstrates that this is a highly potent tool but also that, through coordinated law-enforcement action and legal reform, it is possible to significantly increase the costs associated with its use. Montenegro and Bosnia illustrate how entrenched economic interests can make government response to covert and illicit financial activities more difficult.

4.2 Disinformation, propaganda and information space

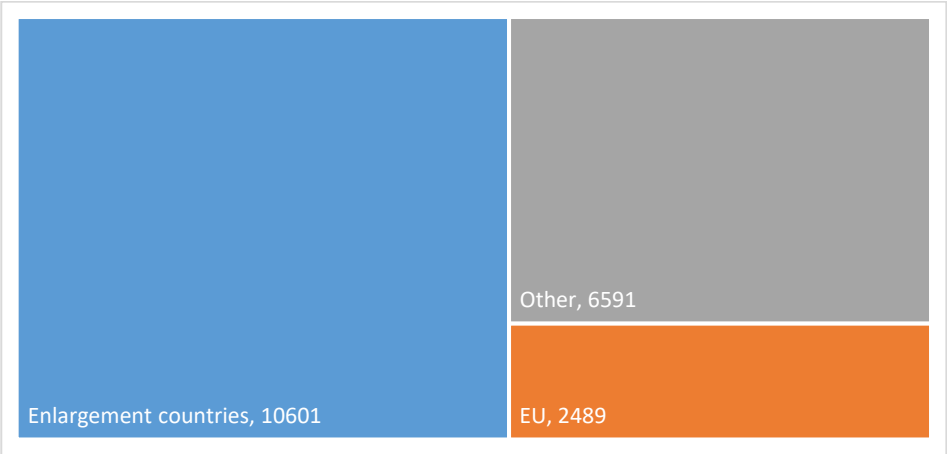
Information operations are the most ubiquitous instrument in Russia's hybrid toolkit. Instead of relying solely on overt state media, Russia increasingly launders narratives through local outlets, social media ecosystems and sympathetic elites. Narrative laundering, similar to money laundering, describes a process in which Kremlin-linked propaganda passes through different layers of intermediaries and outlets, so that its origin is obscured. Tracing it back to the Kremlin becomes difficult as various credibility-building tactics gradually lead to the normalisation of this processed content in public debate, enabling fringe falsehoods to circulate widely and influence mainstream narratives[52].

In Bosnia and Herzegovina, Russian narratives – including justifications of the war in Ukraine as well as attacks on the EU and NATO – circulate heavily through Serbian-language media tied to Serbia and Republika Srpska, as well as through local portals that rebroadcast RT and Sputnik content without formal branding. These narratives are particularly influential during elections and constitutional crises, where they

[47] Interview with an independent journalist from Montenegro, 3 February 2026, online.
[48] R. Zamfir, Risks and Vulnerabilities in the Western Balkans, *NATO Strategic Communications Centre of Excellence*, April 2020.
[49] Interview with a policy expert from North Macedonia, 3 February 2026, online. See also: M. Asllani, 'Domestic Actors Fuel Russian Disinformation in the Western Balkans', *Bloomsbury Intelligence and Security Institute*, 22 August 2025; Institute for Strategic Dialogue, Monitoring Influence & Disinformation Campaigns in the Western Balkans (MEDIWEB), 2024.
[50] S. Grey et al., 'Special Report: Putin's allies channeled billions to Ukraine oligarch', *Reuters*, 26 November 2014.
[51] A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.
[52] Center for Information Resilience, 'How the Kremlin launders disinformation around the globe', 15 May 2024.

reinforce nationalist grievance frames and normalise secessionist positions. Furthermore, according to the EUvsDisinfo database, between 1 January 2015 and 29 April 2026, the East Stratcom Task Force, created to counter Russian disinformation in the EU, its neighbourhood and beyond, identified 19 681 cases of pro-Kremlin disinformation, more than half of which target enlargement countries, while 13 % of cases approximately target the EU (see Figure 3). This indicates that pro-Kremlin outlets disproportionately target the enlargement countries, suggesting an underlying political agenda.

Figure 3: Distribution of pro-Kremlin disinformation cases



Source: Author's compilation based on EUvsDisinfo database[53].

Montenegro has faced similarly dense information interference. Studies of Russian influence in the Western Balkans show how Moscow used Serbian and local media to attack Montenegro's NATO accession, amplify clerical protests and depict pro-Western governments as corrupt, anti-Serb and anti-Orthodox[54]. Pro-Russian television channels and online outlets, some linked to business interests close to Russia, have repeatedly spread disinformation about the EU, NATO and domestic opponents of pro-Kremlin parties. North Macedonia's information space has also been saturated with disinformation, particularly during the 'name' dispute as well as subsequent referenda and elections, with Russian narratives framing EU-NATO integration as a threat to national identity[55].

In Albania, systematic monitoring shows that anti-NATO and anti-EU narratives originating from Russian officials and state media have been widely recycled by local outlets, even though there is no strong pro-Russian constituency[56]. The mechanism is narrative laundering: Russian statements are translated, excerpted and re-framed as 'news', entering domestic debate via under-resourced and weakly regulated media. Kosovo experiences similar processes during security crises in the north, with Russian and Serbian Telegram channels and portals portraying Kosovo as an illegitimate, Western-imposed entity and NATO as an aggressor[57].

Georgia, Moldova and Ukraine have been long-standing testbeds for Russian information warfare. Transparency International Georgia has documented systematic campaigns framing the EU and NATO as existential threats to Georgian values and security, often using fear of war and loss of sovereignty as central

[53] EUvsDisinfo, 'Database', webpage, nd.
[54] W. Zweers et al., Little substance, considerable impact: Russian Sources of Influence in Serbia, Bosnia and Herzegovina, and Montenegro, *Clingendael*, August 2023; B. Stanicek and A. Caprile, Russia's Influence in the Western Balkans: Geopolitical confrontation, economic influence and political interference, PE 747.096, *European Parliamentary Research Service*, April 2023.
[55] Interview with a policy expert from North Macedonia, 3 February 2026, online.
[56] E. Kaziaj and V. Keta, *The Distribution of Disinformation Narratives by Hostile Actors Against NATO and the EU in the Albanian Media*, Balkan Investigative Reporting Network, Tirana, 2024; National Democratic Institute, The Vulnerability of Albanian Politics to Foreign Interference, June 2024.
[57] Interview with a university professor of West Balkan politics, 4 February 2026, online.

tropes[58]. In Moldova, it has been shown how Russian-linked actors used TikTok and other platforms to spread fears about war, mobilisation and loss of identity, attempting to swing the 2024 presidential election and concurrent referendum, the latter aimed at bringing about constitutional change signalling EU aspirations[59]. In Ukraine, Russian propaganda via television, online platforms and social media has for years framed the Kyiv government as 'Nazi' and the West as puppet-master, justifying both the 2014 aggression and the 2022 full-scale invasion[60].

Based on the EUvsDisinfo database, it can be argued that the countries of the Eastern trio, particularly Ukraine, are priority targets for Russian disinformation efforts. The three countries together account for the vast majority of disinformation cases featured in the database. Ukraine is the most frequent target with over 86 % and 46 % share of cases referring to enlargement countries and the total number of cases, respectively. However, a more telling story emerges when trends before and after the invasion of Ukraine are observed. The average number of days it takes to register a single case of disinformation targeting a given enlargement country has increased across the board, except for Moldova and Ukraine. This indicator describes the intensity of disinformation across the nine countries. The data shows that the intensity of disinformation has fallen since the invasion of Ukraine in all enlargement countries but Moldova and Ukraine (see Table 2).

Table 2: How many days does it take on average to produce one case of disinformation discussing a given enlargement country?

#	Country	1 Jan 2015 – 23 Feb 2022	24 Feb 2022 – 29 Apr 2026
1	Albania	174	No cases of disinformation
2	Bosnia and Herzegovina	114	254
3	Georgia	5.5	7.7
4	Kosovo	65	76
5	Moldova	9.6	7.3
6	Montenegro	90	1526
7	North Macedonia	137.4	No cases of disinformation
8	Serbia	29	34
9	Ukraine	0.5	0.4

Source: Author's calculations based on the EuvsDisinfo database[61]. The numbers are given in days calculated by dividing the total number of days in each period by the number of disinformation cases discussing the given country in that period.

Three conclusions can be drawn from this data. Firstly, Georgia, Moldova and Ukraine are the top priorities for Russia, followed by Serbia and Kosovo, while the rest of the enlargement countries are less prioritised. Secondly, the decreasing frequency of cases in Georgia indicates that Russia does not need to engage with Georgia as much as before, probably because of the current political discourse in Georgia. Finally,

[58] S. Tsetskhladze, Spreading Disinformation in Georgia: state approach and countermeasures, *Transparency International Georgia*, 2023.

[59] L. Pitaval, 'The shadow of the bear: The role of Russian interference and hybrid warfare in the 2024 elections in Georgia and Moldova and their impact on EU accession prospects', *Relações Internacionais*, 2025, pp. 40–52.

[60] N. Mihaylov, 'Cyber Dimensions of a Hybrid Warfare', *CyberPeace Institute*, 8 April 2025; M. Galeotti, The Secret Battlefield: How the EU Can Help Georgia, Moldova and Ukraine Protect Against Russian Subversion, *European Council on Foreign Relations*, December 2021.https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/705166266/cb7e3aac-6755-44cc-8cad-a19b5c7e91b0/RI_SPECIAL_ISSUE_2025_LucasPitaval-10.pdf

[61] EUvsDisinfo, 'Database', webpage, nd.

increasing disinformation campaign activity in Moldova and Ukraine may limit and deprioritise Russian efforts elsewhere.

Across all nine countries, the impact of this instrument is cumulative rather than immediate, producing the following effects over time: corroding information integrity; deepening polarisation; and normalising conspiracy frames that align with Moscow's interests. The Bosnian and Montenegrin cases show how information operations are especially dangerous in exploiting unresolved identity disputes and media capture.

4.3 Legal and constitutional obstruction via proxy elites

Another cross-cutting instrument of Russian hybrid interference is the use of domestic elites and legal-constitutional levers to obstruct pro-EU reforms, delegitimise oversight institutions and entrench friendly regimes. Bosnia and Herzegovina offers one of the clearest examples. Russia has consistently backed Milorad Dodik and the Republika Srpska leadership in their efforts to undermine the High Representative for Bosnia and Herzegovina, resist alignment with EU sanctions on Russia and threaten secession[62]. This backing is diplomatic and political rather than purely covert: Russian officials meet Dodik, support his positions in international fora and frame EU pressure as anti-Serb persecution. The result is a chronic weakening of Bosnia's constitutional order and a steady erosion of the Dayton framework's legitimacy – a 1995 peace settlement following the three-year Bosnian war, which preserved Bosnia and Herzegovina as a single state but with two constituting entities: Federation of Bosnia and Herzegovina together with Republika Sprska[63].

In Montenegro, Russia has leveraged sympathetic political forces and clerical networks to obstruct or reverse reforms tied to NATO and EU integration, including laws on religious property and security-sector reform[64]. Legal battles around the Serbian Orthodox Church's status and attempts to roll back pro-Western policies after elections, illustrate how formal institutions can become vehicles for hybrid interference when captured by elites aligned with Moscow[65].

Georgia has recently moved even closer to the Russian model[66], which is often characterised as an example of digital authoritarianism. Digital authoritarianism refers to powerholders using digital technology or a combination of digital and analogue and digital technology for repressive acts in order to undermine public opposition and retain political power[67]. The adoption of a 'foreign influence' law in 2024, explicitly inspired by Russia's 2012 'foreign agents' legislation, has provided Georgian Dream with a legal tool to stigmatise and constrain civil society, as well as media receiving Western funding[68]. Combined with electoral engineering, politicised prosecutions and the manipulation of oversight bodies, this legal architecture is gradually limiting the space for pro-EU actors, making Georgia more receptive to Russian leverage. Moldova, by contrast, has moved in the opposite direction by explicitly embracing 'militant democracy' – tightening party-finance and participation rules to exclude actors financed by Russia-linked oligarchs –

[62] D. Sito-sucic, 'Bosnian Serb Leader Dodik: From Western Darling to Pro-Russian Separatist', *Reuters*, 27 March 2025.
[63] OSCE, 'OSCE Mission to Bosnia and Herzegovina', webpage, nd; OSCE, The General Framework Agreement for Peace in Bosnia and Herzegovina, 14 December 1995.
[64] W. Zweers et al., Little substance, considerable impact: Russian Sources of Influence in Serbia, Bosnia and Herzegovina, and Montenegro, *Clingendael*, August 2023.
[65] Interview with a researcher working on Bosnia and Herzegovina, 9 April 2026, online.
[66] Free Russia Foundation, How Georgia Turned towards the Kremlin and Cracked down on Pro-Western Dissent, February 2026.
[67] T. Roberts, and M. Oosterom, 'Digital authoritarianism: a systematic literature review', *Information Technology for Development*, Vol 31, No 4, 2025, pp. 860–884.
[68] I. Sirbiladze, 'Anti-democratic, anti-Western, and Russia-friendly governing elites as enablers of Russian influence in Georgia', in A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

thus seeking to close legal pathways for interference[69]. Although it is difficult to assess to what extent the EU support has contributed to this strategy, a shifting paradigm from democracy promotion towards democracy protection[70] in the context of the enlargement policy has potentially facilitated the Moldovan strategy.

Serbia, North Macedonia and, to a lesser extent, Kosovo and Albania show milder but still significant forms of this instrument: politicised regulators, discretionary enforcement and weak judicial independence. All create room for Russia-friendly actors to block or dilute reforms that would reduce Moscow's leverage, especially in the media, security and energy sectors[71]. In Ukraine, pre-2014 laws and elite structures constrained Kyiv's ability to align with the EU and NATO, while Russia's post-2014 military aggression has combined with legal-political pressure in occupied territories to undermine Ukrainian sovereignty from within[72].

Legal obstruction is thus not only an internal governance problem; it is also an instrument of hybrid interference when external actors cultivate and sustain elites who weaponise constitutional and regulatory tools against democratic reform.

4.4 Energy, economic and oligarchic leverage

Energy dependence and oligarchic economic networks constitute another central instrument that Russia deploys across the nine countries. In Montenegro and Serbia, Russian companies have historically held significant stakes in key sectors, especially energy and metallurgy, providing Moscow with influence over pricing, investment and employment[73]. Threats of supply disruption, preferential pricing and long-term contracts have been used to shape national debates on sanctions, diversification and alignment with EU energy policy[74].

Bosnia and Herzegovina has been similarly vulnerable, with Republika Srpska in particular maintaining strong energy and economic ties to Russia, which the entity leadership uses to justify resistance to EU energy rules and sanctions[75]. In North Macedonia and other Western Balkan states, Russian gas and oil imports have been declining but still provide leverage, especially in moments of price spikes and infrastructure disputes[76].

Moldova and Georgia illustrate how energy dependence and oligarchs interact. In Moldova, reliance on Russian gas and electricity supplies via Transnistria has historically given Moscow both economic and hard-security leverage, while oligarchs with business ties to Russia (such as Shor and Platon) have used their positions to mediate political influence inside the country[77]. Georgia's legislation facilitating tax-free offshore fund transfers and its role as a hub for potential sanctions circumvention have similarly raised

[69] G. Capoccia, 'Militant Democracy: The Institutional Bases of Democratic Self-Preservation', *Annual Review of Law and Social Science*, Vol 9, No 1, 2013, pp. 207–226; A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

[70] A. Tyushka, Engagement, Enlargement and Estrangement: EU Democracy Promotion and Protection in its Eastern Neighbourhood in-between Three Relational Paradigms, *REUNIR – Occasional Paper*, 2025.

[71] Interview with a university professor of West Balkan politics, 4 February 2026, online.

[72] Interview with a researcher of Ukrainian politics, 10 April 2026, online.

[73] W. Zweers et al., Little substance, considerable impact: Russian Sources of Influence in Serbia, Bosnia and Herzegovina, and Montenegro, *Clingendael*, August 2023.

[74] Interview with an independent journalist from Montenegro, 3 February 2026, online.

[75] B. Stanicek and A. Caprile, Russia's Influence in the Western Balkans: Geopolitical confrontation, economic influence and political interference, PE 747.096, *European Parliamentary Research Service*, April 2023.

[76] Interview with a policy expert from North Macedonia, 3 February 2026, online.

[77] I. Burmester, 'Soft Hegemony in the Shared Neighbourhood: How the European Union and Russia Co-opted Moldovan and Armenian Societies between 2000 and 2021', *Europe-Asia Studies*, Vol 77, No 3, 2025, pp. 389–414.

concerns that economic arrangements enable Russian capital to sustain pro-government elites and blunt Western pressure[78].

Ukraine again stands at the far end of the spectrum. Before 2014, Russian energy and trade were central to Ukraine's economy; afterwards, Moscow's weaponisation of gas supplies, pipelines and industrial ties became part of the broader war effort, while oligarchs with Russia-linked interests played ambiguous roles in domestic politics. The subsequent diversification of Ukraine's energy mix has reduced but not eliminated this leverage, especially given Russia's continued attacks on energy infrastructure.

In Albania and Kosovo, where direct energy dependence on Russia is lower, economic leverage still appears through indirect channels – investment flows, tourism, or local business elites with interests in Russia-linked markets – but plays a smaller role than in Serbia, Montenegro, Bosnia and Herzegovina, Moldova, Georgia and Ukraine. Overall, energy and economic instruments allow Russia to create structural incentives for domestic actors to resist alignment with EU rules and sanctions, or to frame diversification as economically costly.

4.5 Cyber operations and technical sabotage

Cyber operations and technical sabotage form a distinct but closely integrated instrument across the region. Georgia experienced a landmark case in October 2019, when thousands of websites and a number of broadcasters were disrupted in a large-scale cyberattack later publicly attributed by Georgia, the United Kingdom and the USA to Russia's intelligence centre, Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)[79]. This attack demonstrated Russia's ability to target government, media and civil-society infrastructure, thereby underscoring the cyber domain as a routine front in Moscow's pressure on Georgia.

Ukraine has faced the most intense cyber onslaught. Since the annexation of Crimea, attacks have been conducted on its energy grid and since 2022 the range of targets has expanded. With the 2022 Viasat satellite disruption and thousands of cyber incidents against government institutions, defence and critical infrastructure, Russian cyber operations have sought to degrade state capacity and induce panic[80]. Ukrainian authorities report that a large share of recorded cyberattacks originate from Russia but note that the proportion of highly critical incidents has declined as defences have improved, which includes action through public-private partnerships and the creation of a dedicated cyber force[81].

Moldova has seen a rapid escalation of cyber interference since 2022: recorded incidents rose from 173 in 2018 to more than 1 300 in 2024 and the Central Election Commission faced massive DDoS attacks during the 2024 vote, with nearly 900 million malicious requests on election day alone[82]. Thanks to prior risk assessments and international support, critical systems withstood the assault but the episode shows how cyber operations now routinely accompany financial and informational interference in elections.

In Montenegro, government networks and media outlets have been targeted by suspected Russia-linked hackers, particularly after NATO accession and during domestic political crises, disrupting services and

[78] European Commission, Georgia 2025 Report: Accompanying document to 2025 Communication on EU enlargement policy, SWD(2025) 757 final, 4 November 2025.
[79] M. Antidze and J. Stubbs, 'Georgia, Backed by U.S. and Britain, Blames Russia for Paralysing Cyber Attack', *Reuters*, 20 February 2020.
[80] J. Pearson, 'Russia downed satellite internet in Ukraine -Western officials', *Reuters*, 10 May 2022; Reuters, 'Ukraine Blames Russia for Most of Over 2,000 Cyberattacks in 2022', 17 January 2023.
[81] State Service of Special Communications and Information Protection of Ukraine, 'Cyber Threats Ukraine: Analytics for the H2 2025', 2026.
[82] A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

leaking data in ways that fuel domestic mistrust[83]. Bosnia and Herzegovina, Serbia, North Macedonia, Albania and Kosovo have all experienced cyber incidents and probing of critical infrastructure, although attribution is often less clear and the capacity for forensic investigation is limited.

The pattern across countries is that cyber operations rarely stand alone; they are sequenced with disinformation campaigns, financial interference and diplomatic pressure. The Ukrainian, Georgian and Moldovan cases provide the clearest evidence base, while Montenegro and Bosnia illustrate how states with weaker cyber capacity can be kept under constant low-level pressure.

4.6 Security-sector penetration and support for proxy violence

Finally, Russian hybrid interference often involves security-sector penetration and support for proxy violence or sabotage. Montenegro's 2016 coup plot remains a paradigmatic case: Montenegrin prosecutors and courts concluded that Russian GRU officers and Serbian extremists planned to storm parliament, assassinate the prime minister and block NATO accession, using local militants as proxies[84]. This operation combined intelligence tradecraft, cyber-attacks, paramilitary mobilisation and domestic political polarisation into a single violent scheme.

Bosnia and Herzegovina shows a subtler but ongoing version. Reports of paramilitary training in Republika Srpska, including camps linked to individuals associated with Russia's Wagner Group and the presence of armed formations loyal to Dodik's leadership, highlight how Russia-friendly actors can cultivate capacities for street violence and intimidation below the threshold of open conflict[85]. Russian backing for genocide denial and anti-Dayton narratives further contributes to an environment in which violence against opponents or central institutions can be legitimised.

In Kosovo, the 2023 Banjska attack, carried out by heavily armed Serbs and linked by Pristina to Serbian security structures, illustrates how local armed groups can be used to challenge state authority and test international responses. While there is no evidence of direct Russian operational control, Russian official rhetoric and media framing immediately shielded Serbian narratives and portrayed Kosovo as a Western puppet, providing political cover for potential escalation[86]. In Serbia itself, security-sector ties with Russia – including military cooperation, intelligence exchanges and training – have long raised concerns about Moscow's access to sensitive information and its capacity to influence security decisions[87].

Ukraine represents the most advanced and lethal use of this instrument. Russia has combined regular forces with proxy militias, covert operatives and recruited saboteurs inside Ukraine, using online platforms, criminal networks and economic incentives to direct attacks on infrastructure and gather intelligence. Georgia and Moldova also live under the shadow of Russian troops and security structures in separatist regions, which enable intelligence operations, coercive signalling and, potentially, renewed military action.

Albania has experienced lower-level but telling incidents, such as the 2022 Gramsh military plant espionage case. Russian nationals were arrested after attempting to photograph a former military facility, highlighting Russia's interest in mapping and probing defence infrastructure, even in strongly pro-Western[88] environments. North Macedonia has reported concerns about foreign links to radical groups and the need to strengthen oversight of security services to prevent infiltration.

---

[83] W. Zweers et al., Little substance, considerable impact: Russian Sources of Influence in Serbia, Bosnia and Herzegovina, and Montenegro, *Clingendael*, August 2023.
[84] W. Zweers et al., Little substance, considerable impact, *Clingendael*, August 2023.
[85] Interview with a researcher working on Bosnia and Herzegovina, 9 April 2026, online.
[86] Ministry of Foreign Affairs and Diaspora of the Republic of Kosova, Preliminary report: Initial Analysis of Serbia's Paramilitary Aggression on Kosova, 20 October 2023.
[87] W. Zweers et al., Little substance, considerable impact: Russian Sources of Influence in Serbia, Bosnia and Herzegovina, and Montenegro, *Clingendael*, August 2023.
[88] Reuters, 'Albania Arrests Two Russians, One Ukrainian Trying to Enter Military Plant', 20 August 2022.

Across all nine countries, this instrument targets the core of democratic security: it uses or cultivates domestic armed actors to intimidate opponents, test state resolve and, in some instances, prepare the ground for more open aggression. Bosnia and Herzegovina, as well as Montenegro, alongside Ukraine, show how close such operations can come to tipping a fragile equilibrium into violent conflict.

Taken together, these six instruments – covert political finance, information operations, legal-constitutional obstruction via proxy elites, energy and economic leverage, cyber operations and security-sector penetration with proxy violence – form a modular toolkit that Russia uses and continues to reuse across enlargement countries (see Table 3). Apart from these instruments, Russia, along with Belarus, has been reported as instrumentalising migration and flooding the EU borders with migrants from countries such as Iraq or Afghanistan, targeting eastern EU Member States[89]. However, such weaponisation of migration does not target enlargement countries but rather aims at overwhelming the EU borders. Hence, this instrument is not covered in detail here. Furthermore, the specific configuration varies contextually but the underlying logic is consistent: keep states in a grey zone between stability and crisis, weaken their democratic institutions and slow or derail their path toward the EU. For EU policy, this perspective implies that counter-measures should be built around instruments as well as countries. These counter-measures include: closing financial loopholes; securing the information space; hardening legal frameworks against capture; diversifying energy; strengthening cyber defences; and insulating security sectors from penetration. All are mutually reinforcing tasks that must be addressed across the entire enlargement agenda.

Table 3: Structural vulnerabilities and Russian hybrid interference instruments in EU enlargement countries

Country	Main vulnerabilities	Main instruments of hybrid interference
Albania	Political polarisation and weak coalition politics; information-ecosystem fragility; institutional weakness and corruption; energy dependence and economic leverage; electoral processes	Covert and illicit political financing; disinformation and propaganda; cyber operations and technical probing
Bosnia and Herzegovina	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved ethnic, constitutional and status disputes; institutional weakness and corruption; energy dependence and economic leverage; security-sector and critical-infrastructure exposure; electoral processes	Covert and illicit political financing; disinformation and propaganda; legal and constitutional obstruction via proxy elites; energy, economic and oligarchic leverage; security-sector penetration and proxy violence
Georgia	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved ethnic, constitutional and status disputes; institutional weakness and corruption; energy dependence and economic leverage; security-sector and critical-infrastructure exposure; electoral processes	Covert and illicit political financing; disinformation and propaganda; legal and constitutional obstruction via proxy elites; energy, economic and oligarchic leverage; cyber operations and technical sabotage; security-sector penetration and proxy violence
Kosovo	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved	Covert and illicit political financing; disinformation and propaganda; legal and

[89] EU Agency for Asylum, '4.1.1. Situation on the eastern borders', *Asylum Report 2022*, May 2022.

Country	Main vulnerabilities	Main instruments of hybrid interference
	ethnic, constitutional and status disputes; security-sector and critical-infrastructure exposure; electoral processes institutional weakness and corruption;	constitutional obstruction via proxy elites; security-sector penetration and proxy violence
Moldova	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved ethnic, constitutional and status disputes; institutional weakness and corruption; energy dependence and economic leverage; security-sector and critical-infrastructure exposure; electoral processes	Covert and illicit political financing; disinformation and propaganda; legal and constitutional obstruction via proxy elites; energy, economic and oligarchic leverage; cyber operations and technical sabotage; security-sector penetration and proxy violence
Montenegro	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved ethnic, constitutional and status disputes; institutional weakness and corruption; energy dependence and economic leverage; security-sector and critical-infrastructure exposure; electoral processes	Covert and illicit political financing; disinformation and propaganda; legal and constitutional obstruction via proxy elites; energy, economic and oligarchic leverage; security-sector penetration and proxy violence
North Macedonia	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved ethnic, constitutional and status disputes; institutional weakness and corruption; energy dependence and economic leverage; security-sector and critical-infrastructure exposure; electoral processes	Covert and illicit political financing; disinformation and propaganda; legal and constitutional obstruction via proxy elites; energy, economic and oligarchic leverage; cyber operations and technical sabotage
Serbia	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved ethnic, constitutional and status disputes; institutional weakness and corruption; energy dependence and economic leverage; security-sector and critical-infrastructure exposure; electoral processes	Covert and illicit political financing; disinformation and propaganda; legal and constitutional obstruction via proxy elites; energy, economic and oligarchic leverage; security-sector penetration and proxy violence
Ukraine	Political polarisation and weak coalition politics; information-ecosystem fragility; unresolved ethnic, constitutional and status disputes; institutional weakness and corruption; energy dependence and economic leverage; security-sector and critical-infrastructure exposure; electoral processes	Covert and illicit political financing; disinformation and propaganda; legal and constitutional obstruction via proxy elites; energy, economic and oligarchic leverage; cyber operations and technical sabotage; security-sector penetration and proxy violence

Source: Author's own compilation.

5 Russian hybrid interference in practice: Comparing Georgia, Moldova and Serbia

This section investigates Russian hybrid interference in Georgia, Moldova and Serbia, with particular attention to: electoral manipulation in Moldova; the internalisation of a Russian authoritarian 'playbook' in Georgia; and Serbia's ambivalent efforts to reduce dependence on Moscow while remaining a hub for Russian influence. It further examines how unresolved ethnopolitical conflicts in Georgia and Moldova are instrumentalised as leverage, concluding by drawing lessons for EU enlargement and hybrid-threat policy.

5.1 Moldova: Elections as a laboratory of hybrid interference

Moldova has become one of the most intensively targeted laboratories for Russian hybrid operations in Europe, especially around electoral processes. The 2024 presidential election and concurrent constitutional referendum, followed by the 2025 parliamentary elections, were accompanied by an unprecedented combination of illicit financing, disinformation and cyber-attacks, as documented by international observers[90].

At the core of Russia's electoral interference stands the financial machinery linked to a pro-Russian fugitive oligarch and politician, Ilan Shor and his associated networks, which have channelled large volumes of illicit funds into Moldovan politics from abroad[91]. In the 2024 presidential election and EU referendum, Moldovan authorities and international observers reported extensive vote-buying schemes, opaque offshore transfers and the use of local brokers to distribute cash and in-kind benefits to targeted constituencies[92]. Investigations subsequently indicated that 'criminal entities' affiliated with Shor invested several million euros to purchase approximately 300 000 votes; around half of these cases were documented in subsequent judicial proceedings[93]. This interference directly altered voter incentives, subsidised pro-Russian media and online channels and reduced parties' reliance on domestic fundraising, thus reshaping the competitive environment.

The 2025 parliamentary elections saw an upgraded version of this 'playbook'. The Organization for Security and Co-operation in Europe (OSCE) Office for Democratic Institutions and Human Rights' (ODIHR) final report concluded that the elections were competitive and offered voters a genuine choice but were 'marred by serious cases of foreign interference, illicit financing, cyberattacks and disinformation', with many operations credibly attributed to actors in the Russian Federation[94]. Parallel analysis describes how Shor's network used the encrypted TAITO app, not only to coordinate tens of thousands of activists but also to hide financial flows routed via the sanctioned Russian bank Promsvyazbank and the rouble-denominated stablecoin A7A5[95]. Through this layered chain – rouble accounts, crypto currency, foreign currency conversion and cash-out in Lei – Russian funds were laundered into campaign activities, protests and vote-buying at scale[96]. Moldovan authorities estimated that Russia invested roughly EUR 200 million in the

[90] International Election Observation Mission, Republic of Moldova – Presidential Election and Constitutional Referendum, 20 October 2024: Statement of Preliminary Findings and Conclusions, 20 0ctober 2024; OSCE/ODIHR, Republic of Moldova – Parliamentary Elections, 28 September 2025: Final Report, 18 February 2026.

[91] S. Sandu, 'Moldova's 2025 Elections: A Test Case for Russia's Hybrid Warfare', *Stimson Center*, 2025.

[92] International Election Observation Mission, Republic of Moldova – Presidential Election and Constitutional Referendum, 20 October 2024: Statement of Preliminary Findings and Conclusions, 20 0ctober 2024.

[93] L. Pitaval, 'The shadow of the bear: The role of Russian interference and hybrid warfare in the 2024 elections in Georgia and Moldova and their impact on EU accession prospects', *Relações Internacionais*, 2025, pp. 40–52.

[94] OSCE/ODIHR, Republic of Moldova – Parliamentary Elections, 28 September 2025: Final Report, 18 February 2026.

[95] A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026; S. Sandu, 'Moldova's 2025 Elections: A Test Case for Russia's Hybrid Warfare', *Stimson Center*, 2025.

[96] S. Sandu, 'Moldova's 2025 Elections: A Test Case for Russia's Hybrid Warfare', *Stimson Center*, 2025.

2024 cycle and EUR 350 million in 2025, equivalent to about 2 % of Moldovan Gross Domestic Product, which underscores the strategic value Moscow attaches to Moldovan elections[97].

Information manipulation reinforced these financial operations. OSCE and Parliamentary Assembly of the Council of Europe observers noted widespread disinformation and media bias in favour of certain candidates in 2024. The information environment around the referendum and elections was saturated with narratives framing the EU as a source of war and economic hardship, exploiting fears of mobilisation and the presence of Russian troops in Transnistria[98]. TikTok and other social media platforms were heavily used to target younger voters with personalised, emotion-driven content; the scale of manipulation prompted domestic debates and EU-level discussions on the possible need to regulate or restrict such platforms[99].

Cyber operations formed a third pillar of Russia's hybrid interference. Not only did the cyber-incident statistics show a steep increase in attacks on Moldovan institutions but also on the day of the 2024 parliamentary vote, the Central Election Commission experienced massive DDoS attacks, with almost 900 million malicious requests; these were mitigated through prior risk assessments and support from private cybersecurity providers[100]. In 2025, OSCE/ODIHR again noted that cyberattacks targeted critical election infrastructure, though improved preparedness reduced their impact[101].

These instruments are intimately connected to Moldova's unresolved ethnopolitical conflicts. Transnistria, under *de facto* Russian military and political control since the early 1990s, remains a major blind spot for law enforcement and financial supervision: local banks tied to Russia operate outside the EU sanctions regime and electricity infrastructure is used as a base for opaque crypto-mining operations that can fund covert activities[102]. Gagauzia, an autonomous region with strong pro-Russian preferences, has been a focal point for Shor's networks and for Moscow's narrative of defending minority rights against an alleged 'Romanianisation' of Moldova[103]. These territorial and identity cleavages provide entry points for both financial and informational interference.

Crucially, Moldova is not merely a passive victim but an innovator in counter-strategies. The government has adopted what is often termed as 'militant democracy' – using legal restrictions on parties and media outlets financed by hostile foreign actors to safeguard democratic institutions[104]. Authorities have de-registered parties linked to Shor, strengthened campaign-finance oversight and pursued criminal investigations against vote-buying networks, while civil society and investigative journalists have played a central role in exposing schemes and tracing illicit flows[105]. At the narrative level, Moldovan actors have shifted from purely reactive debunking to 'prebunking' and positive messaging, emphasising the tangible benefits of EU integration to build resilience against Kremlin-driven fear campaigns[106].

As a result, despite intense interference, Moldova has managed to maintain a pro-EU trajectory, to constitutionalise its European orientation and to use the 2024–2025 electoral cycles as a learning process

---

[97] A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

[98] Interview with an expert from Moldova, 5 March 2026, online.

[99] S. Sandu, 'Moldova's 2025 Elections: A Test Case for Russia's Hybrid Warfare', *Stimson Center*, 2025.

[100] A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

[101] OSCE/ODIHR, Republic of Moldova – Parliamentary Elections, 28 September 2025: Final Report, 18 February 2026.

[102] Interview with a researcher of Moldovan politics, 16 January 2026, Zurich.

[103] Interview with a researcher of Moldovan politics, 16 January 2026, Zurich.

[104] G. Capoccia, 'Militant Democracy: The Institutional Bases of Democratic Self-Preservation', *Annual Review of Law and Social Science*, Vol 9, No 1, 2013, pp. 207–226.

[105] P. Culeac, Moldovan Parliamentary Elections: Post-electoral Analysis, *European Platform for Democratic Elections*, 2025.

[106] Interview with a media expert, 26 February 2026, Tbilisi.

for both national authorities and international partners. The country now serves as a reference case for EU discussions on hybrid-threat sanctions, cyber assistance and the design of proactive measures.

5.2 Georgia: Internalising the Russian authoritarian playbook

In Georgia, Russian hybrid interference has taken a more indirect but structurally transformative form. Instead of relying primarily on external electoral manipulation, Moscow has increasingly benefited from the governing Georgian Dream party's decision to adopt a Russian-style authoritarian model, including legal tools first developed in Russia and then transplanted into the Georgian context[107].

The most emblematic instrument is the 'law on transparency of foreign influence', adopted in May 2024 after Georgian Dream overcame a presidential veto. The law requires Non-Governmental Organisations and media outlets receiving more than a specified share of their funding from abroad to register as 'organisations pursuing the interests of a foreign power', echoing the language and logic of Russia's 2012 foreign agents law. Georgia's law copies key features of the Russian model: broad and vague definitions of 'political activity', intrusive reporting requirements as well as stigmatising labelling that facilitates public vilification and administrative harassment.

This law has quickly become a launchpad for repression[108]. Reports indicate that it was enforced through raids and inspections targeting Non-Governmental Organisations and media outlets sympathetic to the opposition just days before the 26 October 2024 parliamentary elections, with the explicit aim of weakening pro-Western actors and discouraging civic mobilisation[109]. OSCE/ODIHR's observation of the elections highlighted: a highly polarised media landscape; the instrumentalisation of social media; pressure on voters; as well as 'hate speech against civil society and dissenting opinions triggered by the controversial law'[110]. Complementary accounts document instances of vote-buying, double-voting, the presence of ruling-party cameras in polling stations and an overall climate of surveillance and intimidation, which all mirror practices observed in Russia's managed elections. However, unlike the Moldovan situation, in Georgia, vote-buying does not necessarily happen through the mobilisation of Russian financial resources. Georgian parties had been practising such clientelistic transactions long before the U-turn of Georgian foreign policy, even under the United National Movement's government prior to Georgian Dream's coming to power[111].

Russia's role in enabling and legitimising this trajectory is evident in official statements and information campaigns. Russia's foreign minister publicly praised Georgia for not being an 'irritant' and described Georgian Dream's foreign policy as aligned with national interests. Meanwhile, Russian intelligence and propaganda outlets accused the EU Delegation in Tbilisi of paying protesters and portrayed mass demonstrations as Western-engineered 'colour revolutions'[112]. It has been documented that there are coordinated campaigns by pro-Kremlin media to discredit pro-European protesters, downplay police

[107] I. Sirbiladze, 'Anti-democratic, anti-Western, and Russia-friendly governing elites as enablers of Russian influence in Georgia', in A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

[108] Interview with an independent expert, 25 February 2026, Tbilisi.

[109] Interview with an independent expert, 25 February 2026, Tbilisi.

[110] International Election Observation Mission, Georgia – Parliamentary Elections, 26 October 2024: Statement of Preliminary Findings and Conclusions, 27 October 2024.

[111] L. Kakhishvili, Electoral Clientelism: A Key Barrier for Fair and Competitive Elections in Georgia, Policy Brief No 57, *Georgian Institute of Politics*, April 2024.

[112] Interview with a university professor, 23 February 2026, Tbilisi.

violence and depict Western allies as destabilising forces, narratives that align with Georgian Dream's own rhetoric[113].

The 2024 elections consolidated Georgian Dream's hold on power, despite opinion polls showing that around 70 % of citizens supported EU membership as opposed to only 10 % who did not[114]. The ruling party's campaign relied on the 'Global War Party' narrative, which claimed that Western actors sought to overthrow sovereign leaders and drag Georgia into war with Russia. Striking visuals were used, such as billboards juxtaposing bombed Ukrainian cities with peaceful Georgian streets under Georgian Dream's rule. Social media monitoring revealed significant activity by bot networks on Telegram and VK, Russia's equivalent of Facebook, with some 70 % of bot comments referencing the war in Ukraine as a warning against changing government, mirroring narratives deployed by Russian authorities domestically[115].

Ethnopolitical conflicts serve as a structural backdrop for these developments. Russia's continued occupation of Abkhazia and South Ossetia, combined with incremental 'borderisation' practices – erecting physical barriers along the occupation line – sustains a persistent sense of insecurity and feeds the ruling party's claim that any assertive pro-Western course risks provoking war[116]. Georgian Dream's messaging has frequently warned that NATO or EU integration could lead to 'another Ukraine', thus using the ongoing war as both a cautionary tale and a justification for distancing from the West while pragmatically engaging with Russia[117].

From the EU's standpoint, Georgia has moved from being a model Eastern Partnership country to a 'blind spot' of democratic security. The European Commission's 2025 report directly links democratic backsliding, information manipulation and limited cooperation on hybrid threats, noting that accession negotiations have effectively become frozen due to the authorities' actions[118]. The EU has suspended or redirected some financial assistance, imposed travel restrictions on selected officials and intensified support for independent media and civil society. Nevertheless, the Union faces an extremely challenging situation given that the main enabler of Russian influence comes from within the country's own ruling elite rather than overt operations driven by Moscow.

Georgia thus illustrates a distinct pattern of hybrid interference: rather than directly hijacking elections through external means, Russia provides discursive cover and strategic encouragement for an allied government to recalibrate the political-legal system along authoritarian lines. This internalisation of the Russian 'playbook' complicates classical deterrence and sanctioning strategies, since formal legal changes are framed as domestic choices and often maintain a veneer of constitutionality.

5.3 Serbia: Hub, hybridisation and partial escape

Serbia occupies a complex middle ground between the Moldovan and Georgian trajectories. On the one hand, disinformation campaigns fuelling scepticism about European integration are promoted by the government dividing the public and aligning with Russian interests[119]. Additionally, the country functions

[113] I. Sirbiladze, 'Anti-democratic, anti-Western, and Russia-friendly governing elites as enablers of Russian influence in Georgia', in A. Pociumban and R. Nierhaus (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

[114] The Caucasus Research Resource Center, 'Caucasus Barometer 2024 Georgia', webpage, nd.

[115] OpenMinds, Russian Electoral Interference in Moldova and Georgia 2024: Mapping Telegram Disinformation Networks, December 2024.

[116] See K. Kakachia et al., Mitigating Russia's Borderization of Georgia: A Strategy to Contain and Engage, *Georgian Institute of Politics*, December 2017.

[117] Interview with a university professor, 23 February 2026, Tbilisi.

[118] European Commission, Georgia 2025 Report: Accompanying document to 2025 Communication on EU enlargement policy, SWD(2025) 757 final, 4 November 2025.

[119] J. Borràs, Disinformation and EU Enlargement: Instability and the Battle of Narratives in the Eastern Neighbourhood and the Balkans, *Barcelona Centre for International Affairs*, December 2024.

as a key regional platform for Russian hybrid operations, particularly in the energy, media and intelligence domains, while simultaneously seeks to preserve its EU accession prospects and has taken some steps to diversify away from Russia[120].

Russian hybrid influence in Serbia is underpinned by dense geoeconomic linkages. Gazprom's controlling stake in Serbia's oil company Naftna Industrija Srbije, long-term gas supply contracts and Russian participation in infrastructure projects give Moscow leverage over energy prices, investment and employment[121]. Recent US sanctions against Naftna Industrija Srbije, effective from October 2025, have not only highlighted the vulnerability of Serbia's energy sector and triggered domestic debates on diversification but also illustrated how sanctions affecting Russian assets can generate short-term social and economic costs that are politically sensitive[122].

Information operations constitute a second central channel. Russian state-owned broadcaster RT launched RT Balkans out of Serbia in 2022, whilst another Russian company Sputnik maintains a strong regional presence; both operate alongside a range of Serbian outlets that rebroadcast Russian content and narratives[123]. RT Balkans and Sputnik regularly misrepresent EU enlargement, portray the EU as hypocritical or anti-Serb, legitimising Russian policies in Ukraine and the Western Balkans, whereas domestic media structures amplify these messages, particularly around sensitive moments such as protests, elections or Kosovo-related crises[124].

The security and intelligence sphere further anchors Russian influence. Russian intelligence services such as the Federal Security Service of the Russian Federation and GRU together with Serbia's Security and Intelligence Agency cooperate on an 'open-book' basis, including joint operations, intelligence sharing and support for actors seeking territorial reconfiguration in the region[125]. This cooperation extends beyond Serbia itself to networks in Republika Srpska and northern Kosovo, where Russian backing for leaders such as Milorad Dodik and Serb paramilitary formations has repeatedly brought Bosnia and Herzegovina and Kosovo to the brink of serious escalation[126].

Serbia's ethnopolitical disputes, especially over Kosovo, are central to these hybrid dynamics. Moscow consistently supports Belgrade's position on non-recognition, uses its UN veto power to block or complicate Kosovo's international integration and frames the Kosovo issue as proof of Western double standards[127]. Russian and Serbian media ecosystems coordinate narratives that depict Kosovo as an illegitimate NATO protectorate and present Serb communities in the north as victims of Western conspiracy, which in turn legitimise hard-line stances in Belgrade and the use of coercive tactics on the ground.

However, unlike the case of Moldova, there is limited public evidence of large-scale Russian-directed electoral interference inside Serbia in the recent cycles, even though concerns about irregularities, media bias and misuse of administrative resources are well-documented. The key difference is that major elements of the Russian 'playbook' – control of media, politicisation of institutions and selective use of legal tools – have been integrated into Serbia's own political system under domestic auspices. This reduces the need for overt Russian intervention: as with Georgia, Moscow can rely on a partner government that shares or at least accommodates many of its preferences.

---

[120] M. Todorović, Long Policy Report on Russia's Ambitions and Leverage, *InvigoratEU Project*, 2025.
[121] E. Vasilj, 'Russia's hybrid warfare and geoeconomics in Southeast Europe', *Defence24.com,* 12 November 2025.
[122] Interview with a university professor of West Balkan politics, 4 February 2026, online.
[123] G. Ramunno, 'The Foreign Information Manipulation and Interference (FIMI) threat and the European Union's response', *Istituto Germani Blog*, 2025.
[124] Interview with a university professor of West Balkan politics, 4 February 2026, online.
[125] E. Vasilj, 'Russia's hybrid warfare and geoeconomics in Southeast Europe', *Defence24.com,* 12 November 2025.
[126] E. Vasilj, 'Russia's hybrid warfare and geoeconomics in Southeast Europe', 12 November 2025.
[127] Interview with a university professor of West Balkan politics, 4 February 2026, online.

At the same time, Serbia has clear incentives to reduce some aspects of dependence on Russia over time. Economic analyses stress that Serbia's growth prospects and access to EU markets depend on alignment with the single market, regulatory approximation and reduced exposure to sanctions-prone Russian entities[128]. Belgrade has engaged in EU-facilitated dialogue with Pristina, joined some EU Common Foreign and Security Policy (CFSP) declarations and begun to explore alternative energy routes, even while refusing to align with EU sanctions against Russia[129]. This dual strategy creates a structural ambiguity: Serbia remains a central node of Russian geoeconomic and information influence but it is also moving, albeit slowly, towards greater integration with EU frameworks, particularly in infrastructure and trade.

In this sense, Serbia differs from Georgia in two important ways. Firstly, while Georgian Dream has openly adopted Russian-style legal instruments and confronts the EU rhetorically, Serbia's leadership presents itself as seeking a balanced position and avoids any direct legal transplantations as radical as Georgia's foreign-agent law. Secondly, Serbian society is more divided in its external orientation, with stronger pro-Russian currents than are experienced in Georgia, which complicates overt realignment but also provides domestic cover for gradual diversification.

5.4 Lessons from the three cases

The comparison of Moldova, Georgia and Serbia yields a number of lessons about how Russian hybrid interference operates in enlargement countries and how domestic agency shapes outcomes.

Firstly, Russian hybrid warfare is best understood as a modular toolkit whose components are recombined according to local conditions. The full spectrum is visible in Moldova but electoral interference via illicit financing and disinformation is paramount. For Georgia, the emphasis is on institutional and legal capture, supported by information operations and the manipulation of war fears. Energy, geoeconomics and intelligence cooperation are the central vectors in Serbia, with elections influenced more indirectly through domestic hybridisation of governance.

Secondly, unresolved ethnopolitical conflicts and territorial disputes are consistently used as objects of manipulation and sabotage, rather than being mere background variables. Transnistria and Gagauzia provide Moscow with platforms for financial opacity, paramilitary leverage and psychological pressure in Moldova. Abkhazia and South Ossetia serve a similar role in Georgia, allowing Russia not only to sustain a permanent security dilemma but also legitimise 'borderisation' and military presence as defensive measures. In Serbia's case, the unresolved status of Kosovo and the broader Serb question regionally enable Moscow's constant involvement in crisis diplomacy, thereby providing opportunities for justifying media campaigns as well as supporting hard-line actors in Bosnia and northern Kosovo. Consequently, hybrid resilience strategies must integrate tools for conflict-resolution and de-escalation, rather than treating security and democracy as separate policy tracks.

Thirdly, domestic elite choices are decisive. Moldova shows that a reformist elite allied with civil society and external partners can use legal innovation ('militant democracy'), investigative journalism and proactive regulation to raise the cost of interference and preserve democratic choice, even in a structurally vulnerable environment. Georgia demonstrates the opposite: this is where ruling elites pursue regime survival through an authoritarian turn, voluntarily adopting Moscow's tools, such as the foreign-agent law and alignment of their propaganda with Russian narratives, thus allowing Russia to reduce its own operational footprint while benefiting from domestic impetus to bring about the erosion of democratic safeguards. Serbia's intermediate position confirms that partial alignment with EU frameworks, particularly on energy diversification and regulatory approximation, can gradually reduce and eventually eradicate

[128] E. Vasilj, 'Russia's hybrid warfare and geoeconomics in Southeast Europe', *Defence24.com,* 12 November 2025.
[129] European Commission, Serbia 2025 Report: Accompanying document to 2025 Communication on EU enlargement policy, SWD(2025) 755 final, 4 November 2025.

some levers of Russian influence but that ambiguity in elite signalling and incomplete reforms leave significant space for hybrid interference.

Fourthly, elections remain critical tests of democratic resilience. Moldova's narrow but ultimately pro-EU outcomes in 2024–2025 underscore that intense hybrid interference does not guarantee success if counter-measures are in place, such as financial investigations, cyber defence, narrative 'prebunking' and diaspora mobilisation. Georgia's manipulated 2024 elections illustrate how the same tools, when wielded by an incumbent who controls the security forces and media, backed rhetorically by Moscow, can entrench authoritarian rule despite a pro-EU majority in society. Serbia's case suggests that hybrid interference can operate more structurally, through long-term media capture and energy dependence, without necessarily taking the form of spectacular electoral subversion, which complicates detection and response.

Ultimately, the trajectories of Georgia, Moldova and Serbia show that Russian hybrid interference is not deterministic. Where governments, societies and external partners act strategically in concert, as in Moldova, hybrid threats can be constrained and progressively neutralised as a strategic weapon. Where ruling elites internalise and deploy the Russian playbook, as in Georgia, external support must refocus on societal resilience and targeted conditionality. Furthermore, where hybrid influence coexists with incremental moves toward the EU, as in Serbia, enlargement policy can become a lever for gradual de-Russification of key sectors, provided that the EU is willing to align its security and enlargement agendas by attaching clear, credible consequences to backsliding.

6 The EU response to Russian hybrid interference and its effectiveness

Russian hybrid interference has forced the EU to redefine how it approaches security, enlargement and democracy in its neighbourhood. Since 2016, the Union has moved from *ad hoc* responses to a more structured framework that treats hybrid operations as a systemic challenge cutting across sectors and borders. This section analyses this evolution and its implications for enlargement policy. Based primarily on the European Commission's 2025 country reports, it first examines how the EU has responded to Russian hybrid interference on the ground in enlargement countries. It then analyses the EU response effectiveness, arguing that outcomes depend less on the formal sophistication of EU instruments than on domestic political will, credible conditionality and the Union's ability to act in a joined-up and timely manner.

6.1 EU's response on the ground in enlargement countries

The EU's response to Russian hybrid interference in enlargement states combines generic instruments – political dialogue, conditionality, sanctions, Common Security and Defence Policy (CSDP) cooperation – with tailored measures reflecting each country's threat profile, policy alignment and domestic politics. Rather than proceeding country by country, this section identifies a common pattern in how these tools are being used across the Western Balkans and Eastern neighbourhood.

Firstly, hybrid-threat resilience is embedded into accession and association frameworks. Association Agreements, together with Stabilisation and Association Agreements, provide the legal basis for political association and economic integration with the EU. Accession negotiations and screening processes introduce obligations linked to the rule of law, security and alignment with the CFSP. Hybrid threats feature increasingly in this context. In Moldova, the EU-Moldova Association Agreement, alongside the Deep and Comprehensive Free Trade Area are now accompanied by accession negotiations as well as a Security and Defence Partnership that explicitly covers cooperation on hybrid threats and FIMI. In the Western Balkans, Stabilisation and Association Agreements together with the region's new Growth Plan incorporate hybrid-relevant benchmarks into broader reform agendas under cluster 1 (Fundamentals) and cluster 4

(Green agenda and sustainable connectivity), for example, through requirements on digital transition, governance and rule-of-law reforms that directly affect vulnerabilities to hybrid interference.

Country reports show that hybrid-threat performance has become part of the Commission's assessment scale and recommendations. In Moldova and Montenegro, the Commission notes active participation in EU cyber-security initiatives and alignment with EU statements condemning Russian hybrid campaigns. In Georgia and Serbia, by contrast, it highlights limited cooperation on FIMI, constrained dialogue and the need for 'credible efforts to close the space for foreign information manipulation and interference'. This indicates that hybrid-threat resilience is being treated as a core component within 'fundamentals of the accession process', closely linked with democratic standards, media pluralism and CFSP alignment, rather than as a stand-alone technical domain.

A second element within this pattern is differentiated security and defence cooperation, centred on CSDP, the European Peace Facility (EPF) and dedicated missions. Moldova is the most advanced laboratory regarding this approach. It is the first country to sign a Security and Defence Partnership with the EU and host the EU Partnership Mission, which supports national institutions in building resilience against hybrid threats and FIMI. At the same time, the armed forces are modernised with substantial EPF assistance. Commission reporting emphasises that Moldova has implemented a 'broad range of measures' to increase resilience, including strengthening a Centre for Strategic Communications and Countering Disinformation, establishing a National Agency for Cyber Security and reducing energy dependence on Russia.

In the Western Balkans, a number of partners participate in CSDP operations and benefit from EPF support, albeit alongside varying levels of hybrid-specific cooperation. For instance, Montenegro contributes to EU crisis-management missions and hosts the Western Balkans Cyber Capacity Centre, a regional capacity-building hub that the Commission explicitly associates with countering hybrid threats. Serbia and Kosovo both take part in EU-facilitated security dialogues and missions, yet their alignment with EU positions diverges sharply. Not only does Kosovo maintain full alignment with restrictive measures against Russia and Belarus but it is also commended for sanctions enforcement. By contrast, Serbia's partial and at times retroactive alignment, combined with intensified high-level contacts with Russia, raises doubts about its strategic orientation. The same EU tools – CSDP cooperation, EPF funding, security dialogues – thus underpin deeper integration where political alignment is strong (Moldova, Kosovo, Montenegro) but are used more cautiously where hybrid interference is tied to domestic elite choices at odds with EU norms (Serbia, Georgia).

Thirdly, this pattern concerns political conditionality, financial instruments and communicative responses. CFSP alignment and restrictive measures now form a central benchmark in all accession and candidate states. The Commission urges Serbia, for example, to improve its alignment, stop actions that contradict EU positions and make credible efforts to restrict FIMI. Kosovo's consistent alignment with sanctions is explicitly praised as evidence of its commitment to EU values. Hybrid-threat performance is also increasingly tied to EU funding access. Moldova's Reform and Growth Facility, worth EUR 1.9 billion for 2025–2027, is framed as supporting economic transformation and EU integration under conditions that include reforms boosting resilience to hybrid interference. In the Western Balkans, Growth Plan disbursements and Reform Agendas hinge on progress in governance, rule of law and digital transition, all of which reduce exploitable vulnerabilities.

Communicative instruments complement conditionality. Where governments adopt positions seen as undermining EU values and amplifying hostile narratives, the EU combines critical public messaging with the withdrawal or redirection of funds. Georgia is the clearest example: democratic backsliding, anti-EU rhetoric and limited cooperation on hybrid threats have triggered a halt in political dialogue and the

withholding of over EUR 120 million in bilateral funds that would directly benefit the authorities. Nevertheless, the EU has continued and even increased support to Georgian civil society and independent media, signalling a shift from state-centric engagement towards societal resilience. By contrast, in Moldova, the EU projects a narrative of strategic partnership, highlighting the first EU-Moldova summit, additional trade liberalisation and deepened sectoral dialogues as evidence of shared threat perceptions and convergent interests.

Overall, the EU's on-the-ground response in enlargement countries is shaped by various factors: the intensity and form of Russian hybrid interference, the stance of domestic elites and the country's stage in the accession process. Where governments cooperate and align, the Union can deploy its toolbox in a mutually reinforcing way, linking security cooperation, financial support and political backing. Where authorities themselves instrumentalise hybrid tactics or propagate hostile narratives, the EU increasingly falls back on negative conditionality and indirect strategies that prioritise societal over governmental partners.

6.2 Assessing the effectiveness of the EU's response

The effectiveness of EU responses to Russian hybrid interference must be judged both at the level of its strategic architecture and in terms of concrete outcomes for enlargement countries. The emerging picture is one of significant conceptual and institutional progress but uneven operationalisation and highly differentiated country-level results.

At a strategic level, the EU has successfully elevated hybrid threats from a peripheral concern to a core element of its security policy framework. The Joint Framework, EUGS and Strategic Compass collectively provide a coherent narrative that recognises hybrid operations as systemic, cross-sectoral challenges. They have generated an increasingly sophisticated toolbox spanning intelligence fusion, cyber defence, strategic communication, sanctions and crisis management. A number of recent major developments testify to a genuine strategic shift: establishment of the Hybrid Fusion Cell; plans for a comprehensive Hybrid Toolbox together with dedicated FIMI and Cyber Diplomacy toolboxes; as well as the incorporation of hybrid-threat language into CFSP practice and enlargement reports.

Yet this architecture also reveals structural limitations. Many of the key instruments remain non-binding, rely heavily on voluntary national contributions and suffer from uneven implementation. Enforcement is particularly weak in sensitive areas such as opaque financial flows, political-party financing and the regulation of cross-border media and platform ecosystems. The EU's capacity to attribute and sanction hybrid operations remains constrained by divergent political appetites among Member States and the need for unanimity on sanctions. Hence, despite strong rhetoric, the costs imposed on perpetrators of hybrid interference are still limited and often slow to materialise.

Moreover, effective toolbox use depends on political will at national and partner-country levels. Where governments are unwilling to recognise the problem or are themselves implicated in hybrid practices, EU instruments have limited traction. The delayed operationalisation of elements such as Hybrid Rapid Response Teams and the full FIMI toolbox exacerbates this dependence on *ad hoc*, case-by-case responses, rather than providing a clearly institutionalised channel through which threatened partners can rapidly access support.

Country-level outcomes in enlargement states reflect these constraints. Moldova stands out as a case where EU engagement has demonstrably contributed to resilience. Facing sustained Russian hybrid pressure, the country has constitutionalised EU integration, managed elections under heavy interference and embarked on systematic efforts to strengthen strategic communication, cyber security and energy

independence. These steps have been enabled by a dense web of EU instruments: association and accession frameworks; a Security and Defence Partnership; an on-the-ground CSDP mission; EPF support; as well as substantial macro-financial and reform-linked assistance. The Moldovan authorities' clear strategic orientation and willingness to adopt 'militant democracy'-style measures against hostile oligarchic networks have allowed the EU toolbox to amplify domestic efforts rather than substitute for them.

Georgia illustrates the opposite scenario. Here, domestic elites have progressively distanced themselves from EU norms, enacted legislation mirroring Russian 'foreign agent' laws and propagated anti-EU narratives. In response, the EU has activated negative conditionality – halting dialogue, freezing funds, suspending elements of cooperation – but its capacity to influence domestic trajectories has been modest. Cooperation on hybrid threats and FIMI with state authorities has largely broken down and continues mainly with civil society. The Georgian case highlights a core structural constraint: EU instruments are not designed to coerce unwilling governments in the absence of a genuine accession perspective; their strength lies in leverage over reform-minded partners, not in regime-change strategies.

Serbia occupies an intermediate position. It actively uses some EU instruments – participation in CSDP, engagement with the Growth Plan and Reform Agenda – yet not only maintains strong economic, energy and informational ties with Russia but also refuses to align with sanctions. The Commission repeatedly calls for improved CFSP alignment and credible efforts to counter FIMI but implementation has been limited. In such conditions, hybrid-threat measures risk appearing technocratic and externally driven, without being fully integrated into domestic governance priorities. EU leverage is further constrained by a perception that the accession process is slow and politicised, which hybrid narratives can easily exploit.

In Montenegro and Kosovo, EU support appears more effective, though on a smaller scale. Montenegro's hosting of the Western Balkans Cyber Capacity Centre and alignment with EU statements on hybrid campaigns signal a degree of regional leadership, even if vulnerabilities in the media and political systems persist. Kosovo's consistent alignment with sanctions against Russia and Belarus strengthens the Union's broader strategy of isolating Moscow and reduces the scope for Russian leverage in its domestic politics, even though internal political instability and the unresolved dispute with Serbia remain significant risk factors.

Taken together, these cases suggest that the EU response is most effective when three conditions are met. Firstly, there must be a clear political alignment and shared threat assessment with domestic elites. Secondly, EU tools have to be used in a genuinely joined-up fashion, linking security and defence measures with rule-of-law, economic and societal instruments rather than deploying them in isolation. Thirdly, civil society and independent media need to be treated as strategic partners, particularly where state institutions are weak or captured.

Whenever any of these conditions is absent, the EU's influence over hybrid-threat dynamics declines. In environments of democratic backsliding and elite complicity, the Union can withhold funds, adjust its narratives and support non-state actors but it cannot easily reverse domestic trends. In contexts of ambiguity, such as Serbia, the absence of a firm and credible enlargement trajectory complicates efforts to use conditionality to drive de-Russification of key sectors. This points to a broader conclusion: the technical sophistication of the EU's counter-hybrid toolbox is necessary but not sufficient. Its effectiveness ultimately hinges on the credibility of the enlargement process itself, the coherence of EU conditionality and the Union's readiness to deploy its instruments swiftly and consistently when partners come under hybrid attack.

7 Conclusions and recommendations

Russian hybrid interference exploits democratic fragilities in enlargement countries and directly affects the credibility of the EU's enlargement policy. To respond, the European Parliament could not only condemn such interference but also use its legislative, budgetary and scrutiny powers to integrate democratic resilience into the enlargement framework. Hence, the recommendations below focus on concrete steps the Parliament can take to: (a) mobilise the EU political will to target hybrid interference, (b) strengthen oversight and transparency, (c) direct EU resources towards front-line vulnerabilities and (d) ensure that resistance to hybrid interference becomes an explicit condition and support area within enlargement policy.

- **Mobilise the EU political will to respond to hybrid interference through diplomatic, political and economic tools**
  - Seek high-level synergy across EU institutions – notably the European Council, Commission and EEAS – and between the Union, Member States and enlargement countries, including through regular joint debates and statements on hybrid interference.
  - Utilise Parliament's resolutions and own reports to frame hybrid interference against enlargement countries as a strategic threat to the EU as a whole and to call explicitly for coordinated diplomatic, security and economic responses.
  - Encourage the European Council, via European Parliament resolutions, to treat serious hybrid interference in candidate or potential candidate countries as a trigger for joint EU responses, for example, coordinated diplomatic démarches, restrictive measures and targeted support packages.
  - Request systematic briefings from the Commission and EEAS on major hybrid-interference cases affecting candidate states, followed by plenary or committee debates that generate political pressure for follow-up at the Council level.
  - Promote regular joint sessions or hearings bringing together representatives of Member States and enlargement countries to discuss hybrid threats and signal shared political ownership of counter-measures.
  - Use parliamentary diplomacy – including European Parliament delegations and inter-parliamentary conferences – to build coalitions with like-minded national parliaments that can push their governments to adopt a more proactive stance on countering hybrid interference.
- **Treat enlargement countries as part of the EU's defensive perimeter**
  - Call for candidate and potential candidate countries to be systematically included in EU-level FIMI, cyber and hybrid-threat exercises as well as information-sharing formats, on a voluntary and secure basis.
  - Ask the Commission and EEAS to invite front-line partners to participate in Hybrid Rapid Response Team deployments and scenario planning.
  - Make this integration a standing point in Parliament's opinions on CFSP and on revisions of the Strategic Compass implementation.
- **Make anti-interference resilience an explicit enlargement benchmark**
  - In annual enlargement resolutions, instruct the Commission to include a dedicated 'hybrid interference and resilience' sub-chapter under Cluster 1 (Fundamentals) for each candidate and potential candidate.

  - Specify that progress towards accession should be assessed against concrete indicators: election integrity (including online campaigning rules), media ownership transparency, enforcement of anti-corruption laws and minimum cybersecurity standards for critical public institutions.
  - Call on the Commission to reflect these benchmarks in Screening Reports, Negotiating Frameworks and annual Reform Agendas linked to the Reform and Growth Facility.
  - Ensure that Member States also adhere to the same standards through coordination with national parliaments to avoid the possibility of discrediting these requirements as potential double standards.
- **Make democratic resilience a visible budget priority in enlargement**
  - During the annual budgetary procedure, insist on clearly labelled budget lines for democratic resilience, strategic communication, cyber-security and rule-of-law in enlargement countries.
  - Request performance indicators (for instance, number of supported outlets, trained officials, incidents mitigated) and make under-performance a trigger for budgetary scrutiny and re-programming.
- **Enforce political advertising transparency as part of the enlargement policy**
  - Ensure that the political advertising regulation and Digital Services Act are implemented externally via association and accession instruments, by making compliance with EU-equivalent transparency rules an explicit requirement for platforms and parties in enlargement countries.
  - Ask the Commission to support partner authorities in setting up public, machine-readable repositories of online political adverts, including information on sponsors, targeting criteria and spending.
  - Integrate an assessment of political adverts' transparency into Parliament's annual enlargement resolutions.
- **Prioritise cyber resilience of electoral and democratic infrastructure**
  - In the context of Instrument for Pre-accession Assistance III as well as the Reform and Growth Facility, insist that each enlargement country has a multi-year programme to secure election commissions, voter registers, public broadcasters and core governmental networks.
  - Request that EU funding cover penetration testing, incident-response planning, secure communications and mandatory cybersecurity training for relevant staff.
  - Link the release of some rule-of-law or public-administration tranches to demonstrate improvements in cyber-incident reporting and follow-up.
- **Promote criminalisation of key Russian interference enabling activities in the national legislation of enlargement countries as well as Member States**
  - In resolutions and own reports, call on national parliaments in the EU and enlargement countries to adopt legislation criminalising activities related to financing political actors, media ownership and financial activities that knowingly facilitate Russian influence operations.
  - Urge the Commission and EEAS to document systematically all such enabling activities in annual reports, with reference to legal action taken.

  - Commission a study on the impact and best practices of the application of measures of militant democracy and explore to what extent such measures can be effective and in line with the EU's human rights policy.

- **Improve EU visibility and narrative coherence in enlargement countries**
  - Prioritise clear and credible communication to counter misleading narratives and manage expectations regarding the enlargement process to foster public trust not only in the candidate countries but also within the EU.
  - Require the Commission and EEAS to develop country-specific communication strategies for each enlargement state, addressing Russian narratives around enlargement 'fatigue', sovereignty and socio-economic grievances.
  - Use Parliament's delegations and its operational antenna offices in Albania, Moldova and Ukraine, to organise regular town-hall events, youth forums and local-language campaigns that showcase concrete EU-funded projects and benefits.
  - Ask for annual 'public diplomacy and visibility' chapters in enlargement communications, detailing efforts and impact indicators.
  - Promote investment in education and public awareness initiatives, particularly those that focus on debunking or 'prebunking' strategies, anticipating hostile narratives and addressing them before they gain traction.

Bibliography

Antidze, M. and Stubbs, J., 'Georgia, Backed by U.S. and Britain, Blames Russia for Paralysing Cyber Attack', *Reuters*, 20 February 2020.

Asllani, M., 'Domestic Actors Fuel Russian Disinformation in the Western Balkans', *Bloomsbury Intelligence and Security Institute*, 22 August 2025.

Belford, A., Cvetkovska, S., Sekulovska, B. and Dojčinović, S., 'Leaked Documents Show Russian, Serbian Attempts to Meddle in Macedonia', *Organized Crime and Corruption Reporting Project*, 4 June 2017.

Bonomi, M., Plottka, J. and Todorović, M., Foreign Interference of China, Russia and Turkey in the EU Enlargement Countries until 2035: Three Scenarios and Policy Implications, *InvigoratEU Project*, 2026.

Bômont, C. and Zorić, B., Shared threats, shared resilience: Integrating enlargement partners in EU digital and cyber security, *European Union Institute for Security Studies*, May 2026.

Burmester, I., 'Soft Hegemony in the Shared Neighbourhood: How the European Union and Russia Co-opted Moldovan and Armenian Societies between 2000 and 2021', *Europe-Asia Studies*, Vol 77, No 3, 2025, pp. 389–414.

Borràs, J., Disinformation and EU Enlargement: Instability and the Battle of Narratives in the Eastern Neighbourhood and the Balkans, *Barcelona Centre for International Affairs*, December 2024.

Caliskan, M. and Cramers, P. A., 'What Do You Mean by Hybrid Warfare? A Content Analysis on the Media Coverage of Hybrid Warfare Concept', *Horizon Insights*, Vol 1, No 4, 2018, pp. 23–36.

Caliskan, M., 'Hybrid warfare through the lens of strategic theory', *Defense & Security Analysis*, Vol 35, No 1, 2019, pp. 40–58.

Capoccia, G., 'Militant Democracy: The Institutional Bases of Democratic Self-Preservation', *Annual Review of Law and Social Science*, Vol 9, No 1, 2013, pp. 207–226.

Center for Information Resilience, 'How the Kremlin launders disinformation around the globe', 15 May 2024.

Culeac, P., Moldovan Parliamentary Elections: Post-electoral Analysis, *European Platform for Democratic Elections*, 2025.

Defence Forces of Ukraine, 'In 2025, SSU Cyber Specialists Repelled More Than 3,000 Enemy Cyberattacks on Ukrainian Systems', *Armyinform*, 27 January 2026.

Deyermond, R., *Security and Sovereignty in the Former Soviet Union*, Lynne Rienner Publishers, London, 2008.

European Commission, Joint Communication on European Democracy Shield: Empowering Strong and Resilient Democracies, JOIN(2025) 791 final, 12 November 2025.

European Commission, Georgia 2025 Report: Accompanying document to 2025 Communication on EU enlargement policy, SWD(2025) 757 final, 4 November 2025.

European Commission, Serbia 2025 Report: Accompanying document to 2025 Communication on EU enlargement policy, SWD(2025) 755 final, 4 November 2025.

European Commission, Joint Communication on Joint Framework on countering hybrid threats: a European Union response, JOIN(2016) 18 final, 6 April 2016.

European External Action Service, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards, March 2026.

European External Action Service, A Strategic Compass for Security and Defence, 2022.

European External Action Service, A Global Strategy for the European Union's Foreign and Security Policy, 15 December 2016.

European Union Agency for Asylum, '4.1.1. Situation on the eastern borders', *Asylum Report 2022*, May 2022.

Free Russia Foundation, How Georgia Turned towards the Kremlin and Cracked down on Pro-Western Dissent, February 2026.

Galeotti, M., The Secret Battlefield: How the EU Can Help Georgia, Moldova and Ukraine Protect Against Russian Subversion, *European Council on Foreign Relations*, December 2021.

Grey, S., Bergin, T., Musaieva, S. and Anin, R., 'Special Report: Putin's allies channeled billions to Ukraine oligarch', *Reuters*, 26 November 2014.

Hoffman, F. G., 'On Not-So-New Warfare: Political Warfare vs Hybrid Threats', *War on the Rocks*, 28 July 2014.

Hoffman, F. G., '"Hybrid Threats": Neither Omnipotent nor Unbeatable', *Orbis*, Vol 54, No 3, 2010, pp. 441–455.

Hoffman, F. G., 'Hybrid vs. Compound War, The Janus Choice: Defining Today's Multifaceted Conflicts', *Armed Forces Journal,* 2009.

Hoffman, F. G., 'Hybrid Warfare and Challenges', *Joint Force Quarterly*, No 52, 2009, pp. 34–39.

Hoffman, F. G., *Conflict in the 21st Century: The Rise of Hybrid Wars,* Potomac Institute for Policy Studies, Arlington, 2007.

Institute for Strategic Dialogue, Monitoring Influence & Disinformation Campaigns in the Western Balkans (MEDIWEB), 2024.

International Election Observation Mission, Georgia – Parliamentary Elections, 26 October 2024: Statement of Preliminary Findings and Conclusions, 27 October 2024.

International Election Observation Mission, Republic of Moldova – Presidential Election and Constitutional Referendum, 20 October 2024: Statement of Preliminary Findings and Conclusions, 21 0ctober 2024.

Internews, Why information matters: A foundation for resilience, May 2015.

Johnson, R., 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies*, Vol 29, No 1, 2019, pp. 141–163.

Kakachia, K. and Lebanidze, B., 'Can small states reshape their regional identities? Examining Georgia's cognitive dissonance between South Caucasus and Eastern Europe', *Nationalities Papers*, 2025, pp. 1–15.

Kakachia, K., Kakhishvili, L., Larsen, J. and Grigalashvili, M., Mitigating Russia's Borderization of Georgia: A Strategy to Contain and Engage, *Georgian Institute of Politics*, December 2017.

Kakhishvili, L., Electoral Clientelism: A Key Barrier for Fair and Competitive Elections in Georgia, Policy Brief No 57, *Georgian Institute of Politics*, April 2024.

Kastueva-Jean, T., 'Russia's Domestic Evolution: What Impact on Its Foreign Policy?', *Russie.Nei.Visions*, No 84, 2015.

Kaziaj, E. and Keta, V., *The Distribution of Disinformation Narratives by Hostile Actors Against NATO and the EU in the Albanian Media*, Balkan Investigative Reporting Network, Tirana, 2024.

Larsen, K. P., The rise and fall of the Wagner Group: Russia is seeking control over its 'private' military companies, *Danish Institute for International Studies*, January 2025.

Markelov, M., 'I investigated millions of tweets from the Kremlin's "troll factory" and discovered classic propaganda techniques reimagined for the social media age', *The Conversation*, 1 October 2024.

McKnight, D. H. and Cherrany, N. L., 'Trust and Distrust Definitions: One Bite at a Time', in R. Falcone, R., Singh, M. and Tan, Y.-H. (eds), *Trust in Cyber-societies,* Springer-Verlag, Berlin Heidelberg, 2001, pp. 27-54.

Mihaylov, N., 'Cyber Dimensions of a Hybrid Warfare', *CyberPeace Institute*, 8 April 2025.

Ministry of Foreign Affairs and Diaspora of the Republic of Kosova, Preliminary report: Initial Analysis of Serbia's Paramilitary Aggression on Kosova, 20 October 2023.

Morson, A., 'DDoS Attacks on Moldova's September 2025 Elections: Real-Time Cybersecurity Analysis', *Mazebolt*, 29 September 2025.

National Democratic Institute, The Vulnerability of Albanian Politics to Foreign Interference, June 2024.

Olari, V. and Brooking, E. T., 'Cross-platform campaign sows anti-Europe division in Moldova', *DFRLab*, 26 March 2025.

Olcott, M. B., Åslund, A. and Garnett, S., *Getting it Wrong: Regional Cooperation and the Commonwealth of Independent States*, Carnegie Foundation for International Peace, Washington DC, 1999.

OpenMinds, Russian Electoral Interference in Moldova and Georgia 2024: Mapping Telegram Disinformation Networks, December 2024.

Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights, Republic of Moldova – Parliamentary Elections, 28 September 2025: Final Report, 18 February 2026.

Organization for Security and Co-operation in Europe, The General Framework Agreement for Peace in Bosnia and Herzegovina, 14 December 1995.

Pearson, J., 'Russia downed satellite internet in Ukraine -Western officials', *Reuters*, 10 May 2022.

Pitaval, L., 'The shadow of the bear: The role of Russian interference and hybrid warfare in the 2024 elections in Georgia and Moldova and their impact on EU accession prospects'. *Relações Internacionais*, 2025, pp. 40–52.

Pociumban, A. and Nierhaus, R. (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

Poliakoff, S., 'Trolls Behind the Mask of Journalists: How Yevgeny Prigozhin's Patriot Media Group Was Organized', *Problems of Post-Communism*, Vol 72, No 5, 2025, pp. 416–428.

Ramunno, G., 'The Foreign Information Manipulation and Interference (FIMI) threat and the European Union's response', *Istituto Germani Blog*, 2025.

Reuters, 'Ukraine Blames Russia for Most of Over 2,000 Cyberattacks in 2022', 17 January 2023.

Reuters, 'Albania Arrests Two Russians, One Ukrainian Trying to Enter Military Plant', 20 August 2022.

Roberts, T. and Oosterom, M., 'Digital authoritarianism: a systematic literature review', *Information Technology for Development*, Vol 31, No 4, 2025, pp. 860–884.

Sandu, S., 'Moldova's 2025 Elections: A Test Case for Russia's Hybrid Warfare', *Stimson Center*, 2025.

Sauer, P. and Burke, J., '"He lived by the troll, he dies by the troll": Putin takes on Prigozhin's business empire', *The Guardian*, 5 July 2023.

Schimmelfennig, F., 'Geopolitical Enlargement', in Pollak, J. and Jopp, M. (eds), *The European Union's Geopolitics: The Lackluster World Power*, Springer, Cham, 2024, pp. 79-98.

Sirbiladze, I., 'Anti-democratic, anti-Western, and Russia-friendly governing elites as enablers of Russian influence in Georgia', in Pociumban, A. and Nierhaus, R. (eds), Countering Hybrid Threats: Lessons from Eastern Europe, *German Council on Foreign Relations*, February 2026.

Sito-sucic, D., 'Bosnian Serb Leader Dodik: From Western Darling to Pro-Russian Separatist', *Reuters*, 27 March 2025.

Stanicek, B. and Caprile, A., Russia's Influence in the Western Balkans: Geopolitical confrontation, economic influence and political interference, PE 747.096, *European Parliamentary Research Service*, April 2023.

State Service of Special Communications and Information Protection of Ukraine, 'Cyber Threats Ukraine: Analytics for the H2 2025', 2026.

Todorović, M., Long Policy Report on Russia's Ambitions and Leverage, *InvigoratEU Project*, 2025.

Tsetskhladze, S., Spreading Disinformation in Georgia: state approach and countermeasures, *Transparency International Georgia*, 2023.

Tyushka, A., Engagement, Enlargement and Estrangement: EU Democracy Promotion and Protection in its Eastern Neighbourhood in-between Three Relational Paradigms, *REUNIR – Occasional Paper*, 2025.

Vasilj, E., 'Russia's hybrid warfare and geoeconomics in Southeast Europe', *Defence24.com*, 12 November 2025.

Vulović, M., 'Western Balkan Foreign and Security Ties with External Actors', *SWP Comment* 2023/C 08, 9 February 2023.

Zamfir, R., Risks and Vulnerabilities in the Western Balkans, *North Atlantic Treaty Organization Strategic Communications Centre of Excellence*, April 2020.

Zweers, W., Drost, N. and Henry, B., Little substance, considerable impact: Russian Sources of Influence in Serbia, Bosnia and Herzegovina, and Montenegro, *Clingendael*, August 2023.

PE 783.619
EP-EXPO/2023/OP/0001/AFET/LOT2/1/C/2

Print ISBN 978-92-848-4179-0 | doi: 10.2861/0036332 | QA-01-26-230-EN-C
PDF ISBN 978-92-848-4178-3 | doi: 10.2861/7064307 | QA-01-26-230-EN-N