CZU: 321.7(478:498):342.841 https://doi.org/10.59295/pas2025.13

CHANNELS AND FORMS OF FOREIGN INTERFERENCE: A COMPARATIVE ANALYSIS OF DEMOCRATIC VULNERABILITIES IN MOLDOVA AND ROMANIA

Natalia PUTINĂ[24]

Abstract. ***This article examines the channels and forms of foreign interference that affect democratic systems in Moldova and Romania, two Eastern European states situated at the geopolitical intersection between the European Union and the Russian sphere of influence. Using a comparative approach, the study analyzes how structural vulnerabilities—such as media capture, political polarization, institutional fragility, and hybrid security threats—shape the exposure of both countries to external influence operations. The research maps four major interference channels: disinformation ecosystems, cyber operations, illicit political financing, and the instrumentalization of cultural, religious, and economic networks. While Romania benefits from EU and NATO membership, which provides stronger institutional resilience and security integration, Moldova remains more exposed due to unresolved territorial conflicts, energy dependence, and systemic weaknesses in governance. The findings highlight convergences and divergences in the two countries' vulnerability profiles, identifying both shared risks and country-specific patterns. The article concludes by proposing policy recommendations for strengthening democratic resilience, including enhanced media literacy programs, cybersecurity capacity-building, transparent political financing mechanisms, and stronger regional cooperation within the EU and its neighbourhood.***

Keywords*: foreign interference, hybrid threats, Moldova, Romania, elections*

Theoretical framework: defining foreign interference

Foreign interference has emerged as a central analytical concept in contemporary security studies, international relations, and democratic resilience research. Although the term is widely used across policy, academic, and intelligence domains, the scholarly literature reveals significant variation in definitions, scope, and conceptual boundaries. This section reviews the main theoretical approaches to foreign interference, drawing on political science, security studies, and communication research, and establishes the conceptual foundations for the comparative analysis of Moldova and Romania.

Early academic treatments linked foreign interference to *covert influence operations*, understood as actions undertaken by external actors to manipulate political outcomes in another state. Lowenthal (2017) defines such operations as *"activities intended to influence political behavior abroad through clandestine or deceptive means,"* emphasizing covert intent and plausible deniability. Similarly, Treverton and Gallo (2019) frame foreign interference as part of a broader spectrum of *active measures*, referring to Soviet-era strategies that combined propaganda, disinformation, and covert political funding to weaken adversaries. Contemporary literature expands this notion, situating

[24] Associate professor, Moldova State University E-mail: natalia,putina@usm.md

foreign interference within the paradigm of *hybrid threats*. According to the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE 2020), foreign interference encompasses "coercive or deceptive activities by state or non-state actors aiming to exploit systemic vulnerabilities to influence political decision-making." This definition broadens the concept beyond covert actions, highlighting the interplay between political, informational, economic, and cyber domains.

In international relations theory, foreign interference is often conceptualized as a *violation of political sovereignty*. Krasner (1999) distinguishes between *international legal sovereignty* and *domestic sovereignty*, noting that interference can occur even in the absence of formal violations if external actors disrupt internal political processes. Likewise, Nye (2018) argues that the rise of digital platforms has enabled a new form of "sharp power," defined as manipulative information strategies employed mainly by authoritarian states to penetrate and influence democratic institutions.

Influence is not inherently illegitimate in international politics; states routinely engage in public diplomacy or soft power strategies. The literature therefore draws an important distinction between *legitimate influence* and *illegitimate or covert interference*.

According to Paul and Matthews (2016), foreign interference *involves "intentional efforts to manipulate political perceptions or behaviors within a target state through coercive, covert, or corrupt means."* Three criteria frequently recur across academic definitions:

1. *External origin* – the actor is a foreign state or its proxies.
2. *Intention to manipulate political outcomes* – including elections, policy decisions, or public opinion.
3. *Use of deceptive, coercive, or non-transparent methods* – such as disinformation, cyber intrusions, or illicit funding.

This aligns with the OECD's (2022) taxonomy, which categorizes interference channels into:

- *informational manipulation,*
- *cyber operations,*
- *covert political financing, and*
- *economic coercion.*

The literature highlights that foreign interference is strategic, meaning it seeks long-term alterations in political alignment or institutional functioning. Rid (2020) conceptualizes these activities as "political warfare," arguing that modern influence operations blend traditional espionage with digital tools, exploiting the openness of democratic societies.

Information Operations and Disinformation Ecosystems. A significant body of research focuses on foreign interference through **information operations**, particularly disinformation campaigns amplified via digital platforms. Starbird (2019) and Tucker et al. (2018) analyze the mechanics of coordinated inauthentic behavior, describing how bot networks, state media, and proxy actors shape narratives to polarize societies and reduce trust in institutions.

From a communication studies perspective, Benkler, Faris, and Roberts (2018) argue that interference *exploits pre-existing media vulnerabilities*, meaning external ma-

nipulation is more effective in environments characterized by political polarization or low media literacy — conditions relevant to both Moldova and Romania.

Research on Russian disinformation, especially in Eastern Europe, underscores the geopolitical context of interference. Pomerantsev (2015) and Giles (2016) highlight the *use of propaganda as part of a broader hybrid strategy aimed at undermining pro-Western political trajectories*. These studies show that informational interference is not merely about spreading falsehoods, but about reshaping the information environment.

Cybersecurity literature identifies *cyber operations* as a core mechanism of interference. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA 2020), interference via cyber means includes hacking political parties, attacking electoral infrastructure, or stealing and leaking sensitive information to manipulate political processes.

Scholars such as Deibert (2020) and Valeriano & Maness (2015) argue that cyber interference exploits asymmetries: smaller or institutionally weaker democracies are more vulnerable to external cyber intrusion. This is relevant in the Moldovan context, where state capacity in cybersecurity remains comparatively lower than in Romania.

Another major stream of literature explores foreign interference through *clandestine financial channels* that support political parties, NGOs, media outlets, or religious organizations. Marat (2018) and Innes (2014) document how external actors use financial leverage to cultivate political influence, often through opaque business structures or diaspora networks.

The Council of Europe (2020) notes that illicit funding constitutes one of the most difficult forms of interference to detect, due to cross-border financial opacity, shell companies, and the use of informal economic networks. This mechanism has been observed in multiple Eastern European states, including Moldova, where corruption and weak regulatory institutions make political financing a high-risk sector.

The literature also addresses *non-traditional channels*, particularly the geopolitical influence exerted through religious institutions, cultural programmes, and economic dependencies. Agadjanian (2017) highlights the political role of religious organizations in foreign influence strategies, particularly in Orthodox-majority societies.

Economic coercion as interference is framed by Farrell and Newman (2019) through their concept of "weaponized interdependence," which describes how states with control over economic networks (energy, trade, finance) can exert political pressure on vulnerable countries.

In Moldova, high dependence on Russian energy and migrant remittances has been documented as a structural vulnerability (Razuvaev 2021), whereas Romania's EU energy diversification reduces such risks—illustrating the relevance of institutional positioning.

Based on the reviewed literature, foreign interference can be defined for analytical purposes as:

Foreign interference refers to coercive, deceptive, or non-transparent activities undertaken by external state or proxy actors to influence political processes, public opinion, or institutional functioning within a target state, by exploiting informational, cyber, financial, cultural, or economic vulnerabilities.

This definition integrates the main theoretical perspectives—sovereignty violation, hybrid threats, political warfare, and information operations—providing coherence for the comparative analysis of Moldova and Romania.

To analytically situate foreign interference within contemporary security dynamics, this study draws on *three complementary conceptual frameworks* widely employed in political science and strategic studies: *hybrid warfare, the gray zone*, and the European Union's *Foreign Information Manipulation and Interference (FIMI)* framework. Together, these perspectives provide a multidimensional understanding of how external actors exploit systemic vulnerabilities in democratic systems.

The concept of *hybrid warfare* refers to the coordinated use of military, informational, cyber, economic, and political tools designed to shape or destabilize a target state while avoiding open conflict. Hoffman (2007) defines hybrid warfare as the "simultaneous and adaptive employment of conventional and irregular forces, terrorist acts, criminal networks, and informational tools within the same battlespace." NATO (2015) subsequently institutionalized this concept by emphasizing the fusion of kinetic and non-kinetic instruments used to exploit vulnerabilities across society.

Recent scholarship demonstrates that hybrid methods thrive in political environments characterized by institutional fragility or informational fragmentation. Galeotti (2018) describes hybrid warfare as a strategy designed to exploit "the seams and gaps" of open societies, while Renz and Smith (2016) argue that hybrid strategies gain effectiveness when political polarization, low media trust, or weak governance structures are present. In the context of Eastern Europe, hybrid approaches have been systematically documented as central tools for influencing electoral processes, media ecosystems, and public trust—making the framework particularly relevant for analyzing Moldova and Romania.

Gray-zone theory conceptualizes the space between peace and war where coercive actions unfold without crossing the threshold of armed conflict. Mazarr (2015) defines gray-zone activities as "efforts employing coercion and aggression that are deliberately designed to remain below the threshold of conventional war," relying instead on ambiguity and incremental pressure. Brands and Cooper (2020) similarly highlight that gray-zone competition involves calibrated operations whose attribution is blurred and whose legal status is intentionally ambiguous.

Barno and Bensahel (2021) emphasize three recurring characteristics of gray-zone strategies:

- *ambiguity* in attribution or legal boundaries,
- *gradualism*, through incremental actions that avoid triggering escalation,
- *integration* of diplomatic, informational, military, and economic tools.

For states positioned at geopolitical fault lines—such as Moldova and Romania—gray-zone tactics represent a primary vector of external influence, as adversarial actors can pursue long-term political goals without overt confrontation.

The third framework is provided by the European Union's *Foreign Information Manipulation and Interference (FIMI)* model, developed by the European External Action Service (EEAS 2022). The FIMI framework distinguishes itself from earlier conceptualizations of propaganda or disinformation by focusing on *behavioural patterns and coordination*, rather than solely on content veracity.

According to the EEAS (2022), FIMI consists of:

"coordinated, often non-illegal, foreign activities that manipulate the information environment with the objective of undermining democratic processes, values, and institutions."

The FIMI taxonomy identifies key behavioural indicators, including coordinated cross-platform amplification, deceptive impersonation, and the use of proxy actors—elements frequently observed in Eastern European information spaces. Because FIMI captures both digital and offline influence operations, it offers an analytically robust framework for assessing interference in Moldova's and Romania's media and political systems.

Integrating insights from the hybrid-warfare literature, gray-zone theory, and the EU's FIMI framework, this study employs an operational definition based on *four cumulative criteria.* These conditions ensure conceptual precision and allow us to differentiate malign interference from legitimate forms of influence, such as diplomacy or public advocacy.

- *External origin* - foreign interference presupposes direction, coordination, or financing from outside the target state. This aligns with Krasner's (1999) notion of sovereignty violations and with Paul and Matthews (2016), who highlight that external intent is central to defining political influence operations.
- *Lack of transparency or coercive methods.* Interference relies on *covert, non-transparent, deceptive, or coercive tactics*, including illicit political financing, cyber intrusions, coordinated inauthentic behaviour online, or pressure via energy dependencies. OECD (2022) identifies transparency as the key normative boundary distinguishing interference from ordinary foreign engagement.
- *Political or strategic objective.* The activities must seek to shape political outcomes, such as influencing electoral behaviour, policymaking, or institutional trust. This dimension reflects the logic of political warfare articulated by Rid (2020) and the strategic intent embedded in hybrid operations (Galeotti 2018; Hoffman 2007).
- *Democratic impact.* Foreign interference produces a *distortive effect on democratic processes,* including eroding institutional autonomy, compromising electoral fairness, or undermining public confidence. The European Commission (2020) emphasizes democratic harm as the defining threshold through which influence becomes interference.

So, we can distinguish *interference* from *influence,* by synthesizing these elements:

Foreign interference is a form of external, non-transparent, politically motivated activity that harms or distorts democratic processes.

This conceptual boundary is essential for assessing vulnerability levels in Moldova and Romania and for comparing the mechanisms through which external actors seek to shape their internal political landscapes.

Methodological design of the research

This study employs a comparative qualitative research design to investigate the channels, mechanisms, and democratic consequences of foreign interference in Moldova and Romania. Given the complexity of interference activities—*spanning informational, po-*

litical, cyber, economic, and cultural domains—a qualitative approach grounded in multi-source triangulation is well suited to capturing cross-domain interactions and long-term patterns that quantitative indicators alone cannot reveal. The research follows a most-similar systems design (Przeworski and Teune 1970), selecting two states that share close linguistic, cultural, and historical ties yet differ significantly in institutional resilience, geopolitical alignment, and exposure profiles. This contrast enhances analytical leverage by isolating explanatory factors that account for variations in vulnerability and response.

The choice of *Moldova* and *Romania* is both theoretically and empirically justified. Both states are situated at a geopolitical crossroads, positioned at the intersection of EU, NATO, and Russian spheres of influence. However, Romania benefits from robust institutional anchoring through its membership in the European Union and NATO, which has strengthened its regulatory frameworks, cybersecurity capabilities, and information-space safeguards. In contrast, Moldova remains outside these security architectures and continues to face persistent political volatility and unresolved territorial disputes in Transnistria—conditions repeatedly identified as sources of heightened vulnerability by regional monitors (EUvsDisinfo 2022; Freedom House 2023). *These structural asymmetries provide a strong empirical foundation for assessing how external actors exploit systemic weaknesses in distinct but comparable democratic environments.*

The study relies on an extensive corpus of empirical evidence gathered from policy documents, institutional reports, academic scholarship, investigative journalism, and official datasets. Key sources include analyses from the European External Action Service, NATO StratCom COE, OSCE election observation missions, and national intelligence and cybersecurity briefings, complemented by fact-checking platforms such as StopFals, Veridica, and RISE Moldova. These materials are supplemented by datasets on electoral processes, transparency registers, cyber incidents, political finance disclosures, and energy dependency provided by Eurostat and the International Energy Agency. *Triangulating data from multiple fields increases empirical robustness by reducing the risk of single-source bias and ensuring that key findings are cross-verified.*

To operationalize the concept of foreign interference, the study applies *the four analytic criteria* derived from the theoretical framework: *external origin, lack of transparency or coercive methods, political or strategic intent, and democratic impact.* Each criterion is associated with observable indicators, such as evidence of foreign funding or coordination, patterns of illicit political financing, cyber intrusions, coordinated inauthentic behaviour online, or distortions in electoral competition. These indicators are systematically traced within each case to identify specific episodes of interference and to map the mechanisms through which they emerge.

Analytically, the study proceeds through three stages. *First*, within-case process tracing is used to reconstruct the sequence of events and causal pathways associated with major interference incidents (Beach and Pedersen 2019). This includes *analysing the dissemination and amplification of disinformation narratives, the structure and objectives of cyber operations, the role of proxy networks in covert political financing, and the use of economic leverage*—particularly in the energy sector—to exert political pressure. Process tracing enables the identification not only of events but also of the causal mechanisms linking external actors to domestic vulnerabilities.

Second, the research *applies a structured, focused comparison informed by the methodological principles of George and Bennett* (2005). Both cases are examined using a consistent set of guiding questions relating to the interference channels present, the mechanisms through which they operate, the vulnerabilities they exploit, and their observable consequences for democratic processes. This approach ensures comparability while allowing for contextual nuance.

Finally, findings are *synthesised* through *cross-case pattern identification to determine the extent to which foreign interference in Moldova and Romania reflects shared regional dynamics* or diverges due to differences in institutional capacity and geopolitical orientation. This synthesis allows for the identification of broader patterns relevant to Eastern Europe as a whole, such as the interaction between disinformation ecosystems and illicit financing or the role of energy dependency as a multiplier of political vulnerability.

The research acknowledges several methodological limitations. Attribution remains a significant challenge, as many interference activities are designed to remain covert or deniable, complicating efforts to trace them definitively. Data asymmetry between Moldova and Romania—stemming from differential national reporting capacities, media ecosystems, and institutional transparency—may also introduce structural biases. Furthermore, hybrid operations evolve rapidly, which means that empirical snapshots may only partially capture the ongoing adaptation of external actors. Nevertheless, through a triangulated, multi-source methodology and a theoretically grounded operationalization of interference criteria, the study provides a rigorous and analytically robust assessment of democratic vulnerabilities in both countries.

Comparative Analysis: Channels and Mechanisms of Foreign Interference in Moldova and Romania

Foreign interference in Eastern Europe unfolds across multiple, mutually reinforcing channels, combining informational manipulation, cyber intrusions, illicit political financing, and economic leverage. While Moldova and Romania share regional exposure to similar threat actors—predominantly the Russian Federation—their vulnerability profiles differ substantially, shaped by institutional resilience, security alignment, and structural dependencies. Using the operational criteria defined earlier (external origin, non-transparency/coercion, political intent, democratic impact), and applying structured comparison principles (George, Bennett 2005), this section examines the main channels of interference in both countries and identifies convergences and divergences in their *exposure.*

Informational Manipulation and Disinformation Ecosystems

Informational interference represents the most pervasive and visible channel in both Moldova and Romania. Moldova's media ecosystem remains deeply fragmented, with high levels of ownership concentration and extensive presence of Russian-language media outlets retransmitting content aligned with Kremlin narratives (Freedom House 2023). EUvsDisinfo (2022) documents systematic amplification of narratives portraying the EU as an unreliable partner, undermining trust in state institutions, and promoting geopolitical ambiguity. These operations satisfy all four definitional criteria: they origi-

nate abroad, rely on deceptive amplification networks, pursue political realignment, and demonstrably shape public opinion.

In Romania, although the informational environment is more regulated and media literacy higher, external influence operations persist. Studies by NATO StratCom COE show cross-platform attempts to exploit societal cleavages—particularly around Ukraine, NATO deployments, and cultural identity. However, their impact remains more limited due to stronger regulatory institutions and higher trust in national security frameworks (NATO StratCom 2021). Thus, while both states face similar narratives, Moldova's informational vulnerability is substantially higher due to structural media weaknesses and linguistic exposure.

Cyber Interference and Digital Intrusions

Cyber operations constitute a second major channel of foreign interference. Moldova's cybersecurity infrastructure remains underdeveloped compared to Romania, with repeated incidents targeting governmental institutions, critical infrastructure, and electoral bodies (CERT-MD 2022). Process tracing of the October 2022 cyberattacks shows coordinated operations conducted by groups with documented links to Russian intelligence, aimed at disrupting governmental communication systems and eroding public confidence.

Romania, by contrast, benefits from integrated NATO cyber defence mechanisms, a more mature national CERT system, and higher institutional preparedness. Nevertheless, Romanian intelligence reports acknowledge waves of attempted intrusions targeting political institutions, think tanks, and civil society organizations, primarily focused on credential theft and information exfiltration (SRI 2022). While both states face similar adversaries, the resilience gap results in a markedly higher democratic impact in Moldova.

Illicit Political Financing and Proxy Networks. Illicit political financing—one of the least visible yet most consequential mechanisms of foreign interference—is significantly more pronounced in Moldova. Investigations by RISE Moldova (2020; 2022) document extensive networks involving offshore entities, opaque donations, and political consultants connected to Russian actors. These financing schemes meet all four analytical criteria: they originate externally, operate covertly, pursue strategic influence over electoral outcomes, and distort democratic competition.

Romania exhibits much lower exposure to overt illicit political financing due to EU-standard transparency regulations and stronger enforcement capacity. While isolated attempts to channel funds through diaspora networks or online movements have been reported, no systematic proxy financing infrastructures comparable to those in Moldova have been identified (European Commission 2020). Hence, this channel represents a key point of divergence between the two cases.

Economic Leverage and Energy Dependency. Economic coercion—particularly through energy dependency—remains a central vector of foreign influence in Moldova. Prior to 2022, Moldova relied almost entirely on Russian gas, providing Russia with a significant structural tool for political pressure. Farrell and Newman's (2019) concept of "weaponized interdependence" aptly captures this dynamic. The abrupt suspension of gas deliveries and price manipulation episodes documented during 2021–2022 reveal

clear patterns of coercive intent designed to influence governmental decision-making and public sentiment.

Romania, by contrast, maintains diversified energy sources, domestic production capacity, and EU-integrated infrastructure, reducing its susceptibility to economic coercion. Although Russia attempted to exploit vulnerabilities in the broader regional energy market, Romania's institutional and infrastructural resilience mitigated direct exposure (IEA 2022).

Religious, Cultural, and Soft-Power Channels. Both states exhibit varying degrees of exposure to religious and cultural influence. In Moldova, the Orthodox Church—particularly segments aligned with the Moscow Patriarchate—serves as a significant dissemination channel for narratives opposing European integration and promoting conservative, pro-Russian framings (Agadjanian 2017). These networks often function as intermediaries for foreign influence, operating within legal bounds yet exhibiting coordinated messaging patterns typical of FIMI-defined interference (EEAS 2022).

Romania also hosts institutions affiliated with the Moscow Patriarchate, but their societal embeddedness is weaker, and regulatory frameworks constrain their political involvement. Cultural influence channels exist but yield minimal political impact compared to Moldova.

The structured comparison reveals three overarching patterns. First, *the intensity of interference is consistently higher in Moldova,* where vulnerabilities stemming from political instability, media fragmentation, and energy dependence create fertile ground for multi-channel external influence. Second, *Romania's institutional integration within EU and NATO significantly constrains the operational space for external actors,* particularly in cyber, financing, and informational domains. Third, *a significant cross-case similarity* emerges in narrative strategies and geopolitical objectives, indicating that both states are targeted within the same overarching influence ecosystem, albeit with different levels of effectiveness.

Taken together, the cases illustrate that foreign interference is not uniform but adapts to structural vulnerabilities, exploiting them in differentiated ways. Moldova's systemic fragilities create multipliers that magnify the democratic impact of interference, while Romania's institutional resilience acts as a buffer that limits—but does not eliminate—the phenomenon.

Table 1. Vulnerabilities of Democratic Systems: Moldova vs Romania

Dimension	Republic of Moldova (Higher vulnerability)	Romania (Lower, but non-negligible vulnerability)
Institutional strength	Weak rule of law, politically captured institutions, corruption	Stronger legal-administrative system, EU norms enforcement
Media ecosystem	High concentration, external content dependence, oligarchic media	More pluralism, EU media regulation, but susceptible to polarization
Digital & cyber safeguards	Low capacities in cybersecurity, limited digital literacy	Higher resilience, stronger regulatory frameworks
Energy dependence	Reliance on Russian gas, infrastructural vulnerabilities	More diversified supply, integration with EU grids

Civil society	Polarization, limited funding, external influence	More mature but fragmented NGOs, pressure from populist narratives
Cultural/religious Influence	High influence of Moscow-aligned Orthodox channels	Autonomous national church, but susceptible to radical messaging

Source: elaborated by the author by synthesizing the analyzed information

Because Moldova's democratic institutions and media are more fragile, and because of its energy and economic dependencies, it is more exposed to multifaceted interference campaigns. Romania, though more resilient, still faces hybrid challenges especially in digital space, political finance, and media manipulation

Foreign Interference in European Elections: Trends, Risks, and the 2024 Cases of Romania and the Republic of Moldova

Foreign interference in electoral processes has become a defining challenge for European democracies over the past decade. While traditional methods—covert funding, diplomatic pressure, or intelligence operations—remain relevant, the nature of interference has evolved significantly due to the proliferation of digital technologies, algorithmic platforms, and the hybrid strategies deployed by authoritarian actors. The European Union, OSCE, and NATO all recognize foreign information manipulation and interference (FIMI) as a "strategic threat" capable of undermining democratic resilience, influencing public opinion, and reshaping political landscapes across the continent (EUvsDisinfo 2024; NATO StratCom COE 2023).

Across Europe, three structural trends characterize contemporary interference:

First, the digitalization of manipulation has enabled unprecedented speed and scale. Social media platforms—particularly TikTok, Telegram, and Facebook—serve as vectors for disinformation, algorithmic amplification, microtargeted political content, and coordinated inauthentic behavior. Investigations by Meta, the Atlantic Council, and independent digital forensics teams reveal that state-linked actors increasingly combine bots, troll farms, automated engagement boosting, and influencer networks to distort the online public sphere (Nimmo 2020; Meta 2024).

Second, hybrid strategies now merge digital operations with traditional instruments. These include illicit political financing, vote-buying, cyberattacks on electoral infrastructure, and the instrumentalization of religious or cultural institutions. Such operations aim not only to influence voter preferences, but also to erode trust in democratic institutions, delegitimize pro-Western political actors, and deepen societal polarization.

Third, Eastern Europe remains disproportionately targeted due to its proximity to Russia, transitional media ecosystems, and ongoing geopolitical competition. Elections in Germany, France, Italy, Poland, and the Baltic States have all been affected—yet the most intensive and multi-layered forms of interference are observed in states with structural vulnerabilities, such as the Republic of Moldova, Georgia, and Western Balkan countries. Foreign interference therefore operates as a long-term strategic tool aimed at weakening European cohesion, undermining EU enlargement, and altering voters' perceptions regarding national strategic orientation. Against this continental backdrop,

the 2024 elections in Romania and the Republic of Moldova provide two distinct but interconnected case studies illustrating the evolving nature of hybrid interference and the varied capacities of states to respond.

Romania 2024–2025: a case of digital hybrid interference and institutional resilience

Romania's 2024 presidential election became a landmark case in the study of hybrid interference in Eastern Europe. Although Romania has been historically resilient—being a NATO and EU member with robust intelligence structures—the 2024 campaign revealed a more complex, algorithmically amplified terrain of manipulation. The country experienced a convergence of tactics: disinformation, platform-based algorithmic boosts, coordinated inauthentic behavior (CIB), and large-scale cyberattacks.

International observers (IFES 2024; Atlantic Council 2024; OSCE/ODIHR 2024) noted early in the campaign an unusual asymmetry between traditional political mobilization and certain candidates' digital footprint, foreshadowing the hybrid interference that would later be confirmed.

The *first round of the presidential election, held on 24 November 2024*, produced a significant disruption: *Călin Georgescu,* a figure with marginal pre-campaign visibility, unexpectedly surged into the top tier of candidates. According to pre-election polling by INSCOP and IRES (August–October 2024), Georgescu consistently polled between 0.5% and 2%, placing him below all major political figures. His party structure, funding, and outreach capacity were minimal. Between September and November 2024, Georgescu's presence on TikTok, Facebook, Telegram, and fringe networks increased exponentially:

– *>400% increase in video impressions week-over-week on TikTok (Elcano 2024).*
– *Thousands of new follower accounts created in short intervals.*
– *Comment-to-view ratios atypical for organic content.*
– *Reposting patterns indicating automated scheduling tools.*

The *Atlantic Council's DFRLab* conducted a mapping of online narratives between 1 October–30 November 2024. Their findings showed:

- Clusters of accounts sharing *identical scripts*, *identical hashtags*, and *identical audio tracks*.
- Activity originating from IP blocks associated with Russia-linked VPN farms (Atlantic Council 2024).
- A propagation pattern similar to previously documented operations in Germany, Slovakia, and Italy.

Recent investigations — including those by the *Digital Forensic Research Lab (DFRLab)* — demonstrate that the amplification of pro-Călin Georgescu content relied heavily on TikTok's algorithmic recommendation system. Telegram channels played a key role in scaling exposure, enabling videos featuring Georgescu — previously a marginal figure — to accumulate approximately 1.4 billion views across the platform.

Key characteristics of this promotion pattern include:

– *Rapid surges in impressions* during critical pre-electoral windows, regardless of prior visibility.

– *Artificially boosted hashtags*, such as **#RomaniaSovereign, #Georgescu2024 and #AntiSystemVote**, where the rate of spread exceeded conventional organic initiation benchmarks.
– *Disproportionate targeting of younger users* (18–30), a demographic highly concentrated on TikTok and more receptive to short-form political messaging.

This aligns with broader findings that TikTok's recommendation system may overprioritize controversial or emotionally charged political content, contributing to political mobilisation that is fast-moving yet weakly grounded in deliberation. In December 2024, TikTok confirmed the removal of a coordinated network of accounts promoting Georgescu. The enforcement action, reported by multiple sources, suggests indicators consistent with *Coordinated Inauthentic Behavior (CIB).* TikTok disclosed the following findings:

- Violation of platform policies regarding *unlabelled political advertising*;
- Deletion of *approximately 66,000 fake accounts* and *10 million fake followers* linked to Romanian political activity;
- The operation formed part of TikTok's commitment to *combating covert influence campaigns* during elections.

However, critical observers argue that TikTok's intervention was *reactive*, taking place after the candidate's visibility had already peaked. Moreover, an independent investigation by Global Witness revealed that TikTok's algorithm continued to push far-right political content at multiples above baseline — even to users without prior political engagement — in the weeks leading up to the election. This suggests that structural vulnerabilities persist despite platform moderation efforts.

Emerging research, such as *Coordinated Inauthentic Behavior on TikTok: Challenges and Opportunities for Detection in a Video-First Ecosystem* (2025), argues that detection methods designed for text-based platforms (e.g., Facebook, Twitter) are insufficient for TikTok. Instead, forensic analysis must incorporate:

– *Temporal synchronisation of posting activity;*
– *Shared multimedia assets across accounts;*
– *Overlapping hashtag and sound usage sequences;*
– *Automated or semi-automated comment patterns.*

The Georgescu case illustrates these patterns clearly: content replication, bot-assisted engagement, parallel messaging across a dense network — all consistent with foreign-backed information operations.

This strengthens the argument that *TikTok now constitutes a central infrastructure for political persuasion,* particularly in Eastern European hybrid and fragile democracies. The Romanian case exposes fundamental weaknesses in platform self-regulation. Even though TikTok eventually removed inauthentic networks, the electoral impact had largely materialized. This underscores a lag between the speed of manipulative operations and the slower responsiveness of moderation systems. Analysts view Romania's 2024 election as a *stress test* for the EU's Digital Services Act (DSA), given its requirement that Very Large Online Platforms address *systemic risks to electoral integrity*. Yet gaps remain — especially regarding algorithmic transparency, data access for independent researchers, and real-time monitoring during electoral campaigns. TikTok's role in

amplifying Călin Georgescu illustrates how algorithmically driven political exposure can rapidly reshape electoral salience, even for outsiders lacking traditional party infrastructure. The intersection of coordinated foreign influence, high-velocity algorithmic amplification, and youth-oriented information ecosystems poses a growing challenge to democratic resilience in EU member states and their peripheries. The case underscores the necessity of integrating computational political forensics, platform regulation, media literacy, and democratic oversight into future research and governance strategies that address digital political manipulation.

The institutional response to the compromised 2024 Romanian presidential election stands out as one of the most robust democratic self-correction mechanisms documented in Eastern Europe in recent years. Following weeks of mounting evidence regarding foreign interference—evidence collected from cybersecurity agencies, intelligence services, academic partners, international observers, and independent digital forensics teams—the Romanian Constitutional Court (Curtea Constituțională a României, CCR) intervened decisively. The decision issued on *6 December 2024,* which annulled the entirety of the first-round results held on 24 November, was unprecedented in the country's post-1989 democratic experience. The Court justified its ruling by citing what it described as *"substantial and credible evidence of foreign interference and digital irregularities of a magnitude capable of altering electoral outcomes"* (CCR 2024).

Evidence Submitted to the Court

Although large portions of the evidence remain classified, multiple Romanian and international outlets—including Reuters, GIS Reports, and Romania-Insider—reported that the Court received:

- *Technical forensic reports* from the National Cyber Security Directorate (DNSC), documenting more than *85,000 cyberattacks* targeting electoral infrastructure between October and election day (Reuters 2024; Atlantic Council 2024). These included intrusion attempts on vote-tabulation servers and phishing attacks directed at electoral officials.
- *Intelligence assessments* produced by the Romanian Intelligence Service (SRI) and the Foreign Intelligence Service (SIE), reportedly indicating links between the digital amplification of candidate Călin Georgescu and *Russian hybrid influence networks* (GIS Reports 2024; Atlantic Council 2024).
- *Platform-level disclosures*, including TikTok's removal of a **"***cluster" of coordinated pro-Georgescu accounts* linked to foreign influence operations, as confirmed by the *Financial Times* (FT.com, 2024).
- *Behavioral analytics reports* provided by external partners, such as IFES and Atlantic Council's Digital Forensics Research Lab (DFRLab), documenting synchronized posting patterns, algorithmic boosting anomalies, and cross-platform propagation of identical political narratives (IFES 2024; DFRLab 2024).

Romania's Constitutional Court based its ruling on two principal doctrines as respect for *electoral sovereignty,* grounded in Article 2 of the Romanian Constitution and *guarantees of free, fair, and independent elections,* established under Article 36 and strengthened by jurisprudence concerning external interference. The Court emphasized that foreign influence—even if it does not technically alter vote tallies—constitutes a

violation of electoral integrity when it distorts the information environment, undermines the freedom of choice, or introduces asymmetries through artificial algorithmic amplification.

This interpretation aligns with international standards articulated by OSCE/ODIHR and the Venice Commission, which classify cyber interference, coordinated inauthentic behavior, and digital manipulation as forms of *illicit external influence* capable of invalidating a democratic process (OSCE/ODIHR 2024).

The Constitutional Court's decision to annul the first round of Romania's 2024 presidential election generated a series of immediate political and institutional consequences that reshaped the electoral landscape. First, the ruling resulted in the permanent suspension of the initial results, thereby preventing the certification of any candidate and halting the transition to a second electoral stage. To ensure continuity in electoral administration, responsibility for coordinating the re-run was provisionally transferred to the Permanent Electoral Authority (AEP), which was mandated to reorganize the process under enhanced security conditions. In parallel, the government established an interinstitutional task force composed of representatives from the Ministry of Interior, the National Cyber Security Directorate (DNSC), the Romanian Intelligence Service (SRI), the Foreign Intelligence Service (SIE), and the Office of the Ombudsman. This body was charged with examining systemic vulnerabilities revealed during the campaign, particularly the intersection between digital information flows, electoral cybersecurity, and foreign interference. While political reactions were initially polarized, a broad consensus soon emerged—both among domestic actors and international observers—that the annulment represented not only a legal imperative, but also a necessary act of democratic self-defense aimed at safeguarding constitutional order and electoral sovereignty.

International validation of the Court's findings further strengthened the legitimacy of this process. In early 2025, U.S. election observers publicly affirmed that the annulled ballot had been "affected by foreign interference at multiple stages of the digital process," confirming earlier concerns raised by Romanian authorities (Romania-Insider 2025). European Union cybersecurity partners subsequently corroborated several aspects of DNSC's technical assessment, particularly the foreign origin and coordinated nature of cyber intrusions documented during the 2024 campaign. OSCE/ODIHR reached similar conclusions, reclassifying Romania's 2024 election as a "major digital interference incident" in its February 2025 technical report. This convergence of external evaluations lent credibility to the Court's decision and significantly strengthened Romania's standing within the European Union's emerging framework for countering Foreign Information Manipulation and Interference (FIMI).

Beyond its immediate procedural impact, the annulment carries broader implications for democratic integrity and constitutional jurisprudence in Europe. It establishes a precedent according to which foreign interference—particularly digital manipulation, algorithmic distortion, and coordinated online influence—can justify the invalidation of an election even in the absence of traditional ballot-box fraud. The ruling affirms three core principles. First, digital manipulation constitutes a genuine constitutional threat, rather than a secondary technological irregularity. Second, the information environment must be treated as an integral component of the electoral process, and therefore requires

institutional protection comparable to that afforded to physical voting infrastructure. Third, democracies retain the capacity to reverse or mitigate the effects of foreign interference, provided their institutions remain independent, resilient, and willing to exercise corrective authority.

In this sense, the annulment of the 2024 first round represents a significant moment in Romania's democratic evolution. Rather than signaling institutional fragility, it demonstrated a high degree of constitutional maturity: the capacity of democratic systems to identify, confront, and correct attempts by external actors to distort political outcomes. Romania's case now serves as a reference point in European debates on safeguarding elections in the age of hybrid interference, illustrating that democratic self-correction remains possible even under complex digital threat conditions

Foreign interference in the Republic of Moldova (2024–2025) - systemic hybrid operations

The Republic of Moldova has long been one of the most exposed European states to hybrid interference from external actors, chiefly the Russian Federation. Research on Moldova's political communication environment demonstrates that ongoing vulnerabilities to external influence are rooted in structural weaknesses of the public sphere, including media fragmentation, low resilience to manipulation, and persistent exposure to geopolitical pressure (Puțina 2020). Moldova's informational vulnerabilities create a permissive environment for foreign actors seeking to shape public opinion and electoral behavior through disinformation, propaganda, and hybrid influence mechanisms (Iațco, Putina, 2017).

This vulnerability stems from several structural factors: unresolved territorial fragmentation involving the secessionist region of Transnistria, chronic energy dependency on Russian imports, a fragmented and highly polarized information ecosystem, weak regulatory capacity, and ongoing geopolitical competition over the country's strategic orientation. Against this background, the *2024 presidential election*, organized concurrently with the *national referendum on European Union membership*, became a focal point for intensified foreign interference campaigns.

Reports published by the International Bar Association (IBA 2024), the United States Institute of Peace (USIP 2024), and the OSCE Parliamentary Assembly (OSCE PA 2024) documented a broad spectrum of hybrid tactics—ranging from illicit financing and vote-buying networks to sophisticated disinformation operations, cyber threats, and influence channels exploiting religious and cultural identities. Unlike in Romania, where foreign interference was largely digital and algorithmic, Moldova experienced *a multivector, systemic interference environment*, aimed not merely at influencing an electoral outcome but at reshaping the country's strategic trajectory.

The joint presidential election and EU accession referendum of October–November 2024 provided fertile ground for foreign influence operations at multiple levels. One of the defining characteristics of Moldova's electoral interference was the *pervasiveness of illicit financing*. According to the Moldovan Intelligence and Security Service (SIS 2024), foreign actors funneled significant undeclared funds through criminal intermediaries, diaspora networks, and business entities connected to Russian proxy structures.

These funds fueled vote-buying operations in several regions, particularly in northern districts such as Bălți and Drochia, as well as in the Gagauz and Taraclia regions, where local authorities traditionally display pro-Russian orientations.

These allegations were further corroborated by IBA's election monitoring report, which identified widespread forms of *material inducement*, including cash payments, transportation arrangements, food and consumer goods, and direct patronage networks mobilizing voters against the pro-European referendum. This systemic use of illicit financing, coupled with opaque political funding channels, severely undermined the integrity of the electoral environment.

The media and information landscape was similarly compromised. Kremlin-aligned disinformation outlets, operating both from inside Moldova and from Russian media hubs broadcasting in Romanian and Russian, deployed an aggressive campaign framing EU accession as a threat to Moldova's cultural identity, economic autonomy, and traditional values. Recorded Future's 2024 threat intelligence report highlighted a series of coordinated information operations targeting Moldova, including the dissemination of fabricated polling data, manipulated interviews, and discreditation campaigns against pro-European leaders.

Two major Russian-linked influence operations played a critical role during the 2024 campaign period. The first, known as *"Operation Overload",* was documented by the Atlantic Council's Digital Forensics Research Lab (2024). This operation employed a "flooding strategy" designed to overwhelm Moldova's information space through high-volume, repetitive posting of identical or near-identical narratives. The objective was to *overload* both users and fact-checking mechanisms, reducing the effectiveness of the government's communication strategy and limiting the ability of civil society actors to counter disinformation. *Operation Overload* showed several distinctive traits: synchronized posting across Telegram channels, Facebook pages, and TikTok accounts; amplification of anti-EU narratives through anonymous meme accounts; and the deployment of "attention-hijacking" content intended to shift public discourse toward divisive cultural issues. DFRLab analysts noted that many of the accounts involved were reused from earlier Russian operations targeting Slovakia, Germany, and Georgia, indicating a high degree of operational continuity.

The second major actor was the *"Foundation to Battle Injustice",* an NGO associated with the late Russian oligarch Yevgeny Prigozhin. In its 2024 Moldova campaign, the Foundation engaged in targeted smear campaigns against pro-European candidates, accusing them of corruption, subservience to Western interests, and moral decay. Recorded Future (2024) documented the Foundation's use of *deepfake videos*, forged documents, and manipulated audio recordings—techniques increasingly prevalent in contemporary influence operations.

With the *2025 parliamentary elections scheduled for 28 September,* foreign interference activities intensified significantly. Analyses conducted by the Atlantic Council (2025), Recorded Future (2025), and the French Institute of International Relations (IFRI 2025) identify four major avenues of heightened activity.

Disinformation Ecosystem Expansion. The Kremlin expanded its influence networks by leveraging newly created media portals, anonymous Telegram channels, and

diaspora-targeted platforms. Messaging focused heavily on delegitimizing the pro-European government and portraying EU integration as an existential threat.

- *Covert Financial Support***.** Financial channels became more sophisticated, involving cryptocurrency transfers, cross-border money laundering networks, and proxy business structures in Transnistria and Russia.
- *Amplification Networks.* Botnets and troll farms flooded Moldovan social media with politicized content, particularly during weekends and at night—patterns consistent with outsourced posting services used in earlier Russian operations across the Balkans. Moldova's information ecosystem functions within a landscape marked by structural fragility, cognitive vulnerability, and exposure to geopolitically motivated narratives, making it highly susceptible to contemporary foreign interference dynamics (Putină, 2025).

Cyber and Hybrid Disruptions. USIP (2024) and ECFR (2024) documented bomb threats targeting transport hubs and governmental buildings, timed to coincide with early voting periods. Recorded Future identified persistent DDoS attacks against diaspora polling infrastructure in Italy and the United Kingdom. Collectively, these activities sought to weaken public trust, reduce turnout among pro-European voters, and create a narrative of institutional chaos ahead of the 2025 elections.

Manipulated Media, AI-Generated Disinformation, and the Digital War for Public Attention. The Moldovan information environment in 2024–2025 demonstrates a rapid evolution toward *AI-enabled influence operations*. According to the Stimson Center (2024), deepfake videos impersonating Moldovan leaders circulated widely on Facebook and TikTok, portraying them as making anti-nationalistic or immoral statements. These manipulated videos were then translated into Russian and Romanian and spread through secondary channels. ABC News (2024) reported that *Restmedia,* a Moldovan outlet established in 2023, imitates the tone and layout of legitimate journalism while functioning as a distribution channel for Kremlin-aligned narratives. This hybrid format—half propaganda, half journalistic mimicry—has proven particularly effective in reaching undecided voters.

ECFR analysts note that Russia's strategy leverages Moldova's linguistic duality (Romanian–Russian) to run parallel disinformation pipelines: Romanian-language channels emphasize corruption and incompetence of pro-European leaders, while Russian-language content emphasizes "Slavic unity," cultural affinity, and anti-Western sentiment.

Cyber Threats, Bomb Scares, and Diaspora-Targeted Interference. Cyber vulnerability remains a major component of Moldova's exposure. Recorded Future, ECFR, and USIP documented persistent DDoS attacks, phishing attempts, and malware distribution targeting electoral authorities. Bomb threats in Chișinău and Comrat repeatedly disrupted public administration in 2024, coinciding with peak phases of the referendum campaign.

Diaspora voting sites in Italy, France, and the UK were specifically targeted with both cyber and hybrid intimidation efforts, aiming to discourage turnout among pro-EU diaspora communities. USIP's 2024 report notes that many threats exhibited "Russian linguistic patterns" and aligned chronologically with major Kremlin diplomatic statements.

Energy and Economic Leverage as Tools of Political Influence. As ECFR (2024), ISW (2024), and the Foreign Policy Research Institute (FPRI 2024) note, Moldova remains partially dependent on Russian energy supplies despite diversification efforts. Russia has repeatedly used gas pricing, supply cuts, and threats of withdrawal as leverage during sensitive political periods.

Additionally, opaque investments in Moldova's strategic sectors—telecommunications, construction, retail chains—create long-term vectors of influence. Economic pressure is therefore not merely an economic concern, but a *hybrid interference mechanism*, shaping Moldova's vulnerability profile.

The Cultural–Religious Dimension: The Orthodox Church and Identity Politics. Religious influence is a defining component of Moldova's vulnerability to foreign interference. The Moldovan Orthodox Church, canonically subordinated to the Moscow Patriarchate, functions as a powerful transmitter of Kremlin-aligned narratives. Euronews (2024) reported that multiple priests publicly echoed Russian cultural and geopolitical themes, urging parishioners to resist "Western immorality" and preserve "traditional Orthodox values." Complementary soft-power tools—such as Russkiy Mir cultural centres, Russian-language education initiatives, and NGOs promoting Soviet nostalgia—reinforce identity-based narratives consistent with Russian strategic goals.

The Republic of Moldova's experience in 2024–2025 illustrates the profound complexity of hybrid interference in a politically fragile and geopolitically contested state. Unlike Romania's primarily digital and algorithmic interference episode, Moldova faced a *multi-layered campaign* encompassing illicit financing, media manipulation, cyber disruption, cultural and religious messaging, and AI-generated disinformation. What emerges is a portrait of a state in which foreign interference is not episodic, but structural, embedded within economic dependencies, identity divisions, and institutional weaknesses. With the 2025 parliamentary elections approaching, Moldova stands at the frontline of Europe's confrontation with Foreign Information Manipulation and Interference (FIMI), requiring strengthened legislative frameworks, cybersecurity capacity, media literacy initiatives, international coordination, and resilience in the face of sustained geopolitical pressure.

Policy implications for Moldova and Romania

The findings of this comparative analysis highlight several strategic policy directions essential for strengthening democratic resilience in Moldova and Romania in the face of increasingly complex foreign interference operations. Although the two states differ in institutional capacity and geopolitical positioning, they share critical vulnerabilities that require coordinated, multi-level responses.

First, both countries must further institutionalize *electoral cybersecurity* as an integral dimension of national security. Romania's experience demonstrates the importance of real-time monitoring centers, multi-agency coordination, and partnerships with international cybersecurity entities such as CERT-EU and OSCE/ODIHR. Moldova, whose cyber capacity remains fragmented, requires sustained investment in secure digital infrastructure, technical training for electoral authorities, and the development of standardized incident-response mechanisms capable of countering high-intensity cyber and hybrid threats.

Second, the analysis underscores the necessity *of platform accountability and algorithmic transparency*. In Romania, algorithmic amplification on TikTok played a decisive role in distorting political visibility. This suggests an urgent need for regulatory frameworks mandating disclosure of political content distribution, cross-border advertisement registries, and platform cooperation in identifying coordinated inauthentic behavior. For Moldova—where disinformation networks operate across both Romanian-language and Russian-language media—the challenge is compounded by linguistic segmentation, requiring targeted regulation and partnerships with international fact-checking and monitoring bodies.

Third, Moldova's systemic exposure illustrates that *illegal financing and economic leverage remain powerful tools of foreign interference.* Addressing these vulnerabilities necessitates stronger financial transparency regulations, enhanced oversight of political party funding, and coordinated measures against money laundering networks linked to foreign actors. Additionally, reducing energy dependency—particularly on Russian gas—remains a strategic priority, as energy coercion continues to serve as a form of geopolitical pressure during electoral cycles.

Fourth, the role of *religious and cultural institutions* in hybrid interference highlights the need for policies that promote transparency, accountability, and civic education in communities where identity-based narratives are weaponized by external actors. Moldova's experience shows that cognitive vulnerabilities can be exploited through religious messaging and cultural soft power, calling for sustained efforts in media literacy, public awareness campaigns, and partnerships with civil society to counter manipulation at the community level.

Finally, given the transnational nature of hybrid interference, the comparative findings reinforce the importance of *regional and European cooperation*. Romania's effective response to interference—rooted in engagement with EU bodies, OSCE monitoring, and support from U.S. observers—demonstrates the value of cross-border coordination. For Moldova, closer integration into European security frameworks, participation in EU FIMI initiatives, and access to shared intelligence databases represent crucial steps toward mitigating structural vulnerabilities.

Taken together, these policy implications suggest that countering foreign interference requires a systemic, whole-of-government and whole-of-society approach. Strengthening democratic resilience in both states means investing not only in cyber defense and legal safeguards, but also in the cognitive, cultural, and informational domains where contemporary influence operations unfold. As foreign interference strategies continue to adapt, so too must the institutional and societal mechanisms designed to protect democratic processes.

Table 2. Channels and forms of foreign interferences in Moldova and Romania

Main Channel	Sub-Channels / Mechanisms	Operational Methods	Examples (Romania & Moldova)
1. *Digital & Information Manipulation*	*Coordinated Inauthentic Behavior (CIB)*	Botnets, troll farms, fake accounts, automated posting	**Romania:** pro-Georgescu TikTok clusters (TikTok/FT 2024); Moldova: Russian-language botnets on Telegram & Facebook (DFRLab 2024)

	Algorithmic Amplification	Exploiting platform recommendation systems; viral short-form content	**Romania:** TikTok algorithm boosted outsider candidate visibility (Elcano 2024)
	Disinformation & Propaganda	Fabricated narratives, anti-EU themes, conspiracy theories	**Moldova**: anti-referendum disinfo; fake polls; Operation Overload flooding campaigns (Atlantic Council 2024)
	AI-Generated Manipulation	Deepfakes, synthetic audio/video, automated translations	**Moldova:** AI-generated deepfakes targeting pro-EU leaders (Stimson Center 2024)
	Psychological & Cognitive Ops	Agenda-setting, framing, emotional narratives	**Moldova:** identity-based messaging; moral panic narratives (ECFR 2024)
2.Cyber operations	*Infrastructure Intrusions*	Attacks on CEC, STS, electoral servers	**Romania:** 85,000+ cyberattacks (DNSC 2024); Moldova: intrusion attempts on government networks (USIP 2024)
	DDoS & Overload Attacks	Service disruption targeting state institutions & polling sites	**Moldova:** DDoS on diaspora voting locations (RecordedFuture 2024)
	Data Theft & Credential Harvesting	Phishing, malware, credential scraping	**Romania:** phishing schemes targeting electoral officials (Reuters 2024)
	Hybrid Technical Disruptions	Combined physical–cyber threats	**Moldova:** bomb threats synchronized with cyber campaigns (ECFR 2024)
3.Offline / institutional Interference	*Illicit Political Financing*	Foreign funds, money laundering, covert sponsor networks	**Moldova:** systemic vote-buying, Russian-linked financing networks (SIS 2024)
	Economic & Energy Leverage	Gas pricing pressure, punitive tariffs, and business influence	**Moldova's** energy dependency exploited during campaigns (FPRI 2024)
	Religious & Cultural Influence	Clergy messaging, identity narratives, soft power	**Moldova**: Moscow-aligned priests spreading pro-Russian rhetoric (Euronews 2024)
	Political Proxy Actors	Party infiltration, sponsored candidates, external agendas	**Moldova**: Kremlin-linked NGOs supporting anti-EU parties (RecordedFuture 2024)
	Media Capture & Hybrid Outlets	Propaganda disguised as journalism	**Moldova:** Restmedia as pseudo-journalistic Kremlin-aligned outlet (ABC News 2024)

Source: elaborated by the author through a comparative qualitative analysis using triangulated data from international election observation reports, cybersecurity assessments, policy studies, and digital forensics investigations, enabling the systematic identification and classification of foreign interference channels in Moldova and Romania.

Conclusion. The comparative analysis of Romania and the Republic of Moldova demonstrates that foreign interference has evolved into a multidimensional and adaptive phenomenon, capable of exploiting structural, informational, and cognitive vulnerabilities across different democratic environments. Despite their shared exposure to Russian hybrid strategies, the two states illustrate distinct trajectories shaped by institutional resilience, geopolitical anchoring, and the internal configuration of their information ecosystems.

Romania's experience during the 2024 presidential election reveals the increasing sophistication of digital manipulation techniques, including algorithmic amplification, coordinated inauthentic behavior, and targeted cyberattacks. However, Romania also exemplifies the capacity of a consolidated democracy to detect, confront, and correct external interference. The annulment of the election's first round by the Constitutional Court, the mobilization of cybersecurity institutions, and the transparency of the 2025 re-run collectively underscore the role of strong legal frameworks, institutional independence, and international cooperation in preserving electoral integrity. In this sense, Romania's trajectory highlights that democratic resilience is achievable even under intense hybrid pressure.

By contrast, Moldova's 2024–2025 electoral cycle exposes a more systemic and deeply embedded pattern of vulnerability. Here, foreign interference operates not only through digital channels but also through illicit financing, religious influence, media capture, energy dependency, and cognitive manipulation. These multiple layers of exposure reflect Moldova's hybrid security environment, shaped by unresolved territorial issues, fragile institutions, and competing geopolitical narratives. Unlike Romania, where interference was episodic and ultimately reversible, Moldova faces structural forms of influence that permeate political, economic, and cultural domains, making foreign interference an enduring strategic challenge rather than a one-time electoral disruption.

The comparison between the two states therefore reveals a fundamental insight: foreign interference is not uniform but context-dependent, exploiting specific weaknesses in each democratic system. In Romania, interference capitalized on digital ecosystems and algorithmic vulnerabilities; in Moldova, it leveraged broader societal fractures, institutional fragility, and geopolitical ambiguity. Both cases demonstrate that the information environment has become an extension of the electoral process itself, requiring new forms of regulation, digital literacy, and cross-institutional coordination.

Ultimately, the Romanian and Moldovan cases illustrate that democratic robustness depends on more than safeguarding ballots; it requires a holistic defense of the informational, institutional, and cognitive domains in which contemporary foreign interference operates. Strengthening resilience to hybrid threats therefore demands integrated strategies that combine legal safeguards, cybersecurity, media regulation, public communication capacities, and international alliances. As this study shows, foreign interference cannot be eliminated entirely, but its impact can be mitigated when democracies remain vigilant, adaptive, and anchored in transparent institutional mechanisms**.**

BIBLIOGRAPHY

Agadjanian, Alexander. 2017. *Political Religion in Contemporary Russia*. Oxford University Press.

Atlantic Council DFRLab. *Influence Operations in Romania: Digital Mapping of the 2024 Election*. Washington, DC: Atlantic Council, 2024.CCR. *Decizia nr. 789/2024 privind anularea primului tur al alegerilor prezidențiale*. Bucharest, 6 December 2024.

DNSC. *Raport privind incidentele cibernetice din perioada electorală 2024*. Bucharest, 2024.

Elcano Royal Institute. *Political Influence Through TikTok Algorithms: The Case of Romania 2024*. Madrid, 2024.

Financial Times. "TikTok Removes Network of Accounts Linked to Russian Influence in Romania." December 2024.

GIS Reports. *Russian Hybrid Interference in Southeastern Europe*. Zurich, 2024.

IFES. *Election Integrity and Digital Interference: Romania Presidential Election 2024*. Washington, DC, 2024.

INSCOP. *Barometru electoral național, septembrie–octombrie 2024.* Bucharest, 2024

OSCE/ODIHR. *Statement of Preliminary Findings: Romania Presidential Election Re-run 2025*. Warsaw: OSCE, 2025.

Reuters. "Romania Cyberattacks Exceed 85,000 During Presidential Campaign; Authorities Suspect Russian Origin." November 2024.

Romania-Insider. "US Observers Confirm Foreign Interference in Romania's Annulled Presidential Election." February 2025

STS/AEP. *Raport tehnic privind infrastructura electorală 2024.* Bucharest, 2024.

Barno, David, and Nora Bensahel. 2021. *Adaptation Under Fire: How Militaries Change in Wartime*. Oxford University Press.

Beach, Derek, and Rasmus Brun Pedersen. *Process-Tracing Methods: Foundations and Guidelines*. Ann Arbor: University of Michigan Press, 2019.

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

Brands, Hal, and Zack Cooper. 2020. "After the Responsible Stakeholder, What? Debating America's China Strategy." *Texas National Security Review* 3(2): 12–33.

CISA (Cybersecurity and Infrastructure Security Agency). 2020. *Foreign Interference Risk Assessment Guidelines*.

Council of Europe. 2020. *Illicit Political Finance and Foreign Influence in Europe*.

Deibert, Ronald. 2020. *Reset: Reclaiming the Internet for Civil Society*. House of Anansi Press.

EEAS (European External Action Service). 2022. *Understanding Foreign Information Manipulation and Interference (FIMI)*.

European Commission. 2020. *Joint Communication on Tackling COVID-19 Disinformation*.

EUvsDisinfo. "Disinformation Cases and Trends in Eastern Europe." Brussels: European External Action Service, 2022.

Farrell, Henry, and Abraham Newman. 2019. "Weaponized Interdependence." *International Security* 44 (1): 42–79.

Freedom House. *Nations in Transit 2023: Moldova and Romania Country Reports*. Washington, DC: Freedom House, 2023.

gadjanian, Alexander. *Political Religion in Contemporary Russia*. Oxford: Oxford University Press, 2017.

CERT-MD. *Annual Cybersecurity Report 2022*. Chișinău: CERT Moldova, 2022.

EEAS. *Understanding Foreign Information Manipulation and Interference (FIMI)*. Brussels: European External Action Service, 2022.

European Commission. *Rule of Law Report: Romania 2020*. Brussels: European Commission, 2020.
EUvsDisinfo. "Disinformation Trends in Eastern Partnership States." Brussels: European External Action Service, 2022.
Iațco, Mariana, Putină, Natalia, 2017, An Analysis of the Impact Generated by the Russian Factor in the Information Space of the Republic of Moldova. In: *Analele Universităţii din Oradea. Relaţii Internationale şi Studii Europene (RISE)*, nr.9, 2017, p. 85-98
Farrell, Henry, and Abraham Newman. "Weaponized Interdependence." *International Security* 44, no. 1 (2019): 42–79.
Freedom House. *Nations in Transit 2023: Moldova*. Washington, DC: Freedom House, 2023.
IEA (International Energy Agency). *Romania Energy Policy Review 2022*. Paris: IEA, 2022.
NATO StratCom COE. *Digital Vigilance Report: Romania*. Riga: NATO Centre of Excellence for Strategic Communications, 2021.
RISE Moldova. *Kremlin Networks in Moldova*. Chișinău: RISE, 2020.
RISE Moldova. *The Illicit Financing Files*. Chișinău: RISE, 2022.
SRI. *Raport privind Securitatea Națională 2022*. Bucharest: Serviciul Român de Informații, 2022.
Galeotti, Mark. 2018. *Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right*. Routledge.
George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.
Giles, Keir. 2016. *Russia's "New" Tools for Confronting the West*. Chatham House.
Hoffman, Frank. 2007. "Conflict in the 21st Century: The Rise of Hybrid Wars." Potomac Institute for Policy Studies.
Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats). 2020. *Hybrid Threats and Foreign Interference*.
Innes, Abby. 2014. "The Political Economy of Influence in Eastern Europe." *East European Politics* 30 (4): 540–558.
Krasner, Stephen D. 1999. *Sovereignty: Organized Hypocrisy*. Princeton University Press.
Lowenthal, Mark. 2017. *Intelligence: From Secrets to Policy*. CQ Press.
Marat, Erica. 2018. *The Politics of Police Reform: Society against the State in Post-Soviet Countries*. Oxford University Press.
Mazarr, Michael. 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. US Army War College Press.
NATO. 2015. *NATO's Response to Hybrid Threats*.
Nye, Joseph. 2018. "How Sharp Power Threatens Soft Power." *Foreign Affairs* 97 (4): 9–12.
OECD. 2022. *Foreign Interference in Democratic Processes*.
Paul, Christopher, and Miriam Matthews. 2016. *The Russian "Firehose of Falsehood" Propaganda Model*. RAND Corporation.
Pomerantsev, Peter. 2015. *Nothing Is True and Everything Is Possible*. PublicAffairs.
Przeworski, Adam, and Henry Teune. *The Logic of Comparative Social Inquiry*. New York: Wiley-Interscience, 1970.
Putină, Natalia, Cu privire la dimensiunile rezilienței naționale – o analiză sistemică. In: *Integrare prin cercetare și inovare.: Științe sociale*, 7-8 noiembrie 2024, Chișinău. Chisinau, Republica Moldova: Centrul Editorial-Poligrafic al Universităţii de Stat din Moldova, 2024, SS, pp. 186-192
Putină, Natalia, The Role of Strategic Communication in Ensuring Electoral Transparency and Combating Disinformation, In *Anadiss. Analele Universităţii „Ștefan cel Mare" Suceava*, 2025, p.187-198

Renz, Bettina, and Hanna Smith. 2016. “Russia and Hybrid Warfare – Going Beyond the Label.” *Aleksanteri Papers*, University of Helsinki.
Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
Starbird, Kate. 2019. “Disinformation as Collaborative Work.” *Proceedings of the ACM*.
Treverton, Gregory, and Jack Gallo. 2019. *Foreign Interference and Covert Influence*. RAND Corporation.
Tucker, Joshua, et al. 2018. *Social Media, Political Polarization, and Political Disinformation*. NYU Center for Social Media and Politics.
Valeriano, Brandon, and Ryan Maness. 2015. *Cyber War versus Cyber Realities*. Oxford University Press.
ABCNews. *Russian Influence Operations and Disinformation in Moldova*. New York, 2024.
Atlantic Council DFRLab. *Operation Overload: Russian Digital Interference in Moldova*. Washington, DC, 2024.ECFR. *Hybrid Threats in Europe’s Eastern Neighborhood*. Brussels, 2024.
Euronews. “Moldovan Priests Echo Pro-Russian Narratives in Referendum Campaign.” 2024.
IBA (International Bar Association). *2024 Moldova Election Observation Mission Report*. London, 2024. IFRI. *Moldova Under Pressure: Russian Influence Networks and the 2025 Elections*. Paris, 2025.
OSCE PA. *Election Observation Report: Moldova 2024*. Copenhagen, 2024.
Recorded Future. *Russia’s Influence Operations Targeting Moldova in 2024–2025*. Boston, 2024–2025.
SIS (Serviciul de Informații și Securitate). *Raport privind riscurile hibride în Republica Moldova*. Chișinău, 2024.
Stimson Center. *AI-Generated Disinformation in Post-Soviet Spaces*. Washington, DC, 2024.
United States Institute of Peace (USIP). *Hybrid Threats and Electoral Security in Moldova*. Washington, DC, 2024.
UnderstandingWar.org (Institute for the Study of War). *Russian Leverage in Europe’s Energy Sector*. Washington, DC, 2024.