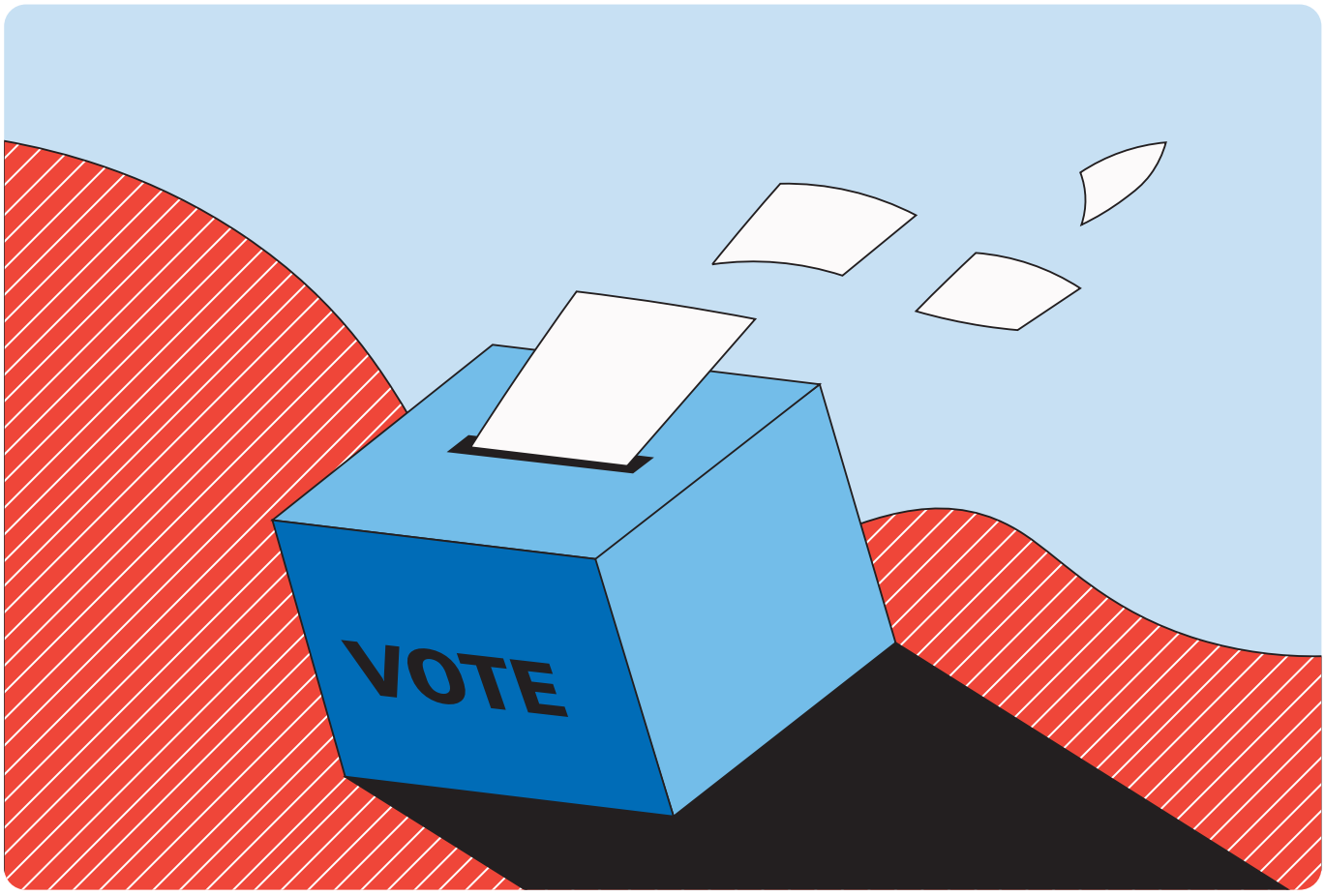
Safeguarding Elections Against Hybrid Threats: **A Defensive Playbook**

Sebastian Bay and Catalina Uribe Burcher
November 2025



Folke Bernadotte Academy
Swedish agency for peace, security and development

FBA

Acknowledgements

The authors of this report would like to thank the many individuals and teams whose contributions made it possible.

First and foremost, we wish to thank Lisa Orrenius, who has overseen the process from inception to finalization and provided continuous feedback and guidance. We are also grateful to colleagues at the Folke Bernadotte Academy (FBA) who have reviewed and commented on the structure, content and framing, including Carl Fredrik Birkoff, Filippa Almlund and Kicki Westin from the Democracy and Governance Unit, as well as Emma Skeppström and Abdalhadi Alijla from the Research Team.

We extend our gratitude to Susanna Kujanpää (formerly of the European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) for her valuable external review and insights.

A special note of appreciation goes to Aina Boris, who oversaw all production details and ensured that the manuscript, layout, illustrations and final delivery came together smoothly. We also thank Essen International and Comactiva Language Partner for their excellent work on copy-editing, layout and illustrations.

Contents

Foreword

Free elections are the cornerstone of democratic governance. They embody the social contract between citizens and the state, offering both the means to govern and the mechanism for accountability. Today that contract is increasingly under attack. Hybrid threats, blending information manipulation, cyberattacks and illicit political finance, target not only electoral processes, but also the very trust and social fabric on which democracy depends.

These threats are neither episodic nor peripheral. They represent a sustained and highly adaptive challenge to democratic governance. The intent behind the threats and attacks is not merely to sway a particular vote, but to corrode confidence in institutions, amplify division and weaken societies from within. The use of artificial intelligence and other emerging technologies has further accelerated this trend, lowering barriers to interference and magnifying its impact.

For the Folke Bernadotte Academy (FBA), defending democracy is a pillar of conflict prevention and a matter of both national and international security. It requires more than technical safeguards; it demands political vision, institutional resilience and collective will. Effective responses must strengthen the capacity of national actors at all levels to act in concert, under the shared understanding that democratic resilience depends on the engagement of all parts of society. At the same time, these efforts must uphold the openness, transparency and rights that define democratic systems. Countering hybrid threats cannot come at the expense of the very values we seek to protect.

This report reflects FBA's commitment to support efforts towards free and legitimate elections. It brings together practical insights to examine how hybrid threats manifest through information operations, illicit finance and cyberattacks, and how coordinated, governance-centred strategies can reinforce electoral integrity. Its recommendations emphasize the importance of whole-of-government and whole-of-society approaches, the institutionalization of cooperation networks, and a continuous cycle of preparedness that extends beyond election day.

At its core, the report argues that electoral resilience is inseparable from democratic resilience. Building defences against hybrid threats is not solely a security exercise; it is an investment in the rule of law, in accountable governance, and in the enduring credibility of democratic institutions.

The examples and lessons presented in this report are relevant to all countries, including our own country – Sweden. Hybrid threats do not recognize borders, nor do they distinguish between mature or emerging democracies. The same tactics that seek to undermine electoral integrity in one context can quickly migrate to another. Building resilience is therefore a shared responsibility – among states, institutions and societies alike. By learning from diverse experiences and fostering cooperation across borders, we can strengthen not only the protection of elections but also the foundations of democracy itself.

Per Olsson Fridh
Director-General, Folke Bernadotte Academy

Glossary of Terms

- **Advanced Persistent Threats (APTs):** Highly resourced, goal-driven threat actors – often state-sponsored or state-tasked – that conduct long-duration, stealthy intrusions to gain and maintain access to targeted networks in support of strategic objectives (espionage, pre-positioning, disruption or influence).

- **Coordinated Inauthentic Behaviour (CIB):** The coordinated use of deceptive or inauthentic accounts to mislead people about the origin, identity or popularity of content.

- **Deepfake:** Synthetic or manipulated media (image, audio or video) generated with artificial intelligence techniques to depict events or speech that did not occur.

- **Disinformation:** Information that is false or misleading and deliberately created and spread to harm a person, social group, organization or country.

- **"Doppelgänger" technique:** A tactic that uses look-alike ("doppelgänger") infrastructure – cloned or closely spoofed news and institutional websites, domains and social accounts – to launder false or misleading content by making it appear as though it comes from trusted outlets. The content is then seeded and amplified through coordinated inauthentic behaviour, paid promotion and cross-platform reposting.

- **Doxing (sometimes spelt "doxxing"):** The online publication or sharing of private, personally identifiable or sensitive information about a person without their consent, typically to harass, intimidate or otherwise cause harm.

- **Foreign Information Manipulation and Interference (FIMI):** A mostly non-illegal pattern of manipulative behaviour, conducted intentionally and in a coordinated manner by foreign state or non-state actors (including their proxies), that threatens or has the potential to negatively impact values, procedures and political processes.

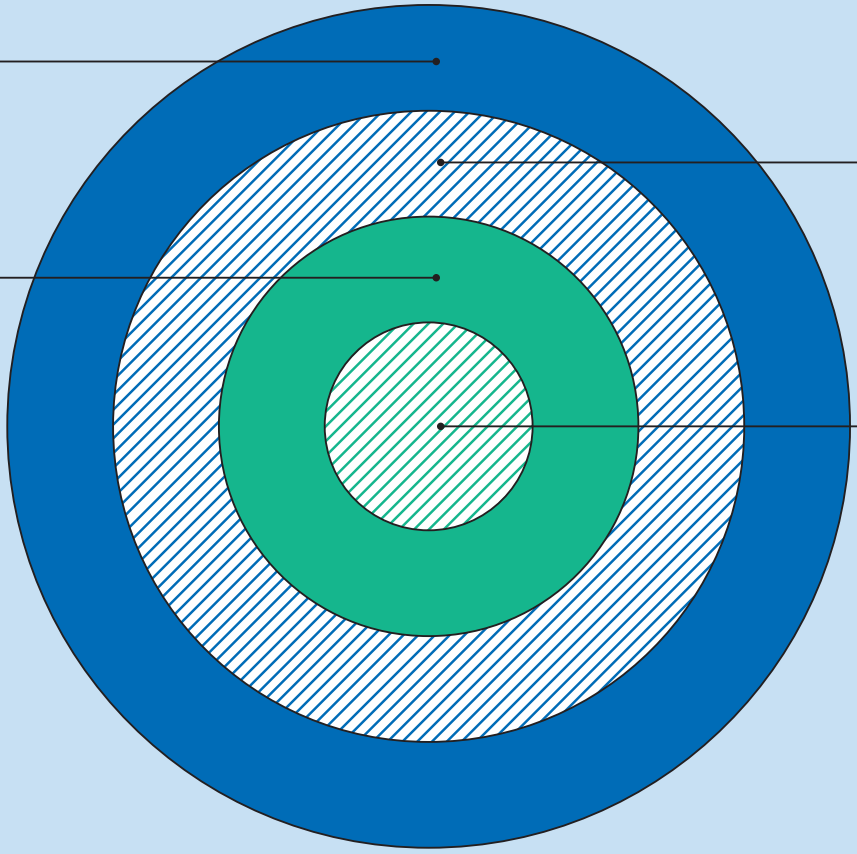
- **Hack-and-Leak Operation:** A coordinated operation that seeks to compromise systems to steal data and release selected, curated or manipulated materials at strategic moments to influence media narratives, public perception or political processes.

- **Hybrid Threats:** Coordinated, intentional and harmful activities that deliberately target systemic vulnerabilities of democratic states and institutions through a mixture of conventional and unconventional means. These activities exploit thresholds of detection and attribution, as well as the interfaces between war and peace and internal and external security. They typically aim to influence decision-making at local, state or institutional levels while remaining below the threshold of armed conflict.

HIERARCHY OF TERMINOLOGY

Hybrid threats
The broad context of coordinated, intentional and harmful activities that include information, cyber and financial means.

FIMI
A pattern of manipulative behaviours conducted by foreign actors, intentional and often coordinated.



Information influence activities (IIA)
Planned efforts to shape perceptions, attitudes or behaviour through information and communication.

Disinformation
False or misleading information deliberately spread to cause harm.

- **Information influence activities (IIA):** Planned efforts to shape perceptions, attitudes or behaviour through the use of information and communication. These activities range from legitimate public communication and diplomacy to covert or deceptive practices such as impersonation and coordinated inauthentic behaviour. IIA is an umbrella term that includes FIMI, which refers specifically to manipulative behaviours conducted by foreign state or non-state actors and their proxies.

- **Misinformation:** Information that is false, but not created or spread with the intention of causing harm.

- **Pre-bunking:** A proactive, inoculation-based communication strategy that forewarns people about likely manipulation tactics or narratives before they encounter them. It provides simple, accurate counters and decision aids to help individuals recognize and resist the manipulation when it occurs. In electoral contexts, pre-bunking is often delivered through a source-of-truth hub, frequently asked questions, and timed public messaging tied to known risk windows (e.g., registration deadlines or silence periods).

- **Spear-phishing:** A targeted social-engineering attack that uses tailored lures to trick a specific individual into revealing credentials, granting access or executing malicious code.

- **Vishing (or voice phishing):** Social engineering conducted over voice calls, often using caller-ID spoofing to trick individuals into revealing information or granting access.

Acronyms

- **AI:** Artificial Intelligence
- **APT:** Advanced Persistent Threat
- **CaaS:** Cybercrime-as-a-Service
- **DDoS:** Distributed Denial-of-Service
- **DSA:** EU Digital Services Act
- **EMB:** Election Management Body
- **FBA:** Folke Bernadotte Academy
- **FIMI:** Foreign Information Manipulation and Interference

Executive Summary

This report provides a comprehensive analysis of hybrid threats to elections and how to effectively counter them. It focuses primarily on developments since 2024 across key avenues of electoral interference, including Foreign Information Manipulation and Interference (FIMI), illicit political finance, and cyber operations. While analysed separately, in practice these are closely intertwined. The report advances a practical defence framework that pairs institutional capacity-building with a networked, whole-of-society support system.

Key trends (since 2024):

- FIMI has evolved into persistent industry-scaled operations driven by coordinated networks rather than isolated campaigns.
- Artificial Intelligence (AI) and automation have accelerated the creation and distribution of synthetic and deceptive content and lowered the cost of social engineering.
- Illicit political finance, including proxy funding, international transfers through crypto-currencies and opaque online expenditure, is increasingly supporting manipulation and vote-buying.
- Cyber operations are disrupting electoral infrastructure and often work in tandem with information operations, amplifying their overall impact.

The key implication of these trends is that adversaries take advantage of gaps between institutions responsible for organizing and supporting elections. Siloed responses lead to inadequate performance. This report consolidates best practices for countermeasures and highlights the idea that protecting elections from these complex threats necessitates:

- Clear ownership, resources, mandates, staff and rehearsed routines within each agency.
- A standing, year-round national cooperation network to share intelligence, conduct joint exercises, and coordinate protective efforts – operating on "analyse together, act within mandate" to preserve institutional autonomy.
- A whole-of-society approach that mobilizes independent media, civil society, academia, local authorities, the private sector (including platforms and telecom operators) and communities to strengthen resilience through media and digital literacy, rapid fact-checking, incident reporting, and inclusive public communication – anchored in radical transparency and implemented in ways that uphold rights, transparency and pluralism.
- Robust international cooperation and support mechanisms that provide surge assistance, enable cross-border takedowns, and align on common baselines (e.g., secure-by-design practices, provenance where feasible, and timely disclosure) – linking national networks into a wider "network of networks" to accelerate support, coherence and accountability.

The report offers practical recommendations for electoral management bodies, governments, civil society organizations, and international support actors in various electoral environments, from established to developing democracies. Key recommendations include strengthening election authorities, achieving operational excellence, establishing well-resourced national election cooperation networks, enhancing legal frameworks on platform accountability and illicit political finance, and adopting a modular approach to international assistance.

The main finding is that, in an era of ongoing hybrid conflict, electoral defence must be continuous, adaptable, proactive and collaborative. Building strong institutional capabilities and a whole-of-society approach offers the most lasting protection for electoral integrity.

01 Introduction

In elections across Europe, hybrid threats have tested the resilience of electoral systems. In Slovakia, just two days before the 2023 election, an AI-generated audio recording allegedly featuring the liberal candidate Michal Šimečka and a journalist plotting to buy votes from Roma communities was circulated during the media silence period. In Romania, in the run-up to the 2024 presidential election, authorities identified coordinated hybrid tactics ranging from vote-buying schemes, disinformation and cyberattacks, to undeclared funding for a pro-Russian candidate. And in Moldova, in September 2025, President Maia Sandu warned that Moscow was waging a vast hybrid war ahead of the parliamentary elections, using disinformation, vote-buying and other forms of illicit political finance as well as intimidation tactics targeting voters.[1]

Together, these examples illustrate how elections are facing increasing challenges and interference by foreign actors targeted by coordinated activity across information, finance and cyber domains, often timed to exploit institutional and societal seams.[2] Because these threats continuously evolve, protecting free and fair elections from hybrid threats has not only become more critical than ever but also a continuous and ever-evolving challenge.[3]

The contemporary threat landscape represents a fundamental evolution from the traditional diplomacy and propaganda of the 20th century. The digital domain is now the centre of gravity: adversaries blend cyber operations, subversive online techniques, and narrative manipulation; domestic actors may knowingly or unknowingly amplify these efforts. Russia's actions during Ukraine's 2014 elections, and particularly during the 2016 US presidential election, served as a watershed moment, catalysing global recognition of the vulnerability of democratic processes to such sophisticated hybrid threats.[4]

A crucial insight is that modern interference is not a series of standalone operations, but a chronic, state-backed information war waged by a complex ecosystem of actors.[5] Intelligence services consistently identify Russia, China and Iran as the principal orchestrators, operating through a network of proxies – from state-run media to hacktivist groups – to maintain plausible deniability.[6] The line is further blurred by domestic political groups that can act as witting or unwitting amplifiers of foreign narratives.[7]

Technological advancements, particularly in AI, have significantly accelerated this evolution. Since 2024, the use of generative AI has emerged as a significant force multiplier, enabling the rapid, low-cost creation of realistic synthetic media, including deepfakes and voice clones; the industrial-scale production of tailored disinformation; and the potential for malicious AI swarms.[8] While the direct impact of AI-generated content on election outcomes remains difficult to quantify, it has demonstrably shaped the information environment and amplified the spread of existing falsehoods.[9] This merging of geopolitical competition, advanced technology and adaptive adversaries defines the current, complex landscape of hybrid threats targeting elections.

1.1. DEFINING HYBRID THREATS IN THE ELECTORAL CONTEXT

Hybrid threats targeting elections are coordinated, hostile actions that blend conventional and unconventional means to undermine democratic processes, while remaining below the threshold of armed conflict and often exploiting detection/attribution gaps and the war–peace/internal–external interfaces.[10]

Bay (2024) identifies three categories of threats related to the electoral process: threats to the conduct of elections, trust in elections, and the will and ability to vote. Building on this process-focused structure, this report applies a four-category approach that also captures

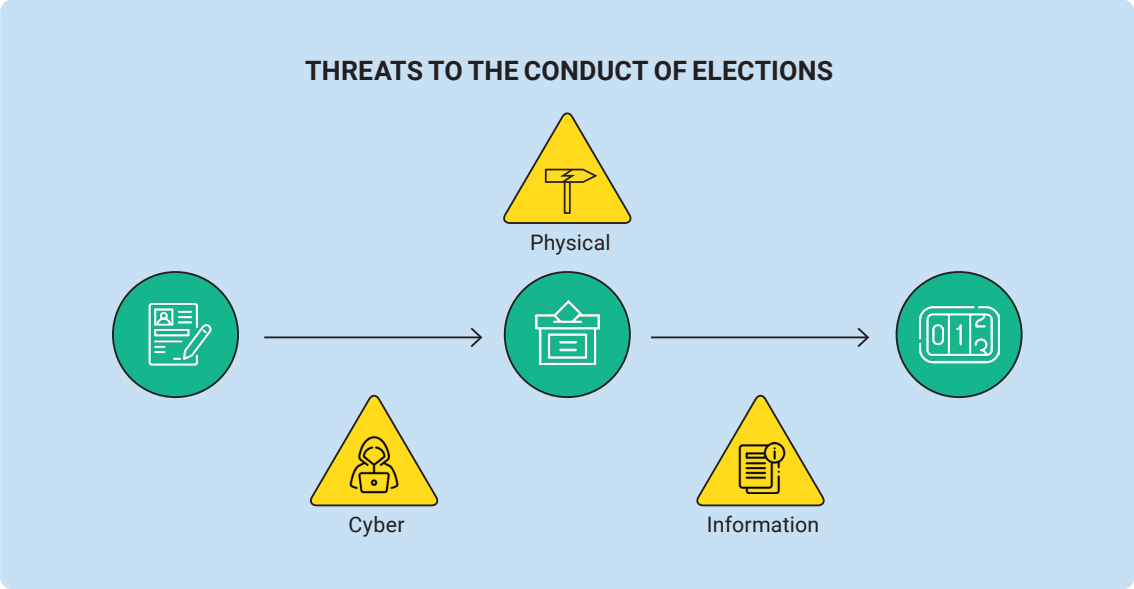
threats targeting political decision-making. For analytic clarity, election-specific threats are grouped into four overlapping categories: (a) conduct of elections, (b) trust in elections, (c) will/ability to vote, and (d) political decision-making. Together, these categories help distinguish disruptions to electoral processes from deeper attempts to shift preferences or corrode legitimacy:

- Threats to the conduct of elections: Actions seeking to disrupt the electoral process itself by targeting officials, infrastructure or logistics through information, physical or cyber means.

- Threats to trust in elections: Efforts aimed at undermining public confidence in the legitimacy of elections by spreading disinformation, promoting conspiracy theories or creating a perception of widespread fraud.

- Threats to the will and ability to vote: Tactics designed to influence voter behaviour by discouraging participation or undermining voters' ability to cast their ballot, such as through intimidation or spreading false procedural information.

- Threats to political decision-making: Attempts to influence voters' preferences using illegitimate or illegal means, including inauthentic coordinated activity on digital platforms, illicit financing or the subversion of candidates.



1.2. IMPACT ON ELECTORAL INTEGRITY, TRUST AND DEMOCRATIC PROCESSES

The strategic objective of hybrid attacks against elections is not only to influence a single vote, but to degrade democratic ecosystems by eroding trust, fuelling polarization and weakening the institutional foundations of democratic states.[11] In practice, this manifests through narrative campaigns that question rules and referees, orchestrated claims of fraud, and timed leaks that shape agendas during silence periods. By attacking the credibility of officials, undermining confidence in voting systems and disseminating inflammatory disinformation, such campaigns aim to deepen polarization and corrode the institutional resilience of the state itself.[12]

"The strategic objective of hybrid attacks against elections is not only to influence a single vote, but to degrade democratic ecosystems by eroding trust, fuelling polarization..."

While not the only cause, such threats have likely contributed to the global decline in average electoral turnout of around ten percentage points over the last 15 years, as well as to the increase in disputes, with nearly one in five national elections between 2020 and 2024 seeing the losing side reject the result.[13]

Recent electoral cycles also show tangible effects: post-election unrest and non-concession incidents; information crises triggered by hack-and-leak efforts; and administrative disruption when cyber incidents delay voter check-in or the communication of results. In several instances, international observers have documented coordinated pressure combining information influence activities, illicit financing and cyber disruption, further stressing already polarized environments.[14]

This erosion is compounded by an exodus of experienced election officials, who face persistent harassment, thereby weakening institutional capacity.[15] The cumulative effect is a feedback loop: declining trust increases vulnerability to manipulation, which in turn further diminishes participation and consent.[16]

Furthermore, narratives about "election fraud" have concrete domestic impacts – prompting a surge of complaints and requests for access to information, pressuring ad hoc recounts or "forensic audits", increasing harassment of officials and reducing willingness to accept election results. These narratives also spread across borders, where the same frames are adapted and reused by aligned influencers and state-linked outlets, shaping expectations long before voting day.[17]

Furthermore, these tactics are crafted to deepen societal divisions. Adversaries inject emotionally charged disinformation into debates on immigration, economic policy and cultural "wedge issues" to fuel targeted polarization.[18] Mechanistically, campaigns increase the prominence of social identities, frame politics as a zero-sum game ("us vs. them"), and associate emotionally charged claims with periods of uncertainty, when audiences depend more on group cues and simplified narratives; in this state, affective polarization intensifies and corrective information is disregarded.[19]

These campaigns often use negative portrayals of marginalized identities – including gender, race and sexual orientation – to magnify social fractures and disproportionately target minority groups and women.[20] Operators also amplify opposing sides simultaneously – a tactic known as "identity convergence" – and exploit intersectional grievances, such as the overlap between religion and gender or class. This increases reach and helps normalize hostility across multiple communities.[21]

This triggers a dangerous feedback loop: a polarized society with low trust is less resilient and even more susceptible to future hybrid attacks. As trust declines, perceived inter-group threat increases, social distance expands and elites face pressure for extraordinary measures – conditions that adversaries reintroduce with new narratives and greater impact.[22]

1.3. THE GEOPOLITICAL DIMENSION

Hybrid threats to elections do not occur in isolation; they are closely tied to the broader geopolitical landscape. The intensified use of these tactics since 2024 is fuelled by the strategic competition between democracies and authoritarian states, the ongoing war in Ukraine, and several other frontline conflicts.[23] Russia often views elections as opportunities to weaken support for Ukraine, undermine alliances such as the North Atlantic Treaty Organization (NATO) and the European Union (EU), and advance a revisionist agenda aimed at reshaping the global order.[24]

For these actors, information warfare is not an adjunct to policy but a central instrument of statecraft, waged persistently and asymmetrically.[25]

> Democratic societies – defined by open information environments and a commitment to freedom of expression – embody intrinsic vulnerabilities that adversaries are adept at exploiting. In contrast, authoritarian regimes benefit from closed, tightly controlled information ecosystems, granting them a significant defensive advantage that underpins their resilience. This operational asymmetry lies at the heart of contemporary conflict.[26]

The war in Ukraine has functioned both as a laboratory and a catalyst for Russia's hybrid threats. Many of the tactics, techniques and procedures deployed against Western elections (and most recently witnessed in full force in Moldova) are directly aligned with Moscow's geopolitical goals as well as its strategic aim of eroding international support for Ukraine.[27] Accordingly, defending elections is no longer just a domestic policy issue; it is integral to international security and the collective defence of the democratic model itself, as iterated by NATO and the EU on multiple occasions.[28]

1.4. PURPOSE, SCOPE AND METHODOLOGY OF THE REPORT

Preventing the challenges posed by hybrid threats requires a thorough understanding of the tactics employed by malign actors and the strategies necessary to counter them. As part of Sweden's commitment to strengthening democracy and the rule of law, the Folke Bernadotte Academy (FBA) supports this goal by researching and sharing knowledge with international actors facing such threats – thereby contributing to the development of more resilient democracies. This support extends beyond election observation and encompasses election support aimed at strengthening preparedness and electoral resilience.

This report compiles and presents expertise on countering hybrid threats to elections, with a chief focus on developments since 2024. It begins with a general overview of hybrid threats to elections, the ecosystem in which they unfold, and their overall impact on electoral integrity, public trust, and democratic processes within the current global geopolitical context. Subsequent chapters delve deeper into three key avenues through which malign actors influence elections: information manipulation and interference, illicit political financing, and cyberattacks. Following this is a chapter on countering hybrid threats, focusing specifically on experiences in establishing election cooperation networks. Finally, a concluding chapter presents key findings and recommendations.

The primary audience for this report comprises institutions involved in organizing, supporting or contributing to electoral processes, especially in conflict-affected and fragile states, as well as countries exposed to hybrid threats, especially in Eastern Europe and the Western Balkans, where FBA is most active. As such, the report also underpins FBA's practical programming to strengthen democratic resilience among electoral actors in these regions.

02 Foreign Information Manipulation and Interference (FIMI) and Elections

FIMI is a core component of contemporary hybrid threats – a sophisticated machinery of influence designed to pollute the information environment and manipulate public opinion. A commonly observed strategy integrates industrial-scale content production with multi-tiered dissemination.[29]

First, adversaries produce vast quantities of content – from articles and memes to AI-generated deepfakes – meticulously crafted to exploit societal "wedge issues" like immigration and economic anxiety.[30] Second, this content is disseminated using a range of techniques, including automated bot networks, coordinated inauthentic accounts, and "influence-for-hire" schemes that use paid influencers to launder state-sponsored narratives.[31] This often involves deceptive infrastructure, such as the "Doppelgänger" technique, cloning legitimate news websites to lend credibility to disinformation.[32]

> *"...reveals a strategic intent that extends far beyond election meddling, aiming instead to wage a persistent information war."*

Overarching strategic frameworks guide these tactical efforts. Leaked Russian documents reveal that operations are directed by meticulously crafted "metodichka" (narrative manuals) that detail how to escalate internal tensions to advance foreign policy objectives. This reveals a strategic intent that extends far beyond election meddling, aiming instead to wage a persistent information war.[33]

2.1. RECENT TRENDS

The period since the beginning of 2024 has provided a series of stark, real-world case studies that illuminate the evolving tactics and escalating intensity of hybrid threats targeting democratic elections. These events, spanning the EU, the United States (US), and Europe's eastern neighbourhood, offer crucial insights into the current operational playbooks of malign actors and the vulnerabilities they seek to exploit.

The 2024 European Parliament Elections: A Transnational Target

The June 2024 European Parliament elections were a significant transnational target for FIMI campaigns, with fact-checkers detecting a sharp rise in EU-focused disinformation across at least eleven countries.[34] Russia's Social Design Agency orchestrated a "comprehensive counter-campaign against Europe", designed to bolster far-right and Eurosceptic candidates by amplifying narratives of economic ruin and the erosion of national values.[35] This campaign

was, in part, executed through the sprawling "Doppelgänger" network, which leveraged cloned media websites and established influence networks to inject pro-Kremlin disinformation into the European information ecosystem.[36]

Romania's Annulled Election: A Watershed Moment

In a dramatic demonstration of impact, Romania's Constitutional Court annulled the first-round results of its late 2024 presidential election, citing coordinated foreign interference and opaque online financing. Intelligence agencies revealed a sophisticated campaign centred on TikTok, where paid influencer networks and large-scale inauthentic activity amplified a previously marginal, pro-Kremlin candidate whose online presence was inconsistent with declared campaign spending.[37] At the EU level, the Commission initiated formal Digital Services Act (DSA) proceedings to investigate TikTok's risk mitigation and recommended systems in relation to the Romanian election.[38]

Analysts identified a network of thousands of dormant and hijacked accounts, many traced to Russia and Iran, that were activated to flood the platform with manipulative content. As described in Chapter 3, this was coupled with strong indications of illicit foreign financing, as the candidate's online presence deviated from the officially declared campaign spending. While independent observers urged caution, noting the difficulty of proving a direct causal link between online activity and votes, the case illustrates how a well-resourced FIMI campaign can undermine confidence in an electoral outcome to the point of invalidation. At the same time, the Romanian case drew criticism, with observers pointing out that reliance on classified intelligence creates gaps in transparency and contestability. Additionally, they argued that sweeping remedies risk overshooting the ultimate goal.

Moldova's Struggle: Election under Hybrid Fire

Moldova provides a real-time example of a country defending against an intense and integrated hybrid assault. While Russia's 2014 attack on Ukraine established the "hack-and-broadcast" playbook, which fuses cyber intrusion with information manipulation,[39] its operations in Moldova have evolved into a state of chronic, multi-domain pressure aimed at capturing the state through the ballot box.[40]

The country's 2024 presidential election and EU referendum faced what international observers described as a "hybrid war" directed from abroad.[41] FIMI served as the integrating layer for this multi-domain coercion. Russia-aligned actors ran a narrative-driven campaign to portray the pro-EU government as incompetent, amplified by coordinated Telegram networks and the Moldovan Orthodox Church.[42] This information assault was underwritten by large-scale illicit financing – with an estimated USD 39 million channelled from a fugitive oligarch to fund vote-buying and protests – and complemented by threats of physical disruption, such as fake bomb threats at diaspora polling places.[43]

The tactics deployed in 2024 were a prelude to an even more intensive campaign targeting the pivotal September 2025 parliamentary elections. Leaked Kremlin documents revealed a multi-pronged strategy aimed at derailing Moldova's path to the EU and ultimately removing President Sandu from power.[44] The plan detailed a textbook hybrid threat model, including:

- A widespread disinformation campaign on platforms like Telegram, TikTok and Facebook, using narratives that paint President Sandu as a foreign puppet pushing the country into war.[45]
- Large-scale illicit financing to buy votes and fund pro-Russian parties.[46]
- The use of compromising material ("kompromat") to pressure officials and the recruitment of the Moldovan diaspora to travel and vote.[47]
- The recruitment of young men from sports clubs and criminal networks to stage violent provocations and disruptive protests.[48]

This plan was actively operationalized. On 22 September 2025, just days before the election, Moldovan authorities conducted a massive operation to dismantle a Russian-backed destabilization plot. Police detained 74 people and conducted over 250 searches, breaking up a network allegedly run with support from Russia's intelligence service, which operated the so-called "Trust" media group to spread propaganda.[49] This followed earlier efforts to crack down on the information front, including an official request to block 443 TikTok channels.[50]

These actions are layered on top of persistent cyber pressure. Since 2022, pro-Russian hacker groups have launched cyberattacks on government institutions, established leak websites, and breached parliamentary email servers in preparation for hack-and-leak operations.[51] In response to these escalating threats, Moldova has received significant international support. In 2023, the EU Partnership Mission in the Republic of Moldova (EUPM) was established to enhance Moldova's resilience to hybrid threats, including cybersecurity and FIMI. Additionally, in 2025, the EU deployed a Hybrid Rapid Response Team and the EU Cybersecurity Reserve to Chişinău – the first-ever activation of the EU's cyber rapid assistance mechanism – to support the country's election defence.[52]

Taken together, the Moldova case demonstrates the reality of modern electoral interference: it is not a series of isolated incidents, but a fully integrated hybrid war. This underscores the need for states to leverage international expertise, learn from one another, and build a whole-of-society defence to shore up their critical democratic systems.

Ukraine: Information Warfare as an Instrument of Conventional Conflict

With elections in Ukraine suspended under martial law, Russia's FIMI campaigns against Ukraine function as a pre-emptive assault on its future democratic processes. The Social Design Agency's "Comprehensive Counter-Campaign against Ukraine" is a direct instrument of the war effort, aimed at undermining Ukraine's leadership, demoralizing its armed forces and degrading social cohesion.[53] By amplifying narratives of corruption and stoking political rivalries, the long-term campaign seeks to ensure that when post-war elections are held, the electorate is fragmented and receptive to pro-Russian alternatives.[54]

The current efforts have evolved from earlier playbooks that fused cyber intrusions with information manipulation. Before and during Ukraine's 2014 presidential election, Moscow-aligned political networks, media assets and oligarch intermediaries were mobilized to advance pro-Kremlin agendas and blunt Ukraine's European trajectory. Pro-Russian parties and figures served as vectors for policy alignment and message amplification, while business interests with ties to Russia extended Moscow's leverage.[55] In parallel, cyber-enabled interference targeted election mechanics: intrusions at the Central Election Commission deleted files and implanted malware designed to display fabricated results, supplemented by Distributed Denial-of-Service (DDoS) attacks to delay reporting; Russian state television subsequently aired the fake graphic – an early instance of fusing cyber intrusion to information manipulation.[56] The next election in Ukraine is expected to take place under challenging circumstances, with the country likely to face heightened external attempts to influence or disrupt the election process.

The 2024 US Presidential Election: A Multi-Actor Onslaught

The 2024 US election was a focal point for multiple foreign actors with distinct playbooks.[57] Russia deployed a broad toolkit, ranging from hoax bomb threats at polling locations to AI-generated deepfakes, the continued use of its "Doppelgänger" influence network, and the mobilization of domestic proxies.[58] The Department of Justice disrupted the "Doppelgänger" network, seizing 32 domains and unsealing charges against Russian operatives linked to Russian state media.[59] China's activity was more targeted, focusing on US "culture-war" fault lines and down-ballot races rather than the presidential contest.[60] Iran combined online reconnaissance with hack-and-leak operations, with US authorities indicting Iran-linked actors for compromising a presidential campaign to steal and leak materials.[61] In response, US agencies pursued a "pre-bunking" posture and used a combination of indictments, sanctions and seizures to raise costs and disrupt infrastructure.[62]

Independent assessments note that, while the cumulative influence effort was substantial and increasingly AI-enabled, the operational impact on core election mechanics was contained – but the informational harm (confusion, polarization, cynicism) remains a central risk for future cycles.[63]

2.2. CHALLENGES IN DETECTION, ATTRIBUTION AND RESPONSE

Defending against FIMI presents several formidable challenges. Attribution remains a critical bottleneck, as the use of proxies and complex information laundering techniques is deliberately designed to create ambiguity and hinder a timely, proportional response.[64] The sheer speed and scale of modern campaigns, amplified by AI, often overwhelm traditional countermeasures like fact-checking.[65] Furthermore, democracies face a difficult balance between security and freedom of expression, a dilemma that malign actors exploit by framing defensive actions as censorship.[66]

A central challenge is platform accountability, as the business models of many social media companies reward polarizing content that maximizes engagement.[67] Securing meaningful transparency over ranking algorithms, content moderation rules and researcher data access remains a contentious regulatory and political challenge.[68] The EU's DSA represents a significant regulatory response, shifting obligations onto very large online platforms to assess systemic risks and increase transparency. Enforcement has begun, with formal proceedings tied to election integrity in 2024, but compliance remains uneven.[69] In parallel, platforms are recalibrating their approach: Google and Meta have announced plans to restrict or end political advertising in the EU, citing the new regulatory landscape.[70]

While regulation is increasing, other forms of transparency are eroding. Meta's retirement of its CrowdTangle tool, which provided real-time insights into public social-media content, reduced visibility into influence networks ahead of major 2024 elections.[71] Voluntary industry efforts, such as the "Tech Accord" to counter deceptive AI in elections, have been criticized for lacking accountability and measurable benchmarks.[72]

A new accountability front has opened around AI provenance and detection. While open standards, such as C2PA Content Credentials, are being adopted to label authentic media, they face a cat-and-mouse dynamic with incomplete coverage.[73] In parallel, tools like Google DeepMind's SynthID embed imperceptible, robust watermarks directly into AI-generated media at the time of creation.[74] However, even Google's own AI chatbots have yet to implement this standard and still cannot detect content they have produced. This underscores the urgent need for strong, interoperable and enforced standards for content provenance.

As generative AI continues to lower costs for influence operations, even as platforms add guardrails, maintaining regulatory control and oversight over these operations will remain a challenge.[75] Research has also documented cases where state-linked or sanctioned entities have been able to buy or place influence content despite platform policies, underscoring the need for auditable ad-tech controls and sanctions screening that work in practice.[76]

2.3. WHAT CAN BE DONE? STRATEGIES TO COUNTER FIMI TARGETING ELECTIONS

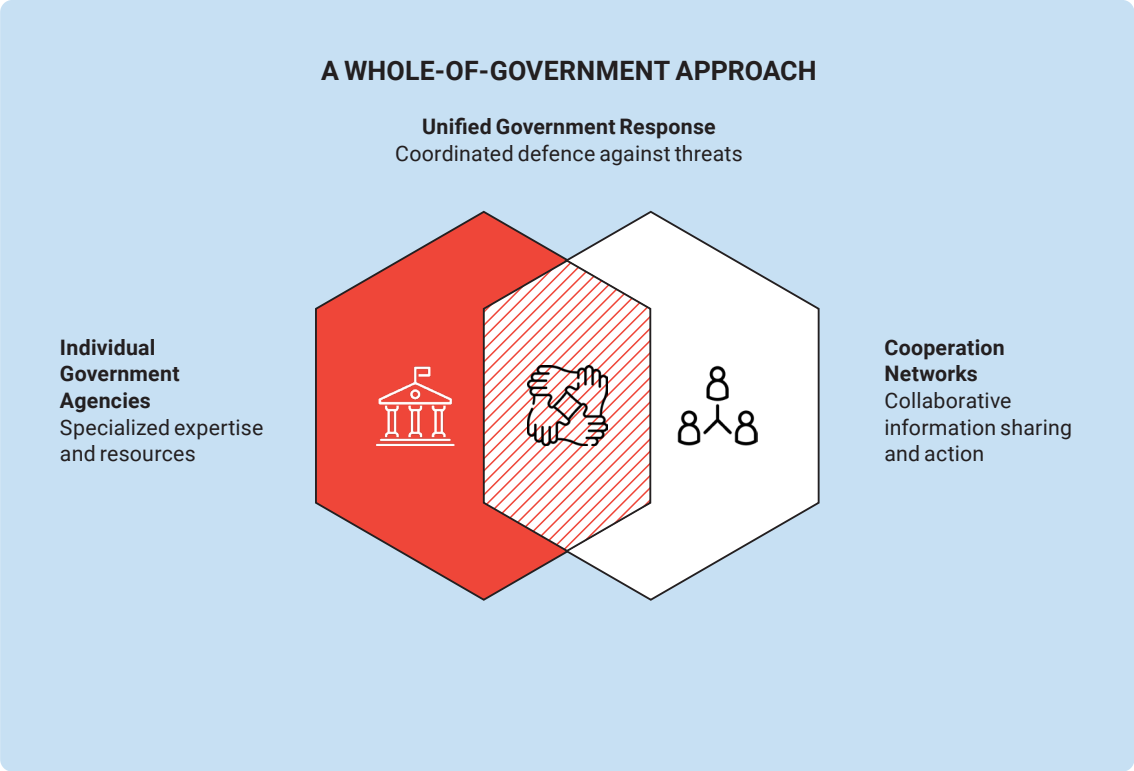
The evolution of electoral interference from episodic attacks into a state of chronic, systemic information conflict requires a fundamental shift in defensive strategy. The speed and scale of modern FIMI campaigns, amplified by AI, often outpace traditional countermeasures, such as reactive fact-checking. Therefore, an effective response must be proactive, collaborative, and multi-layered, addressing the threat's institutional, regulatory and technological dimensions. Crucially, countering FIMI requires a conceptual response that is compatible with democratic norms. The modern, rights-respecting approach adopted by the EU is behaviour-centric. It focuses on targeting observable, manipulative conduct – such as bot networks or coordinated inauthentic accounts. This

allows a state body to counter hostile operations on firm, evidence-based grounds without undermining freedom of speech.[77]

> *"Crucially, countering FIMI requires a conceptual response that is compatible with democratic norms."*

A Whole-of-Government Approach through Cooperation Networks

This report highlights how adversaries deliberately exploit the seams between different agencies' responsibilities, making a siloed security response insufficient. The foundational strategy for countering FIMI targeting elections is to establish an equally integrated and networked defence, as has been done in several countries during recent elections (as detailed in Chapter 5).



Strengthening Legal and Regulatory Frameworks

A central challenge in countering FIMI is platform accountability. The EU's DSA provides a leading model for regulating the information environment, notwithstanding existing debates about its applicability. The Act shifts obligations onto "very large online platforms" to assess systemic risks to democratic processes, make their recommender systems more transparent and provide vetted researchers with access to data. Enforcement of such principles is critical to creating an information environment less vulnerable to manipulation by design.

This regulatory approach must also extend to illicit political finance, which serves as a key vector for funding FIMI campaigns. It is crucial to close loopholes related to anonymous online donations, the unregulated use of third-party campaigners and opaque spending on social media advertising (as detailed in Chapter 3).

Fostering a Whole-of-Society Resilience

A purely state-centric defence is insufficient, as long-term democratic resilience depends on an informed, critical and engaged society. A key strategy is therefore to invest in a whole-

of-society approach that empowers citizens and strengthens the public information space from the ground up.

Independent media ecosystems are essential to this approach. Yet they often operate under severe constraints – financial precarity, market concentration, politicized state advertising, and legal or physical pressure – that threaten both sustainability and editorial independence. Addressing these challenges requires complementary lines of effort.

National initiatives to enhance media and AI literacy are essential for equipping citizens with the skills to critically identify and assess manipulative content, thereby strengthening the population's "cognitive defences". This must be complemented by robust support for independent media, as a diverse and well-resourced media landscape provides a vital bulwark against disinformation by offering citizens reliable, fact-based alternatives to state-sponsored propaganda.

A critical element of this support is dedicated investment in investigative journalism. Time and again, investigative media have proven most effective in uncovering the mechanics of hybrid threats – from exposing complex illicit financing schemes and mapping disinformation networks to identifying the actors behind hack-and-leak operations. Such work is crucial not only for public understanding but also for providing the evidence base needed for official government action.

Building Proactive Defences and Technological Resilience

Given the difficulty of removing disinformation once it has spread, a proactive posture is essential. The objective, however, is not to counter every false claim circulating online. The centre of gravity lies in radical, routine transparency that reduces ambiguity and provides verifiable facts others can rely on.[78]

This is operationalized through a publicly accessible "source-of-truth" hub – containing procedures, FAQs, corrections and change-logs – that standardizes where the public and media find authoritative information and establishes a durable reference point during incidents.[79] Such practices measurably reduce the information voids that adversaries exploit and strengthen institutional credibility over time.[80]

Within this transparency posture, pre-bunking is used selectively and time-boxed around known risk windows (registration, polling, results) to inoculate against tactics, not to refute every narrative, while designing for uneven uptake and incomplete provenance coverage.[81] The emphasis is on concise "what to expect/how to verify/where to report" explainers that help audiences recognize manipulation patterns (e.g., imposter content, hack-and-leak framing) and route attention to the canonical page.[82] Done this way, pre-bunking is a cost-effective accelerant of transparency, not a parallel content war.[83]

This approach recognizes limits. It is impossible to counter every piece of disinformation, and motivated audiences will sometimes prefer congruent falsehoods. The strategy, therefore, is to own the facts, narrow ambiguity and target manipulative behaviours – so that credible actors have a stable anchor to reference and the public has a predictable place to verify.[84]

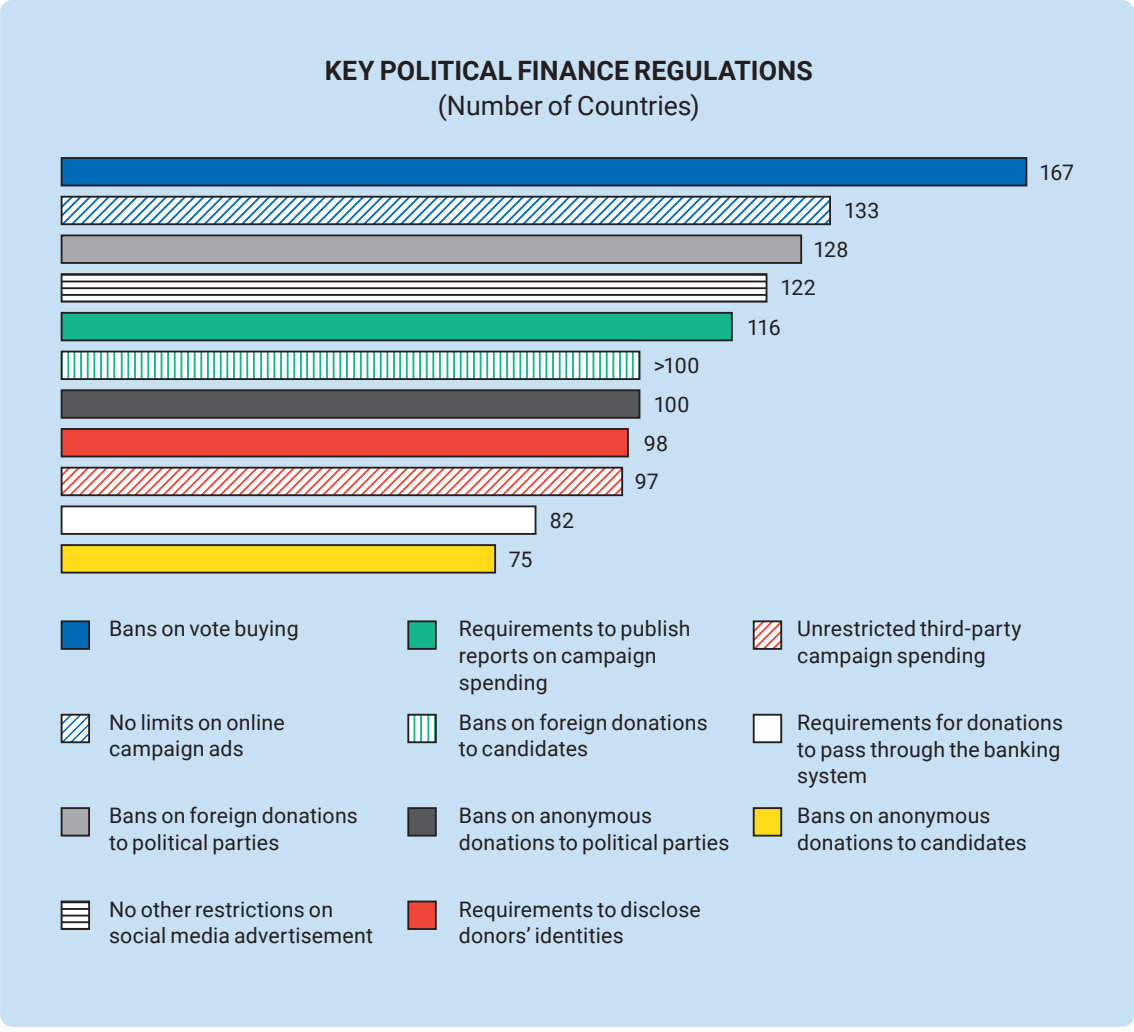
This transparency strategy must be paired with a plan to address the technological arms race, particularly the challenge of AI-generated synthetic media. Defending against deepfakes and voice clones requires moving beyond simple detection, which is locked in a "cat-and-mouse dynamic" with adversaries.[85] The forward-looking strategy is to invest in and mandate the use of content provenance and watermarking technologies. Open standards, such as C2PA Content Credentials, which serve as a digital authenticity label, and robust watermarking tools, like Google DeepMind's SynthID, which embeds an imperceptible, machine-detectable signature into AI-generated media at the time of creation, are critical for re-establishing a baseline of trust in the digital ecosystem.[86]

Ultimately, these strategies must be integrated. As the report's overarching finding concludes, electoral defence in the modern era must be a continuous, adaptive, proactive and collaborative process.

03 Illicit Political Finance and Hybrid Threats

Money is not inherently corrosive in elections; it is also essential. Parties rely on it to promote ideas, recruit members and train candidates, while electoral bodies need it for civic education and to administer election logistics. Yet money in politics poses serious risks to democracy, from unequal access to funding and corruption incentives, to illicit or illegal financing aimed at influencing elections.[87]

This includes money used illegitimately or illegally to interfere with elections at home and abroad. The latter is particularly concerning given the distortions it causes throughout the democratic system, the erosion of public trust it generates, and the geopolitical implications it entails.



Foreign electoral interference through illicit political finance is increasingly recognized, though not a new phenomenon. In Montenegro, for instance, during the 2016 parliamentary elections, allegations of foreign campaign financing arose, with claims that the opposition was serving foreign interests, while already in Moldova's 2021 early elections, observers similarly flagged concerns over foreign funding.[88]

3.1. ILLICIT POLITICAL FINANCE AS A VECTOR FOR INTERFERENCE

There are three critical areas through which malign actors typically seek to influence elections through illicit political financing. These are: (1) vote buying; (2) foreign and anonymous donations, including through cryptocurrencies; and (3) third-party contributions, funding for social media advertising and influencers.

Vote Buying

Although banned in 167 countries, vote buying remains a common means of influencing elections.[89] During Moldova's 2025 parliamentary elections, international observers noted the extent to which vote-buying schemes aimed at influencing voters had been identified, with an organized network funded by Russia coordinating these efforts.[90]

The country had already faced similar challenges in previous elections. In the 2023 local elections, for example, political operatives linked to Russia were accused of attempting to channel funds into the country for vote-buying purposes, thereby furthering Russian interests.[91] Worse still, in the 2024 presidential election and constitutional referendum, international observers noted how law enforcement, many international actors and civil society described Moldova as the target of an ongoing "hybrid war" involving illicit political finance, disinformation and cyberattacks.[92]

These schemes are believed to have involved Russian distribution of cash cards. Analysts described the alleged modus operandi as follows:

> Millions of dollars in cash have reportedly been smuggled into the country by individuals connected to the fugitive, US-sanctioned oligarch Ilan Shor, circumventing law enforcement efforts to stop the illegal flow of funds. Authorities had organized searches at the airport to halt this parade of individuals travelling to Moscow to bring back clandestine cash. However, Russia has found other ways to channel funds into Moldova. Through the Russian MIR payment system, financial resources are reportedly being funneled to Moldovan voters, particularly through the economic networks in the Transnistria region—a breakaway territory that has long served as a base for Moscow's influence operations.
>
> Moldovan authorities have raised alarms about large-scale vote-buying, with the General Police Inspectorate documenting cases of bribery involving at least 130,000 citizens and more than fifteen million dollars in illicit transfers from Russia in September alone. In reality, the scale might be significantly bigger, with some officials estimating it at around $100 million for the entire campaign.
>
> Funds are being funneled into schemes designed to establish a national vote-buying network, resembling financial pyramids with intricate layers of transactions aimed at evading scrutiny. These funds range from "social" allowances for Moldovan pensioners to salary "bonuses" for employees of local government structures in the autonomous territory of Gagauzia. The money is now also, according to police and independent reporting, finding its way into the hands of so-called local "coordinators" and "supporters" of the "Victory" electoral bloc, a political entity created in and reportedly controlled from Moscow (Olari 2024).

Foreign and Anonymous Donations

Bans or limits on foreign and anonymous donations are among the most common regulations in political finance. As of 2025, 128 countries prohibit foreign donations to political parties, with more than 100 countries extending the ban to candidates. Anonymous donations are likewise restricted in 100 countries for parties and 75 countries for candidates.[93]

The ban on foreign donations generally rests on the principle that external interests should not influence national politics. In contrast, the ban on anonymous donations usually aims to block otherwise illegal contributions. Yet implementing these rules is one of the most complex tasks for oversight bodies. Foreign contributions for election interference can move largely undetected across borders, often transiting through offshore jurisdictions and tax havens, where their true source is easily concealed; this makes it exceptionally difficult to trace the funds and conclusively identify their foreign origin.[94]

Cryptocurrencies further complicate the landscape by enabling opaque financial flows, including those from adversarial actors seeking to influence elections abroad. Their use has expanded rapidly over the past decade: while Bitcoin remains dominant, more than 16,000 cryptocurrencies are now traded across over 1,300 exchanges, with an estimated 861 million users worldwide – about 11 per cent of the global population in more than 150 countries.[95] The market is furthermore expected to continue growing, with the value of crypto trading projected to rise from $71.35 billion in 2025 to over $260 billion by 2032.[96]

Political finance has been directly affected, as the anonymity of most cryptocurrency transactions makes foreign donations especially difficult to trace.[97] A notable example was the 2016 US presidential election, when a grand jury indictment revealed that Russian funds were allegedly channelled through cryptocurrency exchanges.[98] The case highlighted the limitations of oversight, demonstrating that even a system with relatively robust safeguards struggled to address cryptocurrencies, as legislation permitted political committees to accept contributions while taking only “minimally intrusive” steps to verify donors’ nationalities.

Third-Party Contributions, Funding for Social Media Advertising and Influencers

Third-party spending can serve as a channel for foreign funds intended to influence elections, with organizations or individuals, including shell companies, NGOs or charities acting as front

organizations, campaigning for or against parties and candidates, and becoming conduits for external influence.[99]

Social media advertising is another powerful tool for fundraising and political operations, with digital campaign spending rising sharply worldwide, particularly since the COVID-19 pandemic.[100] Online media advertising offers foreign actors an easy avenue to interfere in elections, enabled by the physical distance between the sources of advertising and their targets, as well as the ability to conduct micro-targeting and personalize the content generated.[101] For instance, a foreign actor can purchase social media messaging services on behalf of a campaign, beyond the reach of domestic oversight, while the opacity of online payments allows donors to remain anonymous.[102]

The 2018 Cambridge Analytica scandal provides an early example, involving the misuse of private Facebook data from over 50 million users during the 2016 US elections. It also exposed the illegal employment of dozens of foreign nationals, whose work on campaign messaging, data analytics and advertising was deemed an unlawful in-kind foreign contribution.[103]

The 2024 US election offers another example. As part of "Operation Doppelganger", the Department of Justice seized 32 internet domains used by the Russian government for malign influence campaigns. According to the investigation, the operation relied on paid influencers and paid social media advertisements, some of which were AI-generated, and used fake social media profiles posing as US or other non-Russian citizens, to direct users to cybersquatted sites disguised as legitimate news outlets.[104]

That same year, Romania's election showed similar patterns, with the Constitutional Court annulling the first round of voting. One candidate reported no campaign spending, despite an extensive online presence and intelligence findings suggesting undeclared funding from external sources. The case highlighted broader risks of strategic corruption, including third-party financing through proxies to fund digital advertisements without revealing their origins or adhering to legal ceilings, hybrid political finance warfare that boosts online exposure from abroad, and weak oversight by electoral authorities unable to track complex digital advertising networks.[105]

More recently, during Poland's 2025 presidential run-off, international observers reported suspected foreign-funded Facebook ads. Between mid-April and mid-May, two new profiles spent approximately PLN 500,000 ($139,000) on more than 100 video ads supporting one candidate and attacking others, outspending the candidates themselves. The case, reported as likely foreign funding, remains pending. Observers criticized the authorities' delayed response, while Meta stated the ads did not breach its standards or national law. Another account was found to have run ads worth PLN 388,000 (approximately $108,000), allegedly using funds channelled from abroad via a civil society organization. And even though complaints were filed to the National Election Commission and the prosecutor's office for alleged illicit foreign funding, observers noted that "while Meta applies, by means of an automated process, spending limits to advertisers, the implementation of internal rules by a social platform is outside the current scope and capacity of the campaign finance oversight body".[106] This case underscores the growing challenge that foreign-funded online campaigning poses to national oversight mechanisms, as well as the limitations of existing regulatory frameworks in ensuring transparency and accountability in digital political advertising.

3.2. WHAT CAN BE DONE? STRATEGIES TO STRENGTHEN POLITICAL FINANCE REGULATION AND OVERSIGHT AGAINST FOREIGN INTERFERENCE

Given the numerous challenges outlined above, should the response focus on setting more stringent political finance regulations or strengthening oversight?

Tightening Regulations

A typical response is to lower donation limits and restrict campaign spending. While sometimes necessary and even desirable, excessive limits risk creating new imbalances and ultimately affecting the outcome of elections. As mentioned previously, parties and candidates require access to legitimate funds to run their operations without interference; without these funds, they may resort to hidden foreign support or underreport income and expenditure.[107]

That said, stronger regulations are often needed to prevent and mitigate hybrid threats to elections, even though such measures must be carefully designed to ensure that counter-efforts do not themselves generate new distortions or restrictions that undermine core democratic principles.

Bans and Limitations

A vital step is banning foreign and anonymous donations to parties and candidates, where they are not already prohibited.[108] Regulations can also be refined by aligning reporting periods with the actual campaign timeframe – rather than relying on artificial or narrowly defined reporting periods that exclude much of the real campaigning – when the risk of foreign interference is arguably most significant. Identifying mismatches between income and expenditure may then help uncover illicit funding sources.

Another challenge to overseeing foreign interference in elections is the use of third parties to channel campaign spending, a practice still unrestricted in 97 countries.[109] Social media advertising is a significant loophole: 133 countries impose no limits on online campaign ads, and 122 apply no other restrictions. Curbing foreign influence, therefore, requires stronger regulation of online political advertising, including more precise definitions of digital campaigning and greater transparency requirements.[110]

International Alignment

Another priority is strengthening regulations across jurisdictions and advancing international norms and mechanisms to improve transparency in transnational financial flows. This is crucial since illicit political finance often moves through tax havens and offshore structures to conceal its origin. Central to these frameworks is the Financial Action Task Force and its anti-money laundering standards, particularly those related to politically exposed persons and offshore jurisdictions.[111]

Addressing Cryptocurrencies

Addressing hybrid threats to elections also requires more explicit rules on the use of cryptocurrency in political finance, given their anonymous status in most cases and the lack of robust regulation. Oversight is often complicated by the lack of clarity on their legal status – whether they are considered assets, securities or fiat currency – and, linked to that, by the different legal treatment of monetary and in-kind contributions. In most systems, cryptocurrencies are considered assets and are therefore treated as in-kind contributions; however, this is not always the case, making it more challenging for monitoring agencies to determine the applicable legal framework and track them.[112]

In response, some countries have limited or outright banned the use of cryptocurrencies in political finance, aligning with broader restrictions on foreign and anonymous donations. Ireland, for instance, adopted a 2022 law prohibiting cryptocurrency donations to parties.[113] Such measures are especially relevant for those cryptocurrencies that are inherently anonymous, which include some of the most popular ones.[114] Another (indirect) way to limit the use of cryptocurrencies and mitigate related risks in political finance is to require donations to pass through the banking system, as is the case in 82 countries.[115]

Improvidng State Oversight

More critical than tightening regulations is enforcing those already in place. Yet oversight remains the weakest link, with agencies often hampered by unclear mandates, limited capacity and poor coordination. This is particularly critical in relation to the collaboration required between election authorities and financial intelligence units, given the latter's privileged access to key information needed to monitor political finance flows.[116]

> *"More critical than tightening regulations is enforcing those already in place."*

Stronger capacity and collaboration are moreover vital for oversight bodies monitoring cryptocurrency transactions, particularly cooperation with virtual currency exchangers. As financial intermediaries, these actors can provide key information to identify foreign donors and, in some jurisdictions, are already bound by anti-money laundering rules.[117] Equipping oversight bodies with better capacity to monitor online advertising spending is equally essential.[118]

Significantly, the relationship between state and non-state oversight is mutually reinforcing. When authorities publish information promptly and in an accessible manner, civil society can better scrutinize reported spending against its own monitoring.[119] While most countries publish such reports (116), fewer (98) require disclosure of donor identities. The latter is a vital ingredient for exposing foreign actors seeking to influence an election through funding of parties or candidates.[120]

Strengthening Civil Society and Media Monitoring

Civil society, journalists and whistle-blowers play a vital role in exposing illicit political financing, particularly when linked to foreign malign actors seeking to influence elections. Yet media freedom and integrity have deteriorated in recent years, with the Varieties of Democracy Institute reporting increased censorship in 44 countries in 2024 and growing threats to journalists.[121] The trend is also evident in Europe, where digital surveillance, disinformation and political influence over public media have contributed to declines.[122]

More broadly, civil society actors face a range of challenges, including limited access to information and resources, political pressure, and a restricted civic space. These factors constrain their ability to perform their watchdog role effectively.[123] This underscores the need for both robust transparency by authorities and protections for independent oversight, access-to-information guarantees, anti-SLAPP (Strategic Lawsuit Against Public Participation) measures, fair access to state advertising markets, and secure channels for researcher access.[124]

It is also important to note that the media can itself be a target of foreign interference (see Chapter 2 on FIMI and elections). In such cases, outlets may not only fail in their oversight role on illicit political finance but also become channels for mis- and disinformation.[125]

04 Cybersecurity in Elections

The digital domain remains a critical and highly contested vector for electoral interference. Cyber operations are rarely isolated events; instead, they are often integrated into broader hybrid threat campaigns, frequently serving as the primary enabler for information manipulation and psychological operations. The threats can be broadly categorized into those targeting the core electoral infrastructure and those targeting the campaigns, parties and officials who participate in the process.

The period since 2024 has been marked by two transformative trends: the convergence of state-sponsored operations with the cybercrime ecosystem, and the emergence of AI as a potent force multiplier for malicious actors.[126] This convergence has led to increased sophistication and interconnectedness of threats, blurring the lines between espionage, disruption and profit-driven crime, thereby demanding continuous strengthening of cybersecurity resilience.[127]

4.1. THE EVOLVING THREAT LANDSCAPE: CONVERGENCE, COMMERCIALIZATION AND AI

The macro-level shifts in the cyber threat environment define the current challenges to election security. Analysis must move beyond a simple catalogue of threats to explain the underlying dynamics that make adversaries more capable, adaptable and difficult to counter.

The Cybercrime-as-a-Service (CaaS) Ecosystem: A Strategic Symbiosis

The traditional distinction between state-sponsored Advanced Persistent Threats (APTs) and financially motivated cybercriminals is narrowing – though not disappearing. For many years, concerns have been raised about the political use of cyberattacks linked to organized crime, with scandals revealing, for instance, the creation of networks to spy on journalists.[128] A recent study from Europol further highlights the blurring of lines between state-sponsored operations and organized crime, where criminal syndicates are leveraged for their technical skills and infrastructure.[129]

This has given rise to a professionalized Cybercrime-as-a-Service (CaaS) market, which aids state-nexus actors by providing specialized capabilities and a layer of plausible deniability.[130] These services are increasingly utilized in geopolitically motivated campaigns, enabling state actors to augment their abilities, conduct disruptive attacks and engage in sophisticated information operations.[131]

What is actually changing? The convergence reflects two overlapping dynamics:[132]

- Outsourcing for deniability: States task, enable, or tolerate criminal and proxy operators to create additional layers of separation and complicate attribution.

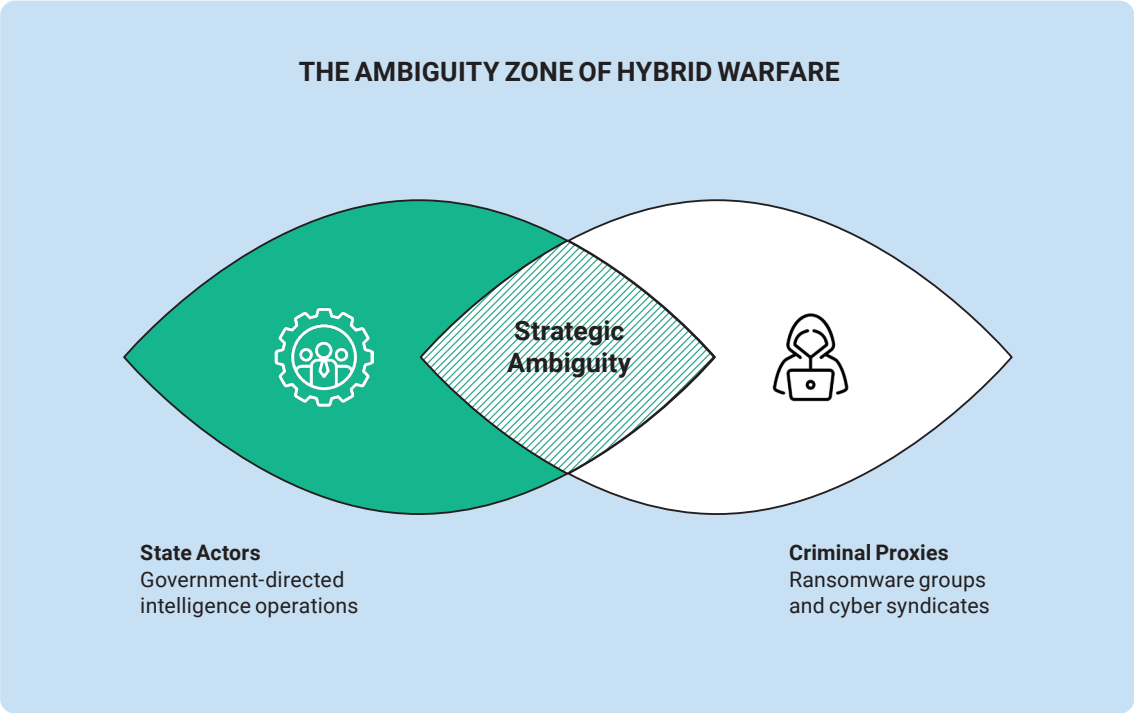
- Market-driven diffusion of capability: Criminal ecosystems now offer APT-adjacent tools “as-a-service”, lowering costs and accelerating operations without altering states’ core strategic aims.

In essence, this is less a doctrinal shift in state intent than an operational evolution that expands options for plausible deniability and surge capacity.[133]

State actors – notably Russia, China and Iran – are consistently identified as the primary foreign threats to critical infrastructure, including election systems.[134] They can now leverage this CaaS ecosystem to a significant effect. For example, in July and August 2024, during the US election cycle, ReliaQuest – a cybersecurity company specializing in threat detection and incident response – investigated a coordinated phishing campaign impersonating an activist group. Emails urged targets to "sign a petition" and redirected them to infrastructure associated with a specific malware family. The objective was to entice users to click through and, on compromised sites, trigger drive-by techniques that commonly present fake browser-update prompts – ultimately installing a remote-access trojan or harvesting credentials.[135] This case illustrates the tradecraft and hand-offs typical of the ecosystem, but does not in itself demonstrate state direction.

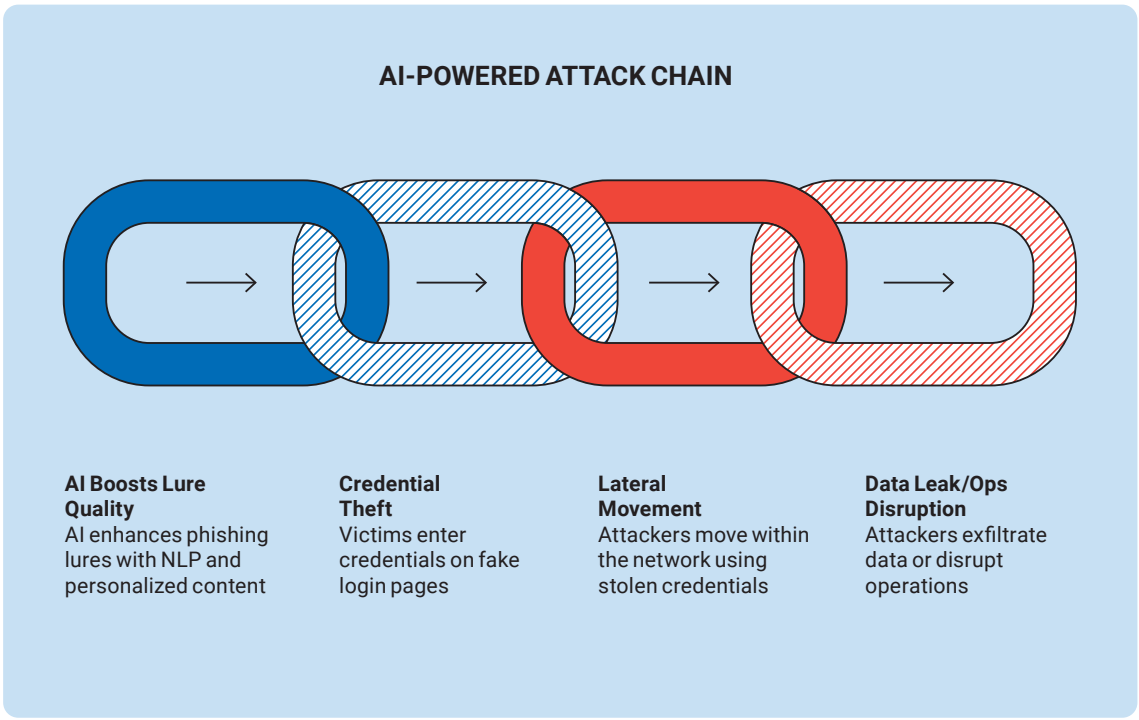
This state-criminal symbiosis is a deliberate feature of modern hybrid warfare, designed to complicate deterrence and attribution. When a state actor operates through a criminal proxy, it creates strategic ambiguity. An attack may be launched by a known ransomware group, but be directed, enabled or tolerated by a state intelligence service. This easily paralyses traditional response mechanisms. It becomes unclear whether an incident is a matter for law enforcement to pursue a criminal syndicate or for national security agencies to deter a hostile state. This ambiguity provides the state sponsor with deniability and slows the international consensus required for a coordinated response, thereby maximizing the disruptive impact of the operation.[136]

The policy implication is that responses should combine behaviour-based thresholds – acting on harm and indicators first – with clear attribution standards and legal pathways that preserve due process while enabling timely defensive action.



AI as a Malign Force Multiplier: Offensive and Defensive Uses

The US Cybersecurity and Infrastructure Security Agency (CISA) assessed that for the 2024–2025 period, generative AI did not introduce entirely new categories of risk but significantly amplified existing ones.[137] AI, however, is being used to enhance the scale, speed and sophistication of social engineering attacks. This includes generating more polished, context-aware phishing emails, producing highly realistic fabricated images and deepfake videos, and creating counterfeit social media profiles to support influence operations.[138]



At the same time, many of the same AI techniques are being applied for defence purposes, such as anomaly detection, triage and auto-labelled phishing queues, underscoring that the technology itself is not the challenge. Instead, the contest lies in the quality of adoption, governance, and the evolving arms race between offensive and defensive uses.

A widely cited experiment conducted by the cybersecurity firm Hoxhunt from 2023 to 2025 empirically demonstrated this evolution. In early 2025, their AI-powered phishing agent became 24 per cent more effective at deceiving users than elite human red teams, i.e., authorized testers who emulate real attackers to identify weaknesses.[139] While results may vary by organization and training baseline, this indicates that AI can now create superior spear-phishing attacks at scale, effectively lowering barriers to capabilities once associated with the most advanced adversaries.

Case studies from 2024 have already demonstrated the use of deepfake audio and video in high-stakes financial fraud, including an incident that defrauded a company of $25 million – illustrating the technology's maturity for deceptive purposes that could be repurposed or adapted for political ends.[140] However, isolated high-loss cases should not be over-generalized to all electoral contexts.

This technological shift has profound implications for election security, as it effectively lowers the barrier to entry for conducting advanced attacks. Less skilled actors can now generate highly persuasive, personalized spear-phishing content that was previously the domain of well-resourced APTs. This development increases both the volume and the overall quality of the threats. The classic indicators of phishing emails – such as poor grammar or generic salutations – are now often removed by AI.

This makes human-centric defences, like user awareness training, necessary but significantly more difficult and less reliable. Security teams and everyday election workers now face an even greater challenge, as the sheer volume and quality of potential breaches increase the likelihood of a successful attack.

This necessitates a shift in defensive strategy towards layered technical controls that rely less on human judgement and more on zero-trust infrastructure – where every user and device is continuously verified – supported by strong technical defences. These include phishing-resistant multifactor authentication and least-privilege and conditional access, which grant users only the minimum access required and only under specific conditions.

It also entails OAuth consent governance – that is, the careful management of which external applications can connect to core systems – as well as attachment and link isolation, whereby potentially risky content is opened in secure, quarantined environments. Application allow-listing is another essential measure that permits only approved software to run, as is macro blocking, which disables automated code in documents.

Other measures include device compliance and attestation – ensuring that all connected devices meet security standards – as well as just-in-time administration, which grants administrator rights only for the brief period needed, and prudent physical separation of critical processes, keeping the most sensitive systems offline or on segregated networks. Where feasible, these controls should be paired with streamlined incident reporting and clear communication protocols to contain downstream information effects.[141]

4.2. THREATS TO CRITICAL ELECTORAL INFRASTRUCTURE (NETWORKS, DATABASES AND VOTING TECH)

The technical infrastructure of elections – encompassing everything from voter registration databases to official results-reporting websites – remains a key target for malicious actors. While the direct manipulation of voting machines to alter vote counts is widely considered difficult to achieve at scale without detection, particularly in systems with robust paper audit trails, the surrounding infrastructure presents numerous vulnerabilities.[142]

A prominent tactic observed in recent years is the use of Distributed Denial-of-Service (DDoS) attacks. These are designed to overwhelm election websites and voter information portals with junk traffic, rendering them inaccessible. Ransomware attacks pose another significant threat. By encrypting critical systems and demanding payment for their release, these attacks can cause severe disruption.[143]

Breaches of Electoral Systems

Breaches of electoral databases pose a particularly insidious threat, as they may not disrupt services immediately but can erode public trust. Any breach, real or perceived, can be weaponized in FIMI campaigns to undermine public confidence in the electoral process.[144] In 2023, it was revealed that the UK Electoral Commission had been hacked by a likely state-affiliated actor, compromising the data of approximately 40 million voters. The attack, attributed in 2024 to a China-linked group, went undetected for many months. Although officials stated that it did not affect the casting or counting of votes, the exposure of such a massive voter register underscores the intelligence value adversaries see in election data.[145]

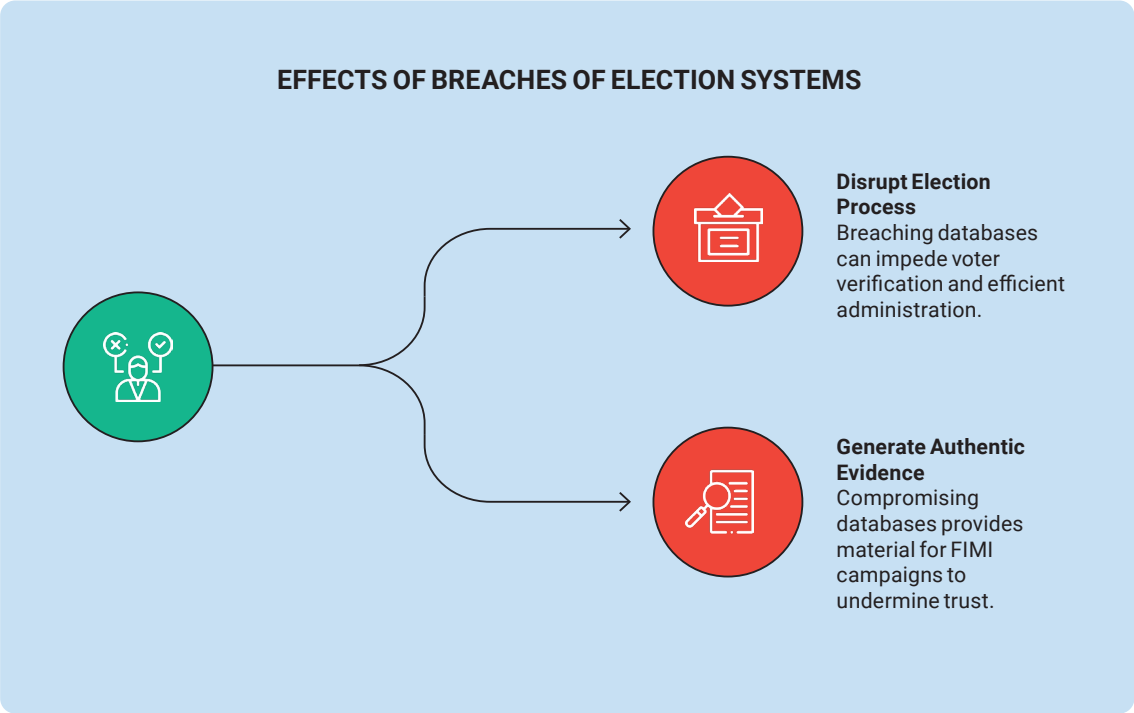
A now-infamous case occurred in Ukraine's 2014 presidential election. Russian hackers infiltrated the Central Election Commission's network and planted fake results showing a fringe nationalist winning; although Ukrainian cybersecurity units neutralized the malware in time, Russian state media still broadcast the bogus victory to deceive the public.[146] This incident highlights how even a thwarted cyberattack can be leveraged in information warfare to cast doubt on legitimate outcomes.

In conflict zones or high-tension regions, cyber threats to infrastructure often accompany physical and FIMI operations. Ukraine's electoral infrastructure has endured repeated assaults since 2014 as part of Russia's hybrid war. Beyond the 2014 episode, Ukraine's election IT systems have been targets of constant probing; officials reported waves of phishing and malware attacks on election commission staff leading up to the 2019 elections.[147] Since 2022, the ongoing war has further heightened concerns: any future elections in Ukraine, currently on hold under martial law, would likely occur amid extremely high cyber threat levels, including the possibility of disruptive attacks on power grids or communications networks during voting.[148]

The lesson from Ukraine and similar front-line states is that safeguarding electoral infrastructure is not just a technical endeavour but a national security imperative, requiring resilience planning for worst-case scenarios, including wartime conditions.

> *"Election systems represent a nexus of operational and informational threats. An adversary does not need to change a single vote to achieve a strategic victory."*

Election systems represent a nexus of operational and informational threats. An adversary does not need to change a single vote to achieve a strategic victory. By successfully breaching a voter database, an attacker can achieve two goals simultaneously. First, they disrupt the election process by impeding officials' ability to verify voters and administer the process efficiently. Second, and more importantly, they generate potent, authentic "evidence" that can be used to fuel FIMI campaigns designed to undermine trust in the election's legitimacy. This makes these databases arguably the single most valuable target for a hybrid threat actor, as compromising them serves multiple strategic objectives at once.



The Persistent Vulnerability of Voter Registration Databases

Voter registration systems are a primary target for cyberattacks and breaches. Ransomware attacks have directly impacted electoral administration by targeting these systems. An incident in 2024 in the United States forced a county to sever its connection to the state's voter registration system as a precautionary measure.[149] Similarly, in late 2024, a Russian-linked ransomware attack on the Clerk's Office at Jefferson County, Kentucky, while not compromising the voting system itself, disrupted operations and highlighted the vulnerability of interconnected government systems.[150]

Voter-registration databases determine who may vote and where. If attackers render them unavailable – through ransomware or denial-of-service – or surreptitiously alter records, such as addresses or ID flags, the likely consequences include longer queues, increased use of provisional ballots, voters arriving at the wrong polling station, and disputes about eligibility – even if vote counting itself is unaffected.

The incentives for attackers are threefold: availability, meaning cyber disruptions that block voter check-in or interrupt e-pollbook synchronization (the real-time updating of voter lists across polling stations and central systems); integrity, involving the editing or deletion of entries to create friction or selective disenfranchisement; and confidentiality, through the theft of personal data for intimidation or spear-phishing. Stolen credentials may also be used to pivot into other election systems.

The theft of voter data is a pervasive problem. Leaked data from US states accounts for an estimated 78 per cent of all voter data circulating on the dark web, with at least 23 states having suffered breaches. This exposed information is then weaponized for targeted disinformation, voter suppression tactics and identity manipulation, with the potential to send misleading messages about polling locations or even attempt fraudulent voting.[151]

The Dual Threat of Ransomware and DDoS Attacks

DDoS attacks continue to be a common tactic for disrupting access to election-related websites, including voter information portals and results-reporting sites.[152] The 2024 US election cycle saw a significant uptick in such attacks targeting campaign websites, political parties and county-level infrastructure. The cybersecurity firm Cloudflare reported blocking over 6 billion malicious requests targeting US election-related properties in the first six days of November 2024 alone, with some attacks reaching a peak of 700,000 requests per second.[153] Similar politically motivated DDoS campaigns were observed during the 2024 European Parliament elections, with websites of Dutch political parties being knocked offline.[154]

The strategic goal of these attacks often extends beyond technical disruption. As CISA and the US Federal Bureau of Investigation have publicly noted, while DDoS attacks are unlikely to prevent any eligible voter from casting a ballot, they can effectively hinder public access to official information and create a perception of chaos and incompetence.[155] This perception is then ripe for exploitation by disinformation campaigns, which can amplify the incident to undermine public confidence in the election's overall integrity and, by extension, democratic principles, values and processes.[156]

Similarly, ransomware attacks on local governments, even if not targeting election offices directly, can cause significant collateral damage. An increase in ransomware incidents targeting state, regional, tribal and territorial governments was reported in the second quarter of 2024. These attacks can disrupt election officials who rely on shared county IT infrastructure.[157] Incidents are not merely technical problems; they are instruments of information influence activities. Their primary target is not a server, but public perception. The adversary's success is measured not in servers crashed, but in news articles written and in social media posts that share narratives of a "hacked election". This makes the strategic communications response to such an incident as crucial as the technical response.

Compromising the Election Technology Supply Chain

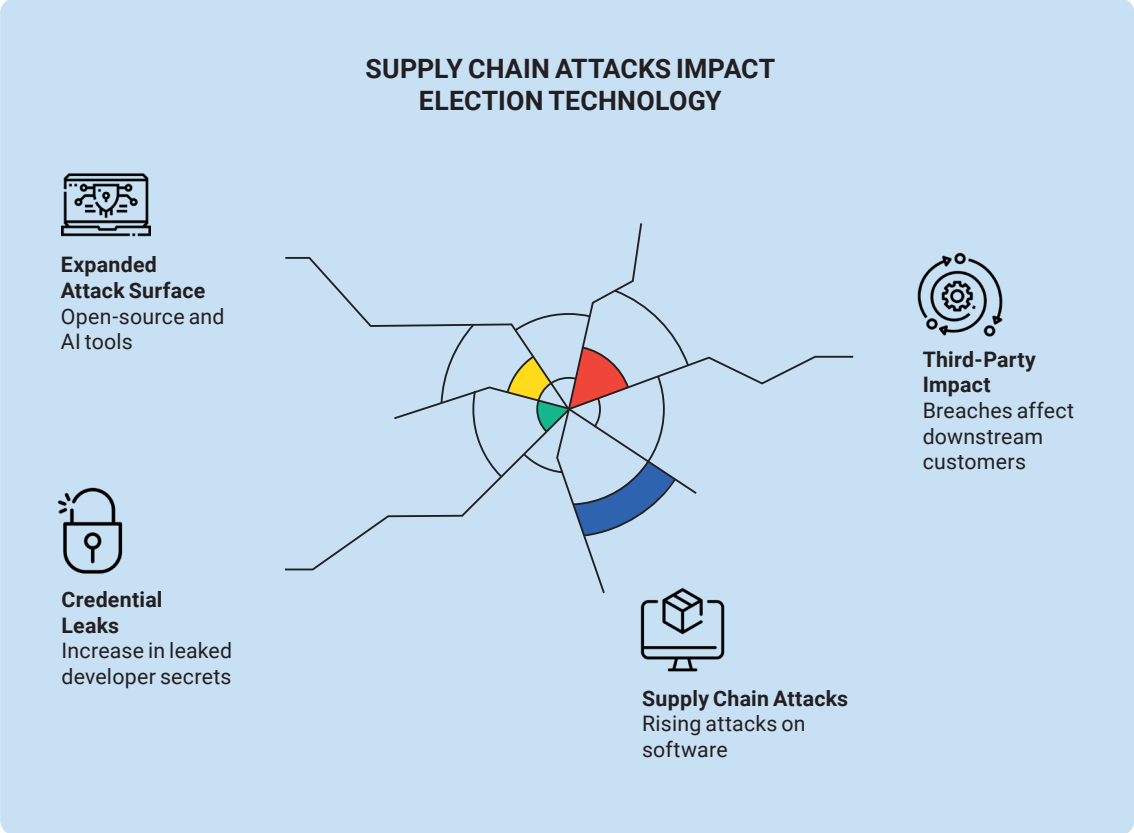
The security of election technology is heavily dependent on a complex software supply chain, which has become a primary target for sophisticated adversaries.[158] In this context, the frequency of attacks on the software supply chain has continued to increase, with a 25 per cent rise in incidents from late 2024 to mid-2025.[159]

The nature of these threats has evolved significantly. Beyond classic insertion of malicious code into software updates, or "package tampering", a 2025 report highlighted a more insidious trend: a 12 per cent rise in exposed developer secrets – hard-coded passwords, tokens and API keys used to authenticate between services – found embedded in commercial products.[160] Taken together, these patterns indicate that adversaries are targeting the entire software development lifecycle, not just the final product. At the same time, the widespread use of open-source software and the rise of AI development tools have expanded complex attack surfaces that can be exploited.[161]

High-profile breaches at major software and service providers demonstrate the cascading third-party impact of a single supply chain compromise, affecting thousands of downstream customers.[162] They serve as a warning for the election technology sector, which relies on similar third-party components and services. For election systems, this means that risks propagate via shared vendors and components. The threat has shifted from merely "infecting the product" to systematically "compromising the process". By stealing developer credentials or exploiting insecure design, an adversary can gain persistent access and multiple avenues for future exploitation.

> *"The threat has shifted from merely 'infecting the product' to systematically 'compromising the process'."*

In other words, this is a more strategic, long-term compromise that places a significant burden on election officials during the procurement process. They can no longer trust a vendor's certification; they also need to scrutinize the vendor's secure-by-design development practices. Consequently, a critical vulnerability may not reside in the election-specific code but in the third-party library it depends on, which makes detection and remediation far more challenging.



4.3. CYBERATTACKS TARGETING CAMPAIGNS, PARTIES AND ELECTION OFFICIALS

Political campaigns, parties and officials are prime targets for cyberattacks aimed at influencing elections.[163] The most impactful tactic is the "hack-and-leak" operation, where stolen materials, such as emails and documents, are strategically released online to fuel disinformation and cause maximum political damage.[164] This playbook has been used repeatedly, from Russia's operations in the 2016 US and 2017 French elections to a 2024 breach of a US presidential campaign by hackers linked to Iran. These attacks are often initiated through spear-phishing, which involves highly tailored emails designed to trick individuals into divulging their credentials.[165]

An emerging threat is AI-powered voice cloning, also known as "vishing", in which an adversary uses AI to impersonate a trusted individual's voice over the phone – a tactic CISA warns could be used to impersonate senior election officials.[166]

Election officials also face a barrage of threats, including phishing and doxing (the malicious publication of personal information), from both foreign and domestic actors seeking to intimidate them or steal credentials.[167] These tools have been disproportionately weaponized against women in politics and journalism through harassment and the creation of non-consensual deepfake pornography.[168]

This development implies that campaigns, parties and officials should assume constant targeting across the election cycle and plan for credential theft and hack-and-leak attempts. Where intelligence points to an imminent leak, measured pre-emptive attribution can blunt impact. With AI boosting lure quality and enabling voice impersonation, government agencies should ban voice-only approvals and require call-back or second-channel verification. There is also a need to protect people and systems to provide legal and support pathways for women facing gendered deepfakes, and shield officials from doxing and harassment.[169]

4.4. WHAT CAN BE DONE? BEST PRACTICES FOR ELECTORAL CYBERSECURITY RESILIENCE

An effective defence against modern cyber and information threats requires a continuous, adaptive and collaborative approach.[170] A broad consensus has emerged around a set of best practices that constitute the core of electoral cybersecurity resilience.[171] Taken together, these layers translate technical resilience into electoral legitimacy. Governance and secure-by-design principles reduce error rates and eliminate single points of failure; proactive operations and rehearsed response minimize attacker dwell time and the visibility of disruption, closing information vacuums; and year-round partnerships enable credible, multi-agency communication and independent verification.

The result is continuity of service – ensuring that people can vote – combined with evidence of integrity, meaning that results are auditable, with a trusted explination provided, ensuring that the public understands what happened and why. These three conditions sustain both the perceived and the actual legitimacy of elections.

Foundational Governance and Technology

Resilience begins with a comprehensive risk assessment of the entire electoral ecosystem, from voter registration to results reporting.[172] Building on this foundation, electoral authorities should adopt technology that is secure by design, requiring vendors to embed security throughout the software development lifecycle.[173] In practice, this increasingly involves implementing a Zero Trust architecture, which removes implicit trust and continuously verifies every user, device and workload connected to critical systems.[174] These baseline choices reduce single points of failure and make subsequent controls more effective.

Proactive Operations and Response

Defensive posture must be proactive. This means continuously hardening systems through technical controls, such as multi-factor authentication and network segmentation, monitoring for threats via intrusion detection, and actively hunting for pre-positioned malware well before an election.[175] Equally important is having well-rehearsed incident response plans that integrate technical containment with strategic communication, preventing operational issues from escalating into legitimacy crises.[176] This operational discipline converts technical resilience into public confidence.

Sustained Partnerships

Ultimately, an effective defence is impossible in isolation. Resilience depends on year-round partnerships and the establishment of robust election cooperation networks. These structures formalize collaboration among Election Management Bodies (EMBs), cybersecurity agencies, intelligence services and law enforcement, creating the shared awareness required for a rapid, coordinated response to emerging threats.[177] By linking governance, operations and partnerships, authorities can detect earlier, respond faster and communicate more credibly – thereby strengthening both the perceived and the actual legitimacy of elections.

05 Countering Hybrid Threats to Elections: The Case for Establishing Election Cooperation Networks

The multi-domain and multi-stakeholder character of hybrid threats renders traditional, isolated security measures insufficient. Adversaries deliberately exploit overlaps in agency responsibilities – for example, during elections – by attacking cyber infrastructure, the information environment and physical security simultaneously. An EMB may be prepared for logistical challenges, a cybersecurity agency for network intrusions, and a law enforcement agency for physical security threats, but none is individually equipped to handle a synchronized attack that combines all three.[178] Malign actors understand these institutional divisions and design their operations to exploit them, creating a strategic challenge that can only be met with an equally integrated and networked defence.[179] Effective defence, therefore, requires a fundamental shift towards establishing robust, permanent election cooperation networks at both the national and international levels.[180]

These networks are essential for institutionalizing collaboration, moving beyond ad hoc crisis management to build a proactive, resilient defensive posture. The main goal of these networks is to develop a common operational picture among all key actors, facilitating quick, coordinated detection and response to emerging threats. The comprehensive framework for countering hybrid threats to elections, developed by the European Centre of Excellence for Countering Hybrid Threats, identifies key functions these networks should focus on, including updating legislation, conducting vulnerability assessments, boosting resilience, improving communication, conducting joint exercises, and strengthening detection and response capabilities.[181]

This proactive networked approach aligns with formal guidance at the European level. The European Commission has explicitly recommended that EU member states establish national election cooperation networks, recognizing them as vital platforms for electoral authorities to collaborate with other key security entities. Such cooperation, the Commission notes, is essential for the prompt detection of threats and the effective enforcement of rules.[182]

A crucial lesson from recent election protection efforts is that cooperation cannot be improvised during a crisis. The relationships, trust and protocols for information sharing must be established and exercised well in advance, as ad hoc efforts assembled under pressure are often ineffective. Therefore, institutionalizing permanent, formal cooperation networks is not merely a best practice but a fundamental prerequisite for building the resilience needed to withstand the chronic pressure of modern hybrid threats.[183]

5.1. ARCHITECTURES OF NATIONAL COLLABORATION

While the principle of cooperative defence is widely accepted, there is no "one-size-fits-all" model for an election cooperation network. National structures are shaped by a country's unique governance and its perceptions of the threats it faces. The examples below summarize each model's core mechanics and scope.

- **Sweden's** decentralized government and consensus-driven culture produce a multi-level network based on a collaboration model. At the national level, the Swedish Election Authority chairs a national election cooperation network, complemented by regional and local networks.[184] Practical features include standing information-sharing groups, routine joint exercises, and clear role delineation between national guidance and municipal execution.

- **The United States'** highly federalized structure necessitates a decentralized model in which federal agencies coordinate with 50 independently run state election systems. Coordination is achieved through voluntary frameworks – such as the Election Infrastructure Information Sharing and Analysis Center, shared playbooks and incident-response support – rather than central direction.[185]

- **France's** statist tradition has given rise to a dedicated state body with the authority to publicly identify foreign interference. This body, Viginum (*Service de vigilance et de protection contre les ingérences numériques étrangères*), embodies a centralized model that prioritizes investigative authority, rapid public advisories, and whole-of-state tasking to operational departments.[186]

- **Canada** has developed an intelligence-led model that is carefully firewalled from the immediate political sphere.[187] This model centres on the Security and Intelligence Threats to Elections Task Force, which conducts integrated threat assessment, and the Critical Election Incident Public Protocol Panel, which manages threshold-based public communication. Elections Canada is not a member of either the Task Force or the Protocol Panel; it remains independent but coordinates with security agencies and receives briefings.[188]

These examples show that, while the core functions of cooperation are universal, the institutional form must be tailored to the national context. Beyond their specific structures, effective election cooperation networks share a set of core operational functions and best practices that are essential for success. These practices shift a country's defensive posture from reactive, event-driven to proactive and continuous. An analysis of the various national models reveals a standard playbook for what these networks must do to be effective.

Establishing a Common Operating Picture: The Fusion Cell Concept

A foundational practice for effective cooperation is establishing a "fusion cell". This concept involves co-locating analysts and liaison officers from all participating agencies, either in person or virtually, to enable real-time information exchange and foster a shared understanding of the threat environment.[189] By breaking down information silos, fusion cells composed of diverse experts – from cyber responders to intelligence analysts and strategic communicators – can synthesize multiple threat streams into a single, coherent "common operating picture".

To balance analytical integration with institutional autonomy, fusion cells should operate on an "analyse together, act within mandate" basis: analysis is shared, while operational decisions and authorities remain within each institution. This shared awareness is the bedrock of coordinated response and can be designed to respect the EMB's operational independence.[190]

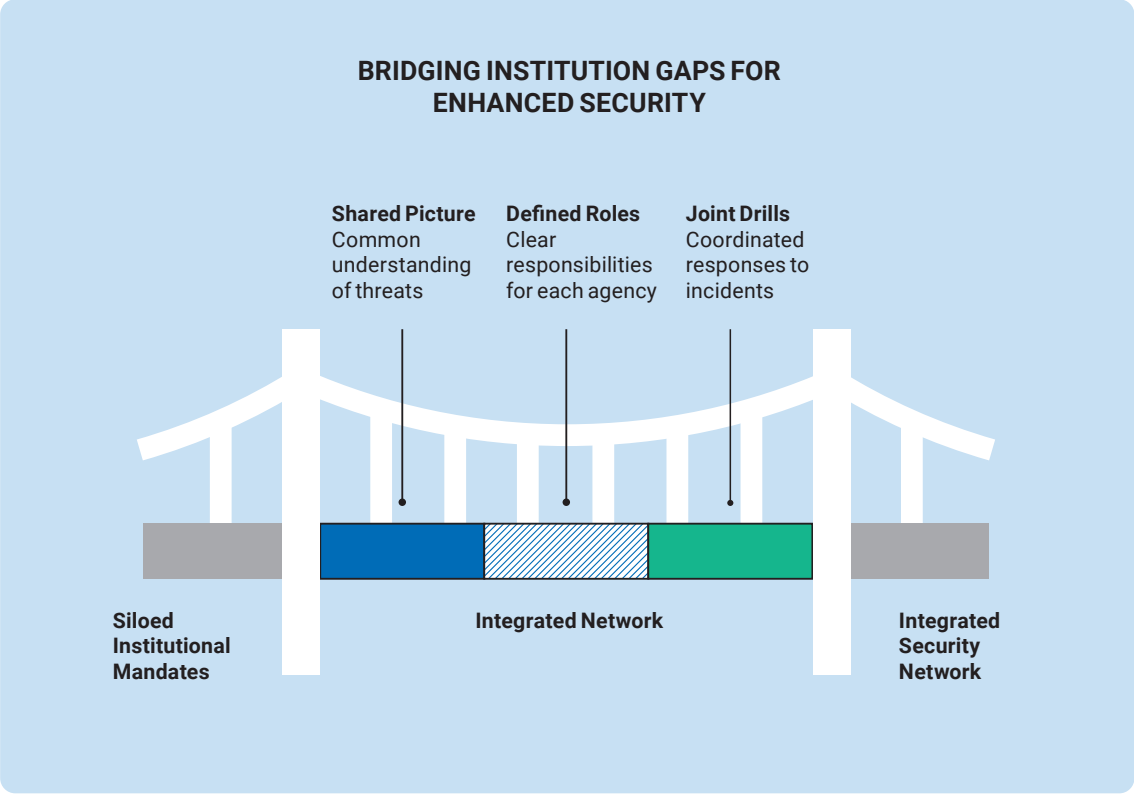
In practice, the balance is maintained through purpose-limited data sharing and role-based access, formal memorandums of understanding, strict separation between analysis and operations, and auditable sharing logs. The solution lies in design, not distance: fusion cells should remain strictly analytical, with purpose-limited information exchange that keeps operational decisions within each institution's remit, ensuring that the EMB retains sole authority over electoral processes.

When implemented in this way, fusion cells deliver tangible outcomes, including faster threat detection and triage ("time-to-detect"), reduced duplication of effort across agencies, and stronger trust and message coherence in joint responses.

Proactive, Continuous Work Between Election Cycles

Effective networks operate continuously, not just in the months leading up to a vote. Key proactive activities include:

- **Joint Risk and Vulnerability Assessments:** Regularly and systematically mapping the electoral ecosystem to identify and prioritize risks before they can be exploited.[191]
- **Scenario-Based Planning and Joint Exercises:** Regularly conducting tabletop and functional exercises to test response plans, identify coordination gaps and build institutional "muscle memory".[192] The EU's joint cybersecurity exercises before parliamentary elections are a key example.[193]
- **Formalized Protocols for Information Sharing and Response:** Establishing clear, pre-agreed protocols that govern how threats are reported, assessed and acted upon. This avoids improvisation during a crisis and helps depoliticize decision-making.[194]



5.2. NETWORK OF NETWORKS

In a globalized information environment, purely national defences are insufficient, requiring a "network of networks" that connects national bodies to robust international frameworks.

The EU has the most sophisticated regional ecosystem. Its European Cooperation Network on Elections serves as a central hub for national authorities to exchange best practices on everything from cybersecurity to countering disinformation.[195] This is connected to specialized networks, such as the Rapid Alert System for FIMI threats, and is supported by a Joint Mechanism for Electoral Resilience that can deploy expert teams to member states. This integrated system was seen as essential in ensuring the smooth conduct of the 2024 European Parliament elections.[196]

Broader cooperation extends through the North Atlantic Treaty Organization (NATO), which identifies hybrid threats as a core security challenge and works to improve intelligence sharing among Allies, and the G7 Rapid Response Mechanism, which coordinates responses to foreign state-sponsored disinformation.[197] At the global level, intergovernmental organizations like the International Institute for Democracy and Electoral Assistance play a key role in building norms and fostering a community of practice through initiatives like the Global Network for Securing Electoral Integrity.[198]

5.3. CHALLENGES TO EFFECTIVE COOPERATION

Despite the significant progress made in establishing cooperative defence mechanisms, their long-term effectiveness and viability face profound and persistent challenges. In practice, these include political turnover and polarization, funding cliffs, legal uncertainty, and the everyday frictions of data-sharing and coordination.

A key hybrid-threat sustainability paradox is that the very mechanisms built to counter coordinated information, cyber and financing pressures can themselves become targets – vulnerable to FIMI-driven delegitimization, polarization, and legal or budgetary attacks by the same actors they are designed to resist. Put simply, the guardrails we build can be weakened by the very forces they are meant to contain.

These obstacles – spanning the political, financial and operational realms – threaten to erode the very structures created to protect democratic processes. Addressing them is essential for building sustainable, rather than episodic, resilience.

> *"The path to sustainable resilience requires not only the creation of these networks, but also a broader societal effort to depoliticize election security and embed it as a core, non-negotiable national interest."*

Long-term durability, therefore, depends on practical institutional insulation – clear mandates, cross-party backing and protected budgets – combined with broad-based political support that outlasts any single government. The path to sustainable resilience requires not only the creation of these networks, but also a broader societal effort to depoliticize election security and embed it as a core, non-negotiable national interest. It should be anchored in a shared social contract and public trust, and operationalized through a whole-of-society approach.

06 Conclusions and Recommendations

The period from 2024 to the present has confirmed that hybrid threats represent a persistent, adaptive and increasingly sophisticated challenge to electoral integrity worldwide. Analysis of recent cases of hybrid attacks targeting elections underscores the evolution of these threats – from episodic interference to a chronic, systemic form of conflict that now operates as a full-spectrum campaign. These campaigns synchronize FIMI, cyber operations, illicit political finance, lawfare and offline pressure, coordinated across state, proxy and criminal actors, and timed to exploit institutional seams throughout the electoral cycle.

The analysis of recent events underscores several key findings:

- **A shift to chronic conflict:** Electoral interference has moved from occasional incidents to a continuous information conflict. Malicious state actors persistently work to undermine democratic systems by eroding public trust, fuelling polarization and weakening institutions.[199]

- **Industrial-scale operations and new technologies:** Adversaries now operate at an industrial scale, leveraging sophisticated, centrally controlled propaganda networks.[200] The weaponization of AI has become a significant force multiplier, enabling the low-cost, rapid creation of synthetic media and hyper-realistic disinformation, dramatically increasing both the volume and quality of threats.[201]

- **Integration of threat vectors:** Successful hybrid operations rarely rely on a single method. Instead, they integrate information manipulation, illicit political finance and disruptive cyberattacks into cohesive campaigns. Illicit funds – often channelled through cryptocurrencies and third parties – support information influence activities and vote-buying. At the same time, cyberattacks are used to steal data for "hack-and-leak" operations and to disrupt electoral processes, sowing confusion and distrust.[202]

- **Detection, attribution and accountability remain bottlenecks:** The use of proxies, information laundering and fragmented data access hinders timely and proportionate responses. Meanwhile, inconsistent platform transparency limits external oversight. Progress on open standards for provenance and researcher data access should be paired with auditable ad-tech controls and effective sanctions screening.[203]

6.1. RECOMMENDATIONS

These findings underscore the need to build and strengthen networked defence. Because adversaries deliberately exploit the seams between institutional mandates, traditional siloed security responses are no longer sufficient.

The following recommendations are directed to stakeholders responsible for safeguarding democratic processes. They are organized around four core actions aimed at fostering sustainable national and international resilience.

1. **Building internal agency capacity:** Individual institutions must take ownership of their own defence, supported by clear mandates and professionalized routines.

This begins with explicitly assigned responsibilities for risk mapping, incident command, public communication and supplier management, all documented in practical, usable plans. These plans should be embedded into daily practice through regular drills simulating hybrid threat scenarios, including a rehearsed leak-response playbook with pre-approved messaging and post-exercise remediation efforts tracked to completion.

Technology and procedures should follow secure-by-design principles – such as least-privilege access, continuous verification of users and devices, and offline backups for critical operations – to ensure continuity under stress. Procurement standards should require evidence of secure development practices, prompt incident reporting, and transparency on third-party components to avoid single points of failure.

Indicators of progress include faster detection and containment, timely and transparent public updates, and comprehensive audit trails that clarify incidents without disclosing sensitive information.

2. **Fostering a national support ecosystem:** Internal capacity must be reinforced by a robust, whole-of-government network, as no single agency can succeed in isolation.

A standing cooperation network should operate year-round, linking the election authority with technical, regulatory, security and oversight partners. A lightweight fusion-cell model enables real-time information sharing ("analyse together, act within mandate"), ensuring that all parties maintain a common understanding while preserving operational independence. Shared services may include an assistance line for local authorities and smaller organizations, rapid escalation channels to major online platforms, and a verification mechanism for suspicious audio or video to help journalists and the public access authoritative sources.

Lawful and proportionate cooperation should be guaranteed through written protocols, role-based access and transparent records of shared information. Such networks enable earlier cross-agency warnings, reduce duplication of effort, and promote more consistent public messaging when it matters most.

3. **A whole-of-society approach:** Democratic resilience depends on engaging independent media, civil society, academia, local authorities, the private sector and communities to enhance literacy, verification and inclusive public communication – implemented in ways that uphold rights, transparency and pluralism.

Transparency should become standard practice through dedicated, easily accessible web pages for each key process. The use of pre-emptive messaging should be limited and aligned with the election cycle, focusing on clear cues – what to expect, how to verify and where to report – and consistently directing audiences to official sources.

Trusted local outlets and organizations can help extend reach by providing ready-made explanations suitable for republication. Support for independent media and investigative journalism should be expanded but kept at arm's length to safeguard editorial independence, complemented by clear pathways to address harassment, doxing and gender-based abuse. Collaboration with private providers should ensure secure verification for sensitive requests, rapid response if harmful content spreads, and greater transparency around political advertising.

Ultimately, this approach fosters a more informed and engaged public, faster correction of rumours, and wider reuse of reliable information.

4. **Building international cooperation and support mechanisms:** National systems should integrate with cross-border assistance, shared standards and joint actions, enabling support to scale when attacks surpass domestic capacity.

Mutual-aid arrangements should be prepared in advance, covering technical response, forensic support, and public communication during election periods. Practical channels for cross-border takedowns or related actions should be established with pre-approved templates to minimize delays. Standard baselines for protecting election-relevant systems and for disclosing incidents should be aligned, and basic provenance practices for official media should be adopted where feasible to streamline verification and increase transparency.

Knowledge should be transferred ahead of primary cycles through exchanges and secondments, while cooperation networks should "peer" with counterparts abroad to share indicators and playbooks. The results are faster assistance when it matters most, clearer updates across jurisdictions, and stronger evidence when accountability is at stake – transforming resilience into legitimacy both domestically and with international partners.

All countermeasures must be lawful, necessary and proportionate, and grounded in a human rights-based approach. In practice, this means targeting manipulative behaviours rather than lawful speech, and prioritizing process remedies – transparency, provenance and accountability – over content removal. It also entails implementing data minimization and privacy-by-design; employing time-bound, purpose-limited actions with independent oversight, audit trails and avenues for redress; and maintaining proactive transparency through a canonical source of truth that allows the public to verify claims.

These safeguards align with access-to-information guarantees (e.g., the Tromsø Convention), freedom-of-expression standards (e.g., the International Covenant on Civil and Political Rights, General Comment No. 34), and rights-respecting platform governance (e.g., the DSA). At the same time, media pluralism and editorial independence provide a counterbalance to overreach – ensuring that defensive measures protect the very democratic values that hybrid threats to elections seek to erode.

For governments and legislators

1. **Establish and sustain a national election cooperation network:** Make this a national security priority by creating a formal, permanent body that brings together the election management body, cybersecurity agencies, intelligence services, law enforcement and strategic communications units. This network should operate continuously to conduct joint risk assessments, run simulation exercises and develop shared response protocols.

2. **Strengthen legislative and regulatory frameworks:**

    - **Illicit political finance:** Where not already in place, prohibit anonymous and foreign donations to political actors. Update regulations to address the use of cryptocurrencies, increase transparency in online advertising, and require that political donations over a certain amount pass through the formal banking system to enhance traceability and oversight.

    - **Platform accountability:** Implement and enforce robust regulatory frameworks for social media platforms, with a focus on transparency in algorithmic content curation, political advertising, and data access for vetted researchers.

    - **Electoral and criminal codes:** Conduct a comprehensive review of the electoral legal framework to identify and close loopholes vulnerable to hybrid threats. Modernize the criminal code to explicitly define and penalize offences targeting the electoral process – such as coordinated disinformation campaigns and cyberattacks on infrastructure – to ensure effective prosecution.

3. **Invest in a whole-of-society resilience strategy:** Fund and support national initiatives that enhance public resilience through a two-pronged approach. First, empower citizens and civil society by investing in long-term media and AI literacy campaigns, and by providing sustained support for a diverse and independent media sector. A critical component of this is dedicated funding for investigative journalism, which is essential for exposing the mechanics of hybrid threats. Second, these societal efforts should be complemented by the government's own commitment to proactive communication, operationalized through the pre-bunking of likely narratives and the establishment of official source-of-truth hubs to anchor public information and help inoculate citizens against manipulation.

4. **Provide shared technical infrastructure and services:** Establish and fund a centralized capability to deliver shared cybersecurity and secure communication services for key democratic institutions. This should include essential protections – such as Distributed Denial-of-Service (DDoS) mitigation – for the websites of election management bodies and other high-value targets, ensuring that they remain accessible to the public, particularly during crises.

For EMBs

5. **Adopt a continuous cybersecurity posture:** Treat electoral security as a year-round process. Implement a proactive defence model that includes deploying foundational technical controls – such as phishing-resistant multi-factor authentication for all critical accounts – adopting a Zero Trust architecture, and requiring secure-by-design principles in all technology procurement.

6. **Develop and rehearse integrated response plans:** Create and regularly update incident response plans that combine technical containment with strategic communication. Agencies must be ready to communicate clearly and transparently with the public during a cyber or information incident to prevent disinformation and maintain trust.

    An essential first step in developing such plans is to establish transparent internal governance by appointing a senior leader with the mandate and authority to convene legal, IT and commu-

nications staff, and to assume ultimate responsibility for managing the response during an incident. These plans must also prepare the agency for hostile information releases. This includes developing a declassification playbook that sets out clear legal protocols for minimal-harm disclosure of information under the time pressure of a hack-and-leak operation, ensuring the agency can respond in a controlled, legally compliant manner.

7. **Actively participate in cooperation networks:** Be an engaged and consistent partner within the national election cooperation network. Use this forum to share and receive threat intelligence, build awareness of the wider risk landscape, and coordinate defensive actions with security and intelligence agencies.

For international support actors

8. **Foster a "network of networks":** Prioritize the strengthening of international cooperation frameworks, such as EU–NATO collaboration and the G7 Rapid Response Mechanism. Facilitate the exchange of best practices and threat intelligence between national cooperation networks to build a global community of practice for democratic defence.

9. **Provide tailored technical and strategic support:** Offer targeted assistance to partner countries to help them establish their own national cooperation networks. Support should be adapted to the national context and focus on practical implementation, including facilitating joint simulation exercises and providing expertise on specialized areas such as cybersecurity and countering FIMI.

10. **Adopt a modular funding approach:** To ensure support is practical and results-oriented, donors should consider funding specific, high-impact capability modules. Strategic investments in shared services can generate crucial economies of scale. Key modules could include:

    - A National Election Cooperation Network Secretariat to manage coordination.
    - A Core Cybersecurity Stack to provide shared services such as DDoS protection for the websites of the election authority and other critical agencies.
    - Agency-Level Capacity Packages to fund the creation of source-of-truth hubs and incident-response playbooks within key institutions.
    - Host-Nation Readiness for International Support to prepare the legal, organizational and technical groundwork – such as a designated national point of contact and pre-approved legal templates – for receiving expert assistance during a crisis.
    - Specialized International Surge Teams to provide deployable, niche expertise for managing complex hybrid-threat tactics, such as dedicated teams responding to cyberattacks and hack-and-leak operations, or offering strategic-communication support. Support should be practical, demand-driven and focused on genuine collaboration.

Ultimately, however, long-term success lies in preventing threats from materializing in the first place. This can only be achieved through operational excellence: running electoral processes flawlessly, communicating with radical transparency, and acknowledging errors with honesty. It is this steady work of building durable institutional capacity and hard-won public trust that forms the strongest defence against those who seek to undermine the democratic process.

07 References

Agrawal, H., Hamada, Y., & Fernández Gibaja, A. (2021). *Regulating Online Campaign Finance: Chasing the Ghost?* International IDEA. https://www.idea.int/publications/catalogue/regulating-online-campaign-finance

Alihodžić, S. (2023). *Protecting elections: Risk management, resilience-building and crisis management in elections.* International IDEA. https://www.idea.int/publications/catalogue/protecting-elections-risk-management-resilience-building-and-crisis

Alliance for Securing Democracy. (2019). Russian hackers behind surge in cyberattacks targeting Ukrainian election. https://securingdemocracy.gmfus.org/incident/russian-hackers-behind-surge-in-cyberattacks-targeting-ukrainian-election/

Anghel, V. (2024). Why Romania just canceled its presidential election. *Journal of Democracy* (online exclusive). https://www.journalofdemocracy.org/online-exclusive/why-romania-just-canceled-its-presidential-election/

Antoniuk, D. (2023, January 7). Moldova's government hit by flood of phishing attacks. *The Record*. https://therecord.media/moldovas-government-hit-by-flood-of-phishing-attacks

Antoniuk, D. (2024, October 21). 'Unprecedented' interference targets Moldova's elections. *The Record / Recorded Future News*. https://therecord.media/unprecedented-interference-moldova-elections-cyberattack

Antoniuk, D. (2025, September 22). Russia steps up disinformation efforts to sway Moldova's parliamentary vote. *The Record*. https://therecord.media/russia-steps-disinfo-moldova-election

Atlantic Council. (2018, September 11). Defining Russian election interference: An analysis of select 2014–2018 cyber-enabled incidents. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/

Atlantic Council. (2023, February 24). *Narrative warfare: How the Kremlin and Russian news outlets justified a war of aggression against Ukraine*. https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf

Atlantic Council / DFRLab. (2024, November 4). Trends in China's US election interference illustrate its longer game. https://dfrlab.org/2024/11/04/china-us-election-interference/

Bakken, M. (2025, February 3). Election observation and hybrid threats. *European Democracy Hub*. https://europeandemocracyhub.epd.eu/election-observation-and-hybrid-threats/

Balmforth, T., & Dysa, Y. (2024, November 2). Moldova says Russia plans to disrupt expatriate voting in Sunday's runoff. *Reuters*. https://www.reuters.com/world/europe/moldova-claims-russia-plans-disrupt-expatriate-voting-sundays-runoff-2024-11-02/

Barata, J., & Lăzăr, E. (2025, January 27). Will the DSA save democracy? The test of the recent presidential election in Romania. *Tech Policy Press*. https://techpolicy.press/will-the-dsa-save-democracy-the-test-of-the-recent-presidential-election-in-romania

Bateman, J., & Jackson, D. (2024). *Countering disinformation effectively: An evidence-based policy guide*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en

Bay, S. (2024). *Countering hybrid threats to elections: From updating legislation to establishing collaboration networks* (Hybrid CoE Research Report 12). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/

Bay, S. (2025). *Protecting electoral integrity: The case of Sweden*. International IDEA. https://www.idea.int/publications/catalogue/protecting-electoral-integrity-case-sweden

Bay, S., Appelgren, J., Isaksson, E., Lindgren, J., & Thunholm, P. (2022). *Threats to Swedish public elections – Examples and scenarios for the Election Administration* (FOI-R--5298--SE). FOI. https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--5298--SE

Bing, C., & Vicens, A. J. (2024, October 23). Iranian hacker group aims at US election websites and media before vote, Microsoft says. *Reuters*. https://www.reuters.com/technology/cybersecurity/iranian-hacker-group-focuses-us-election-websites-media-ahead-vote-microsoft-2024-10-23/

Bjola, C. (2025, February 7). Algorithmic invasions: How information warfare threatens NATO's eastern flank. *NATO Review*. https://archives.nato.int/nato-review-algorithmic-invasions-how-information-warfare-threatens-natos-eastern-flank

Brennan Center for Justice. (2020, October). *2020's lessons for election security*. https://www.brennancenter.org/our-work/research-reports/2020s-lessons-election-security

Bryjka, F. (2024). Russian interference nearly overwhelmed Moldovan presidential election–referendum vote. *Polish Institute of International Affairs* (PISM). https://pism.pl/publications/russian-interference-nearly-overwhelmed-moldovan-presidential-election-referendum-vote

C2PA. (2024). Content credentials & C2PA overview. https://c2pa.org

Canada (Government of Canada). (2025, July 8). *Multi-stakeholder insights: A compendium on countering election interference*. https://www.canada.ca/en/democratic-institutions/services/paris-call-trust-security-cyberspace/multistakeholder-insights-compendium-countering-election-interference.html

The Carter Center. (2025, July 8). Democracy program. https://www.cartercenter.org/peace/democracy

Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory. (2021). *The long fuse: Misinformation and the 2020 election*. Election Integrity Partnership. https://purl.stanford.edu/tr171zs0069

Center for Internet Security. (2025a, July 8). EI ISAC. https://www.cisecurity.org/ei-isac

Center for Internet Security. (2025b, July 8). The IT lifecycle – The CIS guide to election technology procurements. https://election-procurement.docs.cisecurity.org/en/latest/IT_product_services_lifecycle.html

Center for Internet Security. (2025c). Election security spotlight – DDoS attacks. https://www.cisecurity.org/insights/spotlight/election-security-spotlight-ddos-attacks

Cerulus, L. (2025, June). EU comes to Moldova's defense against Russian hacking. POLITICO. https://www.politico.eu/article/eu-moldova-election-cyber-security-russia-hacking/

Chainalysis. (2024a). *2024 cryptocurrency adoption index*. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index

Chainalysis. (2024b). Malign Interference and Crypto: How Crypto Transaction Tracing Can Expose and Disrupt Malign Influence Efforts. https://www.chainalysis.com/blog/malign-interference-and-crypto/

Chan, K. (2024, December 17). EU investigates TikTok over Romanian presidential election safeguards. *AP News*. https://apnews.com/article/0638e90cb3898fc61619e8aed4731a53

Chan, K. (2025, July 25). Meta will cease political ads in European Union by fall, blaming bloc's new rules. *AP News*. https://apnews.com/article/meta-instagram-facebook-eu-european-union-political-89efeac96723308d2a0469740d24d433

CISA (Cybersecurity and Infrastructure Security Agency). (2024a, January 18). Risk in focus: Generative A.I. and the 2024 election cycle. https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle

CISA. (2024b). #Protect2024: Election security. https://www.cisa.gov/topics/election-security/protect2024

CISA. (2025, July 8). Join the Elections Infrastructure Information Sharing and Analysis Center (EI ISAC). https://www.cisa.gov/resources-tools/groups/join-elections-infrastructure-information-sharing-and-analysis-center-ei-isac

CISA, & EAC. (2024a). *Election infrastructure incident response communications guide*. https://www.eac.gov/sites/default/files/2024-10/Election_Infrastructure_Incident_Response_Comms_Guide_508.pdf

CISA, & EAC. (2024b). *Enhancing election security through public communications*. https://www.eac.gov/sites/default/files/2024-06/Enhancing_Election_Security_Through_Public_Communications.pdf

Cisco (Outshift). (2025, July 8). Top 15 software supply chain attacks: Case studies. https://outshift.cisco.com/blog/top-10-supply-chain-attacks

Clayton, M. (2014, June 17). Ukraine election narrowly avoided 'wanton destruction' from hackers. *The Christian Science Monitor*. https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

Cloudflare. (2025, July 8). Exploring Internet traffic shifts and cyber attacks during the 2024 US election. https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/

CNN. (2024a, April 26). Cyberattack forces Georgia county to sever connection to state voter registration system. https://edition.cnn.com/2024/04/26/politics/georgia-coffee-county-cyberattack-voter-system/index.html

CNN. (2024b, August 19). US concludes Iran is behind hacking attempts targeting Trump and Biden Harris campaigns. https://edition.cnn.com/2024/08/19/politics/us-concludes-iran-behind-trump-biden-harris-hacking/index.html

Coherent Market Insights. (2025, March 17). Crypto exchange market size and forecast, 2025–2032. https://www.coherentmarketinsights.com/industry-reports/crypto-exchange-market

CoinGecko. (2025). Cryptocurrency prices, charts and market capitalizations. https://www.coingecko.com

Columbia University, SIPA IGP. (2025, July 8). French official outlines government approach to countering foreign online operations. https://igp.sipa.columbia.edu/news/french-official-outlines-government-approach-countering-foreign-online-operations

Communications Security Establishment Canada. (2025, March). CSE releases 2025 update to report on cyber threats to Canada's democratic process. https://www.canada.ca/en/communications-security/news/2025/03/communications-security-establishment-canada-releases-2025-update-to-report-on-cyber-threats-to-canadas-democratic-process.html

Constella Intelligence. (2025, July 8). Voter database leaks threaten the 2024 U.S. election. https://constella.ai/2024-u-s-election-voter-database-leaks/

Council of Europe. (2024). Internet voting in post-war elections in Ukraine: risks and challenges – results of the study presented. https://www.coe.int/en/web/kyiv/-/internet-voting-in-post-war-elections-in-ukraine-risks-and-challenges-results-of-the-study-presented

Council of Europe. (2025, July 8). Foreign interference in electoral processes at local and regional levels. https://rm.coe.int/0900001680b4cb53

County of San Luis Obispo, Clerk Recorder. (2024, August 1). Federal agencies say cyber attack could hinder public access to election information, not election itself. https://www.slocounty.ca.gov/departments/clerk-recorder/news-announcements/federal-agencies-say-cyber-attacks-could-hinder-public-access-to-election-information-but-not-to-ele

CrowdStrike. (2025a). Zero Trust Security Explained: Principles of the Zero Trust Model. https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security

CrowdStrike. (2025b). Press release: CrowdStrike releases 2025 threat hunting report. https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-threat-hunting-report/

Csernatoni, R. (2024). Can democracy survive the disruptive power of AI? *Carnegie Endowment*. https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai

Cyble. (2024). EU cybersecurity in 2024: Insights from ENISA's latest report. https://cyble.com/blog/eu-cybersecurity-in-2024-insights-from-enisa-latest-report

Cyble. (2025, July 8). Software supply chain attacks surged in April and May. https://cyble.com/blog/supply-chain-attacks-surge-in-april-may-2025

Deloitte. (2024). ENISA threat landscape 2024: Cyber threat landscape in the financial sector. https://www.deloitte.com/ro/en/our-thinking/articles/raportul-enisa-threat-landscape-2024-peisajul-amenintarilor-cibernetice-sectorul-financiar.html

Electoral Commission (UK). (2024). Electoral Commission response to cyber attack attribution. https://www.electoralcommission.org.uk/media-centre/electoral-commission-response-cyber-attack-attribution-0

Elections Canada. (2025, July 8). Our work with security agencies and partners – Media guide for the 45th general election. https://www.elections.ca/content.aspx?section=med&dir=guide&document=p19&lang=e

Electionline. (2024, October). *2024 election threat landscape*. https://electionline.org/wp-content/uploads/2024/10/2024-Election-Threat-Landscape-TLP-CLEAR.pdf

ENISA / NIS Cooperation Group. (2024). *Compendium on elections cybersecurity and resilience*. Press release: https://www.enisa.europa.eu/news/safeguarding-eu-elections-amidst-cybersecurity-challenges

Euromaidan Press. (2014). Russian hacking attempt fails, but fake election news airs. https://euromaidanpress.com/2014/05/26/russian-hacking-attempt-fails-but-fake-election-news-airs/

European Commission. (2016). *Joint framework on countering hybrid threats: A European Union response* (JOIN(2016) 18 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016JC0018

European Commission. (2024). Commission opens formal proceedings against TikTok under the DSA (IP/24/6487). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

European Commission. (2025a). Hybrid threats – Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

European Commission. (2025b). European cooperation network on elections. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en

European Commission. (2025c, June 12). Commission services and Moldovan authorities conduct a stress test on potential digital hybrid threats to election integrity ahead of Moldova's parliamentary elections. *Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en/news/commission-services-and-moldovan-authorities-conduct-stress-test-potential-digital-hybrid-threats

European Digital Media Observatory (EDMO). (2024). *Final report – Outputs and outcomes of a community-wide effort (EP elections)*. https://edmo.eu/publications/final-report-results-and-outcomes-of-a-community-wide-effort/

European External Action Service (EEAS). (2024). *Second EEAS report on Foreign Information Manipulation and Interference (FIMI) threats*. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

European External Action Service (EEAS). (2025a). *Third EEAS report on Foreign Information Manipulation and Interference (FIMI) threats*. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

European External Action Service (EEAS). (2025b). Information integrity and countering FIMI. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

European External Action Service (EEAS). (2025c). About the EU Partnership Mission in the Republic of Moldova (EUPM Moldova). https://www.eeas.europa.eu/eupm-moldova/about-eu-partnership-mission-republic-moldova_en

EUvsDisinfo. (2024a). *Doppelganger strikes back: Unveiling FIMI activities targeting European Parliament elections*. https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/

EUvsDisinfo. (2024b). Who is afraid of the European Moldova? https://euvsdisinfo.eu/who-is-afraid-of-the-european-moldova/

Europol. (2025, February 28). The DNA of organised crime is changing – and so is the threat to Europe. https://www.europol.europa.eu/media-press/newsroom/news/dna-of-organised-crime-changing-and-so-threat-to-europe

FBI. (2024, November 5). Statement on bomb threats to polling locations. https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations

Forbes. (2025, March 10). AI driven phishing and deepfakes: The future of digital fraud. https://www.forbes.com/councils/forbestechcouncil/2025/03/10/ai-driven-phishing-and-deep-fakes-the-future-of-digital-fraud/

Freedom House. (2024). *Freedom in the world 2024: The mounting damage of flawed elections and armed conflict*. https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict

GAO (US Government Accountability Office). (2020, February). Election security: *DHS plans are urgently needed…* https://www.gao.gov/assets/gao-20-267.pdf

Gavin, W. (2025, September 23). Moldova arrests 74 in plot to disrupt election. How Russian-funded fake news network aims to disrupt election in Europe - BBC investigation. *BBC News*. https://www.bbc.com/news/articles/c4g5kl0n5d2o

Gilbert, D. (2024, April 11). Election workers are already burned out—and on high alert. *WIRED*. https://www.wired.com/story/election-officials-threats-disinformation/

Global Witness. (2024, December 6). TikTok pushes far right candidate content in Romanian election, investigation shows. https://www.globalwitness.org/en/press-releases/tiktok-pushes-far-right-candidate-content-romanian-election-global-witness-investigation-shows/

Global Witness. (2025, May 15). Ahead of the second round, TikTok continues to push far right content in Romania. https://globalwitness.org/en/campaigns/digital-threats/tiktok-algorithm-continues-to-push-multiple-times-more-far-right-content-to-users-ahead-of-romanian-election

Google Cloud. (2023, August). *Poll Vaulting: Cyber Threats to Global Elections*. https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections

Google DeepMind. (2025). SynthID – A tool to watermark and identify content generated through AI. https://deepmind.google/science/synthid/

Hedenskog, J., & Hjelm, M. (2020, October 25). Propaganda by Proxy: Ukrainian oligarchs, TV and Russia's influence (FOI Memo 7312). FOI. https://www.foi.se/rest-api/report/FOI%20Memo%207312

Hedling, E. (2025, April 15). *Social identities and democratic vulnerabilities: Learning from examples of targeted disinformation* (Hybrid CoE Paper 24). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2025/04/20250415-Hybrid_CoE_Paper-24-WEB.pdf

Hoffman, F. G. (2022). *Towards a fifth wave of deterrence theory and practice* (Hybrid CoE Paper 12). Hybrid CoE.https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/

Hollis, D. B., & Ohlin, J. D. (2021). *Defending democracies: Combating foreign election interference in a digital age.* Oxford University Press. https://global.oup.com/academic/product/defending-democracies-9780197556979

Hoogensen Gjørv, G., & Jalonen, O. (2023). *Identity as a tool for disinformation* (Hybrid CoE Strategic Analysis 34). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-34-identity-as-a-tool-for-disinformation-exploiting-social-divisions-in-modern-societies/

Hoxhunt. (2025, July 8). AI powered phishing outperforms elite cybercriminals in 2025. https://hoxhunt.com/blog/ai-powered-phishing-vs-humans

Huo, J. (2024, November 12). Foreign influence efforts reached a fever pitch during the 2024 elections. *NPR*. https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iran

Hybrid CoE. (2024, January). *Frequently asked questions on hybrid threats*. https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf

Hybrid CoE. (2025). Hybrid threats. https://www.hybridcoe.fi/hybrid-threats/

International Foundation for Electoral Systems (IFES). (2024, December 20). The Romanian 2024 election annulment: Addressing emerging threats to electoral integrity. https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity

IGP (Inspectoratul General al Poliției). (2025, September 22). Trust Media responsabil de propaganda pro-rusă și dezinformare, finanțat printr o schemă complexă de spălare de bani, vizat în percheziţiile de astăzi. *Poliția Republicii Moldova*. https://www.igp.gov.md/ro/politia-actiune/trust-media-responsabil-de-propaganda-pro-rusa-si-dezinformare-finantat-printr-o

IGP (Inspectoratul General al Poliției). (2025, August 13). Autoritățile intensifică acțiunile împotriva dezinformării în spațiul digital: peste 400 de canale TikTok vizate pentru blocare. *Poliția Republicii Moldova*. https://politia.md/ro/noutati/autoritatile-intensifica-actiunile-impotriva-dezinformarii-spatiul-digital-peste-400-de

International IDEA. (2019). Inter-agency Collaboration on Cybersecurity in Elections: Roundtable Discussion. https://www.idea.int/news/inter-agency-collaboration-cybersecurity-elections-roundtable-discussion

International IDEA. (2023, November 28). Mauritius: Inter agency collaboration against hybrid threats. https://www.idea.int/news/mauritius-inter-agency-collaboration-against-hybrid-threats

International IDEA. (2024, September 17). The Global State of Democracy 2024: Strengthening the legitimacy of elections in a time of radical uncertainty. https://www.idea.int/publications/catalogue/global-state-democracy-2024-strengthening-legitimacy-elections

International IDEA. (2025). Political finance database. https://www.idea.int/data-tools/data/political-finance-database

ISACA. (2025, July 8). The 2025 software supply chain security report. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/the-2025-software-supply-chain-security-report

Ivanti. (2025, July 8). Software supply chain attacks risk on the rise. https://www.ivanti.com/blog/software-supply-chain-attack-risk

Kovalčíková, N., & Spatafora, G. (2024, December 17). The future of democracy: Lessons from the US fight against foreign electoral interference in 2024 (EUISS Brief). *EU Institute for Security Studies*. https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024

Kubica, L. (2024). *Moldova's struggle against Russia's hybrid threats* (Hybrid CoE Working Paper 28). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-countering-the-energy-leverage-to-becoming-more-sovereign-overall

Ledford, H. (2024). Deepfakes, trolls and cybertroopers: How social media could sway elections in 2024. *Nature*, 626(7902), 463–464. https://www.nature.com/articles/d41586-024-00274-7

Levin, D. H. (2020). *Meddling in the ballot box: The causes and effects of partisan electoral interventions.* Oxford University Press. https://academic.oup.com/book/36920

Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., & Zaragoza, M. S. (2020). *The Debunking Handbook 2020.* https://www.climatechangecommunication.org/wp-content/uploads/2020/10/DebunkingHandbook2020.pdf

Liberties (Civil Liberties Union for Europe). (2025). *Rule of law report 2025.* https://dq4n3btxmr8c9.cloudfront.net/files/vdxw3e/Liberties_Rule_of_Law_Report_2025_v.pdf

Lopatka, J. (2024, March 27). Czechs sanction Medvedchuk, website over pro Russian EU political influence. *Reuters.* https://www.reuters.com/world/europe/czechs-sanction-medvedchuk-website-over-pro-russian-eu-political-influence-2024-03-27

Lores, R. (2025). *Global Crypto User Index 2025.* Statista. https://www.statista.com/outlook/fmo/digital-assets/cryptocurrencies/worldwide?srsltid=AfmBOorgqEAOLng7cSMAFDInxing0Kw13xMpvwg1gJcvm_ZC590gOuQg

Martin, T. (2022, November 11). Russia's cyberattacks aimed at 'destabilizing' Moldova, PM says. *The Record.* https://therecord.media/russias-cyberattacks-aimed-at-destabilizing-moldova-pm-says

McGrath, S. (2025, September 22). Moldova detains 74 people over an alleged Russia-backed unrest plot around key election. *AP News.* https://apnews.com/article/moldova-russia-arrests-plot-election-293ee902e878ce1efcca339759eb06d0

McGrath, S., & Alexandru, A. (2025, September 9). Moldova's president accuses Russia of conducting 'hybrid war' ahead of key elections. *AP News.* https://apnews.com/article/moldova-elections-russia-influence-europe-8cc882551dd52957491e3cfd112cc878

McGrath, S., & Dumitrache, N. (2025, May 13). Romania's redo of a presidential election is a high stakes test of a battered democracy. *AP News.* https://apnews.com/article/romania-election-presidency-europe-far-right-russia-baf335441276aa88859c010bc04da686

Meaker, M. (2023, October 3). Slovakia's election deepfakes show AI is a danger to democracy. *WIRED.* https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy

Microsoft. (2025, October). *Microsoft Digital Defense Report 2025.* https://aka.ms/Microsoft-Digital-Defense-Report-2025#page=1

Microsoft Threat Analysis Center. (2024a, April 4). Same targets, new playbooks: East Asia threat actors employ unique methods. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/east-asia-threat-actors-employ-unique-methods

Microsoft Threat Analysis Center. (2024b, September 27). Russia-linked operators engaged in expansive efforts to influence US voters. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/russia-linked-operators-engaged-in-expansive-efforts-to-influence-us-voters

Molas, B. (2024, December 15). Doxing: A literature review. *The International Centre for Counter Terrorism*. https://icct.nl/publication/doxing-literature-review

Moldpres – State News Agency. (2025, August 13). Moldova's Intelligence and Security Service, Police, ANRCETI ask to block over 400 TikTok channels. https://www.moldpres.md/eng/society/moldova-s-intelligence-and-security-service-police-anrceti-ask-to-block-over-400-tiktok-channels

Militära underrättelse- och säkerhetstjänsten (Must). (2025). *Annual Report 2024*. https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/2024-must-annual-report.pdf

Nakamura, D., Belton, C., & Sommer, W. (2024, September 4). Justice Dept. charges two Russian media operatives in alleged scheme. *The Washington Post*. https://www.washingtonpost.com/national-security/2024/09/04/justice-department-election-security

Nardelli, A. (2025, September 22). Revealed: Putin's secret plan to hack Moldova's pivotal election. *Bloomberg*. https://www.bloomberg.com/news/articles/2025-09-22/moldova-elections-russia-s-plan-to-hack-the-vote

National Task Force on Election Crises. (2025a, July 8). National Task Force on Election Crises. Protect Democracy. https://protectdemocracy.org/work/national-task-force-on-election-crises

National Task Force on Election Crises. (2025b, July 8). Lessons from the 2024 general election. https://electiontaskforce.org/lessons-from-the-2024-general-election

NATO. (2022). *Strategic concept*. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. (2024). Countering hybrid threats. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. (2025). NATO's approach to counter information threats (official text). https://www.nato.int/cps/en/natohq/official_texts_231905.htm

NCSC (UK). (2025). *Cyber Assessment Framework v4.0*. https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf

Newman, N., Fletcher, R., Robertson, C. T., Ross Arguedas, A., & Nielsen, R. K. (2024). *Digital News Report 2024*. Reuters Institute. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf

National Institute of Standards and Technology (NIST). (2020). *SP 800 207: Zero Trust Architecture*. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

National Institute of Standards and Technology (NIST). (2022). *SP 800 218: Secure Software Development Framework (SSDF) v1.1*. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf

National Institute of Standards and Technology (NIST). (2023). *SP 800 207A: A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments* https://csrc.nist.gov/pubs/sp/800/207/a/final

National Institute of Standards and Technology (NIST). (2024). *SP 800 218A: Secure software development practices for generative AI & dual use foundation models*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf

O'Brien, M., & Swenson, A. (2024, February 16). Tech companies sign accord to combat AI generated election trickery. *AP News*. https://apnews.com/article/ai-generated-election-deepfakes-munich-accord-meta-google-microsoft-tiktok-x-c40924ffc68c94fac74fa994c520fc06

Ohlin, J. D. (2020). *Election interference: International law and the future of democracy*. Cambridge University Press. https://doi.org/10.1017/9781108859561

Olari, V. (2024, October 18). What to know about Russian malign influence in Moldova's upcoming election. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/what-to-know-about-russian-malign-influence-in-moldovas-upcoming-election

Olari, V. (2025a, March 6). Telegram network seeks to manipulate Moldova's local political discourse. *DFRLab*. https://dfrlab.org/2025/03/06/telegram-network-moldova/

Olari, V. (2025b, March 26). Cross platform campaign sows anti Europe division in Moldova. *DFRLab*. https://dfrlab.org/2025/03/26/cross-platform-campaign-sows-anti-europe-division-in-moldova/

OSCE/ODIHR. (2017). Montenegro, Parliamentary Elections, 16 Oct 2016: Final report. https://www.osce.org/odihr/elections/montenegro/295511

OSCE/ODIHR. (2021). *Republic of Moldova, Early Parliamentary Elections, 11 July 2021: Final report*. https://www.osce.org/odihr/elections/moldova/501518

OSCE/ODIHR. (2024). *Moldova, Presidential Election and Constitutional Referendum, 20 Oct 2024: Statement of preliminary findings and conclusions*. https://www.osce.org/odihr/elections/moldova/578815

OSCE/ODIHR. (2025a, February 20). *Poland, Presidential Election, Run off, 2025: Final report*. https://www.osce.org/odihr/elections/poland/591761

OSCE/ODIHR. (2025b, September 28). *Republic of Moldova, statement of preliminary findings and conclusions*. https://www.osce.org/files/f/documents/4/7/597800.pdf

OSCE/ODIHR. (2025c, March 14). *Republic of Moldova: Presidential election and constitutional referendum, 20 Oct & 3 Nov 2024, Final report*. https://www.osce.org/files/f/documents/3/9/587451_0.pdf

OSCE/ODIHR. (2025d, May 5). Notable efforts to address electoral integrity but certain aspects… (Romania). https://www.osce.org/odihr/elections/romania/590330

Pamment, J., Nothaft, H., Agardh-Twetman, H. & Fjällhed, A. (2018). *Countering Information Influence Activities: The State of the Art*. MSB. https://rib.msb.se/filer/pdf/28697.pdf

Pamment, J., & Tsurtsumia, D. (2025, May). *Beyond Operation Doppelgänger: A capability assessment of the Social Design Agency (SDA)*. Lund University & Swedish Psychological Defence Agency. https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-05/Beyond%20Operation%20Doppelg%C3%A4nger.pdf

Pamment, J., & Isaksson, E. (2024). *Psychological Defence: Concepts and Principles for the 2020s* (MPF Report Series 6/2024). Lund University & Swedish Psychological Defence Agency. https://www.mpf.se/wp-content/uploads/2024/03/mpf_rapport_6_2024_psychological_defence.pdf

Perdomo, C., & Uribe Burcher, C. (2017). Money, influence, corruption and capture: can democracy be protected?. *The Global State of Democracy 2017 Exploring Democracy's Resilience. International IDEA*. https://www.idea.int/gsod-2017/files/IDEA-GSOD-2017-REPORT-EN.pdf

Popescu Zamfir, R. (2025, September 26). *Moldova's Election Is a Test for Russian Influence in Europe. Carnegie Endowment for International Peace.* https://carnegieendowment.org/research/2025/09/moldovas-election-is-a-test-for-russian-influence-in-europe?lang=en

Posetti, J., et al. (2020). *Online violence against women journalists: A global snapshot of incidence and impacts.* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000375136/PDF/375136eng.pdf.multi

Rainsford, S. (2024, December 4). Romania hit by major election influence campaign and Russian cyber attacks. *BBC.* https://www.bbc.com/news/articles/cgq18w507dko

ReliaQuest. (2024, September 24). 2024 US election: Top cyber threats & organizational impacts. https://www.reliaquest.com/blog/2024-us-election-top-cyber-threats-organizational-impacts/

Reuters. (2024a, October 24). Chinese influence operation targets U.S. down ballot races, Microsoft says. https://www.reuters.com/world/us/chinese-influence-operation-targets-us-down-ballot-races-microsoft-says-2024-10-23/

Reuters. (2024b, November 5). Hoax bomb threats linked to Russia target polling places in battleground states, FBI says. https://www.reuters.com/world/us/fake-bomb-threats-linked-russia-briefly-close-georgia-polling-locations-2024-11-05/

RFE/RL Moldovan Service. (2024, October 25). Moldovan police accuse pro Russian oligarch of $39M vote buying scheme. https://www.rferl.org/a/moldova-police-accuse-shor-russia-oligarch-39m-vote-buying/33172951.html

Roth, A. (2024, September 4). Russia accused of trying to influence US voters through online campaign. *The Guardian.* https://www.theguardian.com/us-news/2024/sep/04/russia-us-election-online-campaign-sanctions

Saeva, E., & Tasheva, I. (2024). The 2024 EU elections and cybersecurity: A retrospective and lessons learned. *European View* (Martens Centre). https://www.martenscentre.eu/wp-content/uploads/2024/11/12.pdf

Schroeder, D. T., Cha, M., Baronchelli, A., Bostrom, N., Christakis, N. A., Garcia, D., … Kunst, J. R. (2025). How malicious AI swarms can threaten democracy. *arXiv.* https://doi.org/10.48550/arXiv.2506.06299

Stimson Center. (2024, August 8). RAI Session: AI & democracy (event). https://www.stimson.org/event/rai-session-ai-democracy

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hal, J., & Kieran. (2024). *AI enabled influence operations: Safeguarding future elections.* The Alan Turing Institute (CETaS). https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections

Tanas, A. (2024, October 24). Moldovan president says bribery affected election, pledges run off vote. *Reuters.* https://www.reuters.com/world/europe/moldova-police-say-businessman-shor-channelled-24-million-pay-off-voters-2024-10-24/

Turing Institute / CETaS. (2024). AI enabled influence operations: *Safeguarding future elections.* https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections

Uribe Burcher, C. (2017). Assessing the threat of nexus between organized crime and democratic politics: Mapping the factors. *International Relations and Diplomacy*, 5(1). https://www.davidpublisher.com/index.php/Home/Article/index?id=30183.html

Uribe Burcher, C. (2019). *Cryptocurrencies and political finance*. International IDEA. https://www.idea.int/publications/catalogue/cryptocurrencies-and-political-finance

U.S. Cyber Command. (2024, September 12). Russian disinformation campaign Doppelgänger unmasked: A web of deception. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception

U.S. Department of Justice (DOJ). (2024a). Election threats. https://www.justice.gov/archives/voting/election-threats

U.S. Department of Justice (DOJ). (2024b, September 4). Justice Department disrupts covert Russian government–sponsored foreign malign influence operation. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

U.S. Office of the Director of National Intelligence (ODNI). (2024, March 11). *Annual threat assessment of the U.S. Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

U.S. Office of the Director of National Intelligence (ODNI). (2025, March 18). *Annual threat assessment of the U.S. Intelligence Community 2025*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

U.S. Treasury (OFAC). (2024a, September 4). Treasury takes action as part of a U.S. Government response to Russia's foreign malign influence operations. https://home.treasury.gov/news/press-releases/jy2559

U.S. Treasury (OFAC). (2024b, December 31). Treasury sanctions entities in Iran and Russia that attempted to interfere in the U.S. 2024 election. https://home.treasury.gov/news/press-releases/jy2766

V-Dem Institute. (2024). *Democracy report 2024: Democracy winning and losing at the ballot*. https://v-dem.net/publications/democracy-reports

V-Dem Institute. (2025). *Autocratization turns viral: Democracy report 2025*. https://v-dem.net/publications/democracy-reports

Vanderlee, K., & Collier, J. (2024, April 25). Poll vaulting: Cyber threats to global elections. *Google Cloud / Mandiant*. https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections

Weatherbed, J. (2024, November 14). Google says it will stop serving political ads in the EU. *The Verge*. https://www.theverge.com/2024/11/14/24296510/google-dropping-political-ads-in-the-eu-ttpa

Westminster Foundation for Democracy (WFD). (2025). *Understanding and addressing the cost of politics*. https://www.wfd.org/cost-of-politics

WHAS11. (2025, July 8). Jefferson County Clerk's Office says voting system remains safe after ransomware attack. https://www.youtube.com/watch?v=diY7hpMlY5o

Wilson, A. (2023). *Democracy under siege: Tackling Russian interference in Moldova*. ECFR. https://ecfr.eu/article/democracy-under-siege-tackling-russian-interference-in-moldova/

Wilson Center. (2025, March 19). Ukraine's presidential elections amid war: Political, legal, and security challenges. https://www.wilsoncenter.org/blog-post/ukraines-presidential-elections-amid-war-political-legal-and-security-challenges

08 Endnotes

1 Global Witness, 2025; Meaker, 2023; Rainsford, 2024; McGrath and Alexandru, 2025
2 Bay et al., 2022; Hollis and Ohlin, 2021
3 Bay, 2024; EEAS, 2025a
4 Bay et al., 2022; Bay 2024; Levin, 2020; Ohlin, 2020
5 Pamment and Tsurtsumia, 2025
6 US Office of the Director of National Intelligence, 2025; Communications Security Establishment Canada, 2025
7 Bay, 2024
8 Stockwell et al., 2024; Csernatoni, 2024; Schroeder et al., 2025
9 Stockwell et al., 2024; Csernatoni, 2024; Schroeder et al., 2025
10 Bay, 2024; Hybrid CoE, 2025
11 Bay, 2024
12 Bay, 2024; Alihodžić, 2023; Center for an Informed Public et al., 2021
13 International IDEA, 2024
14 Bryjka, 2024; OSCE/ODIHR, 2025b; OSCE/ODIHR, 2025c
15 Gilbert, 2024
16 Center for an Informed Public et al., 2021
17 Center for an Informed Public et al., 2021; International IDEA, 2024; DFRLab, 2023; EUvsDisinfo 2024
18 Huo, 2024; Hedling, 2025
19 Hedling, 2025
20 Hoogensen Gjørv & Jalonen, 2023
21 Hedling, 2025
22 Hedling, 2025
23 US Office of the Director of National Intelligence, 2025
24 Pamment and Tsurtsumia, 2025
25 Bay, 2024
26 Hoffman, 2022
27 Atlantic Council 2023; Pamment and Tsurtsumia, 2025
28 Bay, 2024; European Commission, 2016; EEAS, 2024; EEAS 2025a; NATO, 2022; NATO, 2025
29 EEAS, 2025a; EEAS, 2025b
30 cf. Huo, 2024; Pamment and Tsurtsumia, 2025; Stockwell et al., 2024
31 Pamment and Tsurtsumia, 2025; Microsoft Threat Analysis Center, 2024a; Microsoft Threat Analysis Center, 2024b
32 EEAS, 2025a; U.S. Cyber Command, 2024
33 Pamment and Tsurtsumia, 2025
34 EDMO, 2024
35 Pamment and Tsurtsumia, 2025
36 EUvsDisinfo, 2024a
37 Bjola, 2025; IFES, 2024; Global Witness, 2024
38 Chan 2024; European Commission, 2024
39 Clayton, 2014; Atlantic Council, 2018
40 Nardelli, 2025
41 OSCE/ODIHR, 2024; OSCE/ODIHR, 2025b

42 Kubica, 2024; EUvsDisinfo, 2024b
43 Tanas, 2024; Balmforth & Dysa, 2024
44 Antoniuk, 2024; Antoniuk, 2025; Olari, 2024; Olari, 2025a; Olari, 2025b
45 Kubica, 2024; EUvsDisinfo, 2024a; DFRLab, 2024
46 Tanas, 2024; Balmforth & Dysa 2024; OSCE/ODIHR 2025; RFE/RL Moldovan Service, 2024
47 DFRLab, 2024; EUvsDisinfo, 2024a; Balmforth & Dysa, 2024
48 McGrath, 2025; IGP, 2025
49 McGrath, 2025; IGP, 2025
50 Moldpres, 2025; IGP, 2025
51 Antoniuk, 2023; Antoniuk, 2024; Antoniuk, 2025; Martin, 2022; OSCE/ODIHR, 2021
52 Cerulus, 2025; EEAS 2025c; European Commission 2025c
53 Pamment & Tsurtsumia, 2025
54 Euromaidan Press, 2014; EEAS, 2025a
55 Hedenskog & Hjelm, 2020; Lopatka, 2024
56 Clayton, 2014; Atlantic Council, 2018; Euromaidan Press, 2014
57 ODNI, 2024; ODNI, 2025
58 FBI, 2024; Reuters, 2024a; Roth, 2024; U.S. Treasury, 2024a, 2024b
59 DOJ, 2024b; Microsoft Threat Analysis Center, 2024b; Nakamura, Belton & Sommer, 2024
60 Atlantic Council, 2024; Microsoft Threat Analysis Center, 2024a; Reuters, 2024a
61 Bing & Vicens, 2024; DOJ, 2024a Gavin, 2025
62 DOJ, 2024a; FBI, 2024; U.S. Treasury, 2024a; 2024b
63 Kovalčíková & Spatafora, 2024; National Task Force on Election Crises, 2025a; National Task Force on Election Crises, 2025b; Turing CETaS, 2024
64 Bay, 2024
65 Ledford, 2024
66 Pamment & Tsurtsumia, 2025
67 Zuboff, 2019
68 Cf. Mutu, 2024; Newman, Fletcher, Robertson, Ross Arguedas, & Nielsen, 2024
69 European Commission, 2024
70 Weatherbed, 2024; Chan, 2025
71 Elliott, 2024
72 O'Brien & Swenson, 2024; Brennan Center for Justice, 2024
73 C2PA, 2024
74 Google DeepMind, 2025
75 Newman et al., 2024
76 Pamment & Tsurtsumia, 2025
77 Bateman & Jackson, 2024; Bay, 2025; Pamment et al. 2018; Pamment & Isaksson, 2024
78 OECD 2021; OECD 2022
79 ENISA 2023; International IDEA 2023; Bay 2025
80 Center for an Informed Public et al. 2021
81 Lewandowsky et al., 2020
82 EEAS, 2025
83 OECD, 2021
84 Center for an Informed Public et al., 2021; C2PA, 2024; ENISA, 2023
85 OECD, 2022
86 C2PA, 2024; Google DeepMind, 2025
87 Perdomo & Uribe Burcher, 2017: 128; WFD, 2025
88 Bakken, 2025; Popescu-Zamfir, 2025; OSCE/ODIHR, 2017: 12; 2021: 16
89 International IDEA, 2025
90 OSCE/ODIHR, 2025a: 1–2
91 Wilson, 2023
92 Wilson, 2023; OSCE/ODIHR, 2025b: 1
93 International IDEA, 2025
94 Perdomo & Uribe Burcher, 2017: 134
95 CoinGecko, 2025; Lores, 2025; Chainalysis, 2024a
96 Coherent Market Insights, 2025

97 Uribe Burcher, 2019: 14
98 Uribe Burcher, 2019: 13; Chainalysis, 2024b
99 International IDEA, 2025
100 Perdomo & Uribe Burcher, 2017: 139; Wolfs, 2025: 3–4
101 Wolfs, 2025: 5
102 Agrawal, Hamada & Fernández Gibaja, 2021: 12
103 Ryan, 2018; Britzky, 2018
104 DOJ, 2024a
105 IFES, 2024
106 OSCE/ODIHR, 2025a: 8–9
107 Perdomo & Uribe Burcher, 2017: 137–138
108 Council of Europe, 2025: 4
109 International IDEA, 2025
110 Wolfs, 2025: 2
111 Perdomo & Uribe Burcher, 2017: 141
112 Uribe Burcher, 2019: 7, 9–11
113 Vasani, James & Holly, 2022
114 Uribe Burcher, 2019: 15–16
115 International IDEA, 2025
116 Perdomo & Uribe Burcher, 2017: 138–139
117 Uribe Burcher, 2019: 16
118 Wolfs, 2025: 2
119 Perdomo & Uribe Burcher, 2017: 144
120 International IDEA, 2025
121 V-Dem, 2024; V-Dem, 2025; UNESCO, 2025; Posetti et al., 2020
122 Council of Europe, 2025; Liberties, 2025; Freedom House, 2024
123 CIVICUS, 2024; OSCE/ODIHR, 2023
124 OECD, 2021; OSCE/ODIHR, 2023
125 Perdomo & Uribe Burcher, 2017: 136
126 Europol, 2025a; Hoxhunt, 2025
127 Bay, 2024
128 Uribe Burcher, 2017
129 Europol, 2025a
130 Cyble, 2024
131 Deloitte, 2024
132 Europol, 2025a
133 Europol 2025a; Deloitte 2024
134 Must, 2025; ReliaQuest, 2024
135 ReliaQuest, 2024; Center for Internet Security, 2025a
136 Europol, 2025a
137 CISA, 2024
138 CISA, 2024
139 Hoxhunt, 2025
140 Forbes 2025
141 CISA 2024a; NIST 2020; FIDO Alliance 2023; ENISA 2023; MS-ISAC 2024; C2PA 2024
142 Bay, 2024; ReliaQuest, 2024
143 Bay et al., 2022
144 Bay, 2024
145 UK Electoral Commission, 2024
146 Euromaidan Press, 2014
147 Alliance for Securing Democracy, 2019
148 Council of Europe, 2024; Wilson Center, 2025
149 CNN, 2024a
150 WHAS11, 2025
151 Constella Intelligence, 2025
152 Center for Internet Security, 2025a; Center for Internet Security, 2025b; Center for Internet Security, 2025c
153 Cloudflare, 2025

154 Saeva & Tasheva, 2024
155 Bay et al., 2022; County of San Luis Obispo, 2024
156 Bay, 2024; ReliaQuest, 2024
157 Electionline, 2024
158 Ivanti, 2025
159 Cyble, 2025
160 ReversingLabs 2025; ISACA, 2025
161 ISACA, 2025
162 Cisco, 202
163 International IDEA, 2019
164 Bay, 2024
165 Google Cloud, 2023
166 CISA, 2024
167 Molas, 2024; Cybersecurity Dive, 2024
168 Stimson Center, 2024
169 International IDEA 2019; Bay 2024; Google Cloud 2023; CISA 2024a; Stimson Center 2024
170 cf. Microsoft, 2025
171 Vanderlee & Collier, 2024; NCSC, 2025
172 Bay, 2024; International IDEA, 2023
173 Center for Internet Security 2025a; NIST, 2022; NIST, 2024
174 CrowdStrike 2025a; NIST, 2020; NIST, 2023
175 CISA, 2024b; CrowdStrike, 2025b
176 CISA & EAC, 2024a; CISA & EAC, 2024b; CISA, 2024b
177 Bay, 2024; Bay, 2025
178 Bay, 2024
179 Canada, 2025
180 Bay, 2024
181 Bay, 2024
182 European Commission, 2016; European Commission, 2025b
183 Bay, 2024; Bay, 2025
184 Bay, 2025
185 GAO, 202
186 Columbia University, 2025
187 Elections Canada, 2025
188 Government of Canada, 2025; PCO, 2025
189 Canada, 2025, CISA 2025
190 Cf Bay, 2025
191 Hybrid CoE, 2024
192 Bay, 2025; Canada, 2025
193 European Commission, 2025b
194 Bay, 2024; Elections Canada, 2025
195 European Commission, 2025b
196 European Commission, 2025a
197 NATO, 2024; Elections Canada, 2025
198 International IDEA, 2025; The Carter Center, 2025
199 US Office of the Director of National Intelligence, 2025; Pamment & Tsurtsumia, 2025
200 Pamment & Tsurtsumia, 2025
201 Stockwell et al. 2024; CISA, 2024a
202 IFES 2024; Bay, 2024
203 Brennan Center for Justice, 2020; Elliott, 2024; European Commission, 2024; C2PA, 2024; Pamment & Tsurtsumia, 2025

Folke Bernadotte Academy (FBA) is the Swedish government agency for peace, security, and development. As part of Sweden's international development cooperation, we promote peace in conflict-affected countries. We offer training and advice and conduct research to strengthen peacebuilding and governance, in peace and security contexts. Moreover, we deploy civilian personnel to peace operations and election observation missions primarily led by the UN, EU and OSCE. The agency is named after Count Folke Bernadotte, the UN's first peace mediator.

If you want to know more about FBA, meet us at:

linkedIn.com/FolkeBernadotteAcademy

instagram.com/FolkeBernadotteAcademy

facebook com/FolkeBernadotteAcademy

soundcloud.com/FolkeBernadotteAcademy

www.fba.se

Folke Bernadotte Academy
Swedish agency for peace, security and development

FBA