From Global Tensions to Local Targets: Election Interference in Canada and Alberta

Executive Summary

Elections are pivotal political events with outcomes that reach far beyond national borders, often shaping the broader geopolitical landscape. The 2024 election year was particularly significant, marking the largest global election cycle in history, while 2025 has already seen several consequential elections with far-reaching implications. While these moments empower voters to democratically shape their political futures, they also create strategic openings for threat actors to interfere, attempting to manipulate outcomes and voter behaviour in pursuit of strategic aims.

Election interference involves efforts to manipulate democratic processes to influence outcomes, undermine confidence, or erode trust in democratic institutions. These actions can destabilize governments, polarize societies, and weaken the independence of elected officials.

Three principal categories of attack define the modern election interference threat landscape:

- **Influence operations** that exploit social media platforms and domestic grievances to target the electorate with disinformation.
- **Cyberattacks** targeting political organizations and election infrastructure to steal sensitive voter data or undermine political operations.
- **Covert operations** by human agents who attempt to manipulate voters and targeted members of political organizations, often from diaspora communities, to advance foreign strategic objectives.

These threats are most frequently directed at NATO and EU member states, where democratic systems are viewed as barriers to the geopolitical ambitions of nation-states with conflicting interests. The threat of interference intensifies during head of state elections but remains substantial even for local elections, placing Canada's federal and provincial governments at heightened risk of ongoing interference beyond the recent federal election this year.

Within this context, Alberta emerges as a unique and increasingly attractive target. The province's significant natural resources, considerable political influence, and its large diaspora communities make it susceptible to all three forms of interference. Alberta's past policy decisions involving China, and Russia, combined with growing internal debates over sensitive domestic policies, and a possible referendum on separation, create fertile ground for exploitation by foreign actors. Furthermore, Alberta may attract further interest from interferers in the near future as the province aspires to become a global leader in developing artificial intelligence (AI) data centres. Even when the province is not the primary target, its significance to Canadian national policy means it is often caught in the crossfire of broader campaigns aimed at Canada.

This report identifies influence operations as the most persistent and complex threat, especially with the growing use of Generative AI to impersonate trusted voices and produce highly tailored disinformation. Such content is often laundered through domestic profiles who echo foreign-origin narratives, sometimes for ideological reasons, and sometimes for personal gain. These efforts are further amplified by social media algorithms that prioritize engagement over truth, giving emotionally charged content a disproportionate reach.

Given the evolving nature of these threats, Alberta and Canada must work to raise awareness to these threats and safeguard our digital systems enabling elections. The final section of this report, *Combatting Election Interference*, outlines key recommendations to support election security in future electoral cycles.

Introduction

This report explores the evolving threat of election interference, identifying nation-states behind these efforts, analyzing their operations and tactics, and highlighting democratic institutions most often targeted. It also provides key insights to the specific threats facing Alberta, where political relevance, resource wealth, and demographic factors create unique vulnerabilities. Finally, practical recommendations to help safeguard Alberta's electorate and democratic processhes are provided, as well an outlook on the future of election interference and recent case studies, provided in Appendix B, that illustrate how election interference unfolds and the serious consequences it can carry.

The Victimology and Motivations of Election Interference

Analysis of reported foreign election interference in 2024 demonstrates that NATO and EU member states were disproportionately targeted compared to the rest of the world. This trend has continued in 2025 with election interference targeting Canada (Privy Council Office, 2025)**, Germany** (CORRECTIV, 2025)**, Poland, Romania** (Antoniuk, 2025)**, and Moldova** (Engelbrecht, 2025)**.**

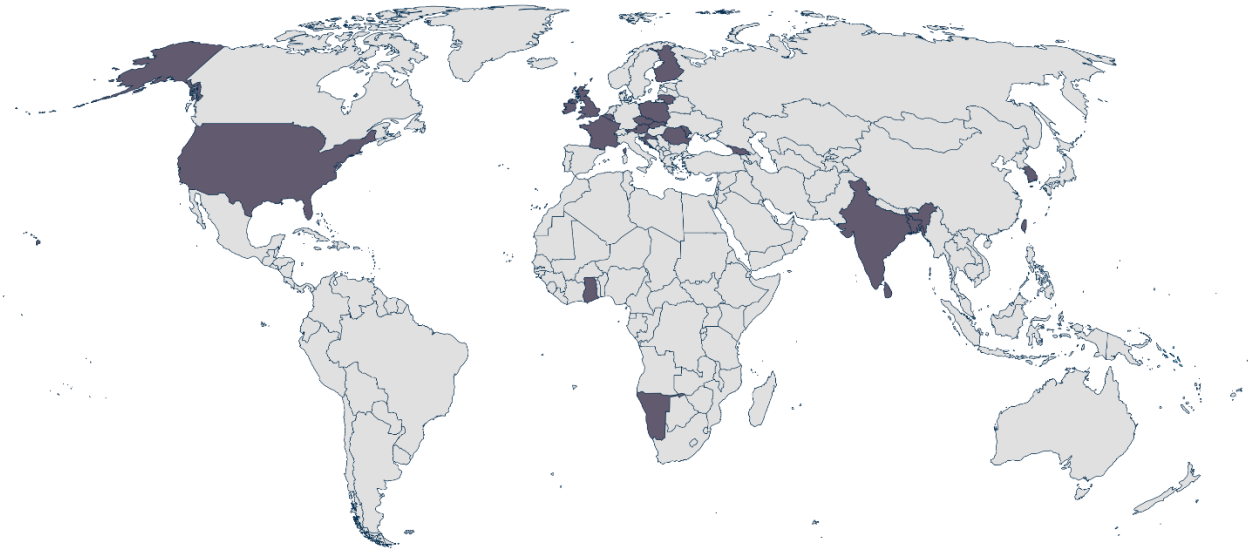

Figure 1 - All countries reportedly targeted by foreign election interference in 2024.

The disproportionate targeting of NATO and EU countries can be attributed to their often-conflicting geopolitical positions with the nation-states often responsible for foreign election interference. These attacks are part of a broader hybrid strategy, commonly referred to as "grey zone" warfare, adopted by global players to deter NATO and EU hegemony, without provoking open conflict or triggering an Article 5 response (North Atlantic Treaty Organization, 2023). The objective is to either erode the geopolitical standing of these democracies or shift the political alignment of other-nation states in favour of the interfering actors.

Consequently, election interference is often aimed at achieving outcomes favourable to the interferer's strategic objectives, including, but not limited to:

- Fracturing formal alliances
- Undermining support for allies
- Exacerbating societal division
- Discouraging criticism of authoritarian regimes

Statistical analysis of the reported foreign election interference activity in 2024 reveals the probability of election interference for NATO or EU members is highest for those holding head of state elections, but the threat remains considerable for local government elections also.

	All types of elections	Head of state	Upper house of parliament	Lower house of parliament	Local government
All Nation-states	24/65 (37%)	17/41 (41%)	2/7 (28%)	3/11 (27%)	2/6 (33%)
Members of NATO or EU, or both	13/16 (81%)	7/8 (88%)	Insufficient data	3/3 (100%)	2/3 (66%)
Non-NATO or EU members	11/49 (23%)	10/33 (27%)	1/5 (20%)	0/8 (0%)	0/3 (0%)

Table 1 - Statistical analysis of reported foreign election interference activity since the beginning of 2024 to the time of writing. Broken down by membership of a formal alliance group and type of election.

Geopolitical Issues Driving Election Interference in Canada and the Spillover into Alberta

The statistical analysis shows that Canada, a key NATO member, is highly likely to be a target of election interference for the foreseeable future. However, Canada has further characteristics that support this assessment. Given its membership in NATO and other major alliances such as the G7, its rich natural resources, deep integrations with the U.S. economy, and ability to exercise political soft power abroad, Canada emerges as a strong target for election interference by would-be adversarial nation-states.

Canada also has ongoing geopolitical tensions with several nation-states, most notably China, Russia, Iran, and India, that may serve as motivation for past and future election interference. These nation-states have been attributed to prior attempts to interfere in Canadian elections which are described in more detail throughout this report. Key points of contention include Canada's support for Taiwan's democracy (Hardie, p.8 2023), sanctions against Russia and support for Ukraine (Government of Canada, 2025), designation of Iran as a terrorist regime (Canadian Border Services Agency, 2024), and support for Sikh Separatism (Biswas, 2024). These issues illustrate the political fault lines between Canada and known interferers and may provide the impetus for interference in Canadian elections, aiming to align Canada's stance on these and other matters more closely with foreign interests.

Alberta's political relevance within Canada, resource wealth, diaspora communities and its ability to influence international policy suggest the province has a realistic possibility of being targeted by election interference. Alberta's policies such as the Memorandum of Understanding (MoU) to support Ukraine's energy sector (Carmichael, 2024) or previous restrictions on partnerships with Chinese

academics (Canadian Association of University Teachers, 2022) may encourage nation-state actors engaged in targeting Canadian elections to focus their attention on Alberta.

Alberta may also be indirectly targeted by election interference aimed at Canada more broadly as issues that are relevant to Alberta, (such as equalization payments, pipeline development, and environmental regulations) frequently feature in national political discourse. These issues often have political fault lines that make them useful pain points for would-be interferers when targeting Canadian or Albertan democratic processes. This report later provides examples of how Alberta's issues can and have been leveraged by inauthentic attempts to undermine the recent federal election.

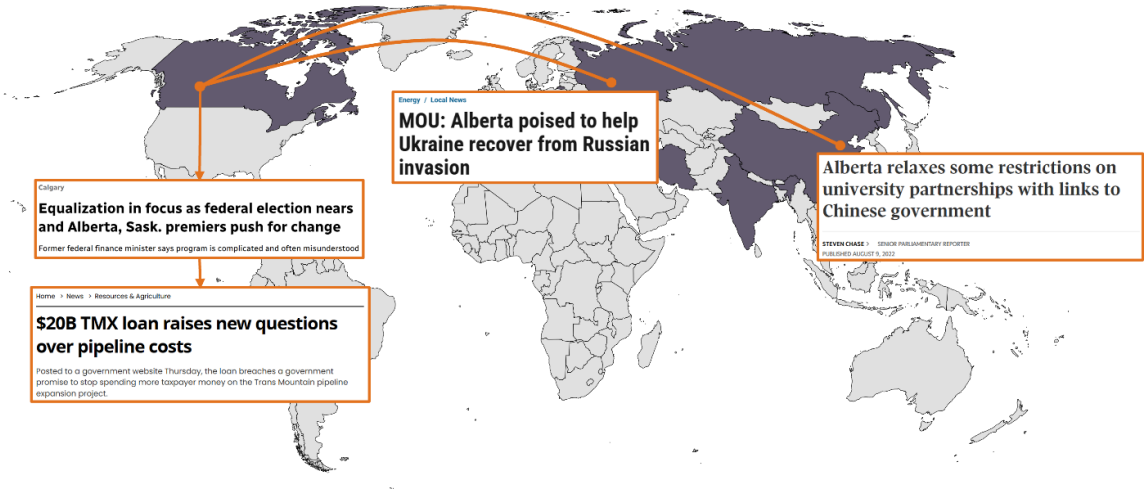

Figure 2 - Examples of wedge issues between Alberta and nation-states, as well as domestic issues relevant to Alberta that may be exploited.

Methods of Manipulation: The Common Threats Enabling Election interference

Election interference involves a range of tactics aimed at manipulating electoral outcomes or destabilizing societies. The primary threat stems from **influence operations** designed to sway voter behaviour. These efforts are often compounded by **cyberattacks** targeting sensitive data within political organizations or attempting to disrupt election infrastructure. Additionally, **covert operations**, typically conducted by human operatives in the physical realm, can further erode democratic processes by exerting pressure on voters and political figures, with a particular focus on members of diaspora communities. The specific tactics and their implications are detailed in the sections below.

Influence Operations: The Role of Harmful Narratives on Political Thought

Influence operations are the most pressing threat to elections today. These campaigns are deliberately designed to compromise public opinion and disrupt political discourse of a target region with disinformation. Typically coordinated by well-resourced nation-states (U.S. Department of the Treasury, 2024), their intent may include supporting a preferred election outcome, degrading outcomes perceived as detrimental, or crudely polarizing a target nation’s electorate, or undermining the ability of target governments to act in their own interests.

Influence operations aim to reach the broadest possible audience to maximize their impact. Their targets are primarily **the electorate**, which consists of all eligible voters, but also includes more influential entities within **political organizations**, including sitting governments, election campaigns, the media, and policy-shaping special interest groups like think tanks and research centres. The higher an influence operation can reach, the further its harmful narratives can spread, impacting not only niche online communities, but also high-profile individuals such as political commentators, celebrities, and even election candidates. When such narratives break through into mainstream discourse, the likelihood of changing voter behaviour, shaping policy, or prompting civil unrest and violence, increases significantly (Nimmo, 2020).

Operators behind influence operations disseminate harmful narratives on the same online platforms where legitimate political discourse occurs and public opinion is shaped (Insikt Group, 2024). These efforts primarily take place on social media, using co-ordinated networks of **inauthentic accounts** (commonly referred to as "bots") (Conspirador Norteño, 2024; Viginum, p.5, 2024) and webpages **impersonating news sites**. These sites attempt to give disinformation the appearance of legitimacy and circumvent sanctions on state-affiliated media entities (CyberAlberta, 2025; Insikt Group, 2024; Social Media Lab, 2024; Molter, 2024). To appear credible, these malign outlets often claim to be locally based, impersonating authentic members of the target audience, presenting themselves as grassroots supporters of certain election campaigns or independent media aligned with popular sentiment.

Figure 3 – Gabriel News, an impersonating news site identified by CyberAlberta, promotes anti-government and hateful views, often exploiting issues relevant to Albertans to advance a narrative targeting the federal government. The account also uses X to amplify its messaging and conduct engagement farming on related posts.

Inauthentic accounts and impersonating news sites often recycle the same narratives, amplify each other's posts, or coordinate comments and likes (a tactic known as engagement farming) to inflate the appearance of popularity and manipulate social media algorithms for increased visibility. Social media algorithms also have a well-documented tendency to favour content that provokes strong negative emotions, such as anger and anxiety, to sustain user engagement (Milli, Carroll, Wang, Pandey, Zhao, & Dragan, 2024). Furthermore, as platforms increasingly scale back their commitments to information integrity and shift responsibility onto users (Silverman, 2025), influence operations are increasingly well-positioned to expand their reach while evading detection.

*As early as 2022, a Russian influence operation known as Doppelganger ran an impersonating news site called Reliable Recent News (RRN) until it was seized in September 2024. Within that time, RRN produced articles with misleading descriptions of government policies undermining former Canadian Prime Minister Justin Trudeau while promoting his then-political opponent, Pierre Poilievre. (*Montpetit, 2024*).*

Leveraging Domestic Profiles to Launder Harmful Narratives

Within any given electorate, there are influential domestic profiles with large followings who express legitimate or perceived grievances against their governments. Foreign influence operations often seek to co-opt these accounts to amplify harmful narratives. This compliance is often attempted by crafting disinformation around divisive issues that are relevant to the target audience, engineered to provoke strong emotional responses. By weaponizing public fears and anxieties, foreign influence operations aim to resonate with these domestic actors, enabling the introduction of new harmful narratives into public discourse or reinforcing existing grievances that confirm prejudices held across the political spectrum and deter reconciliation.

Many of these domestic profiles operate within loosely connected ecosystems that consistently circulate inherently biased content (AllSides, 2025; Kelly, 2024; Starbird, 2017). Some participate unwilfully out of ideological alignment, while others are financially rewarded to disseminate foreign-origin narratives (U.S. Office of Public Affairs, 2024).

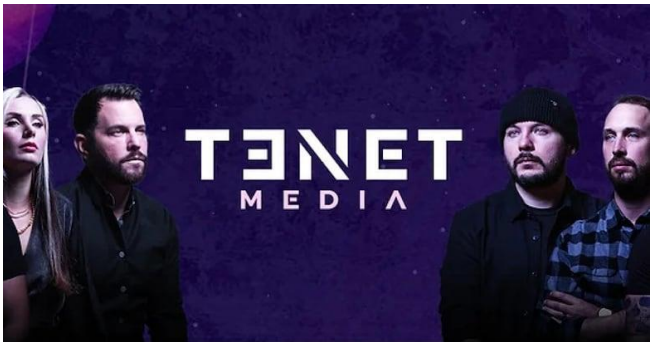

Figure 4 - Site banner of Tenet Media, a U.S.-based alternative news outlet co-founded by Canadian Lauren Chen, indicted by the U.S. Department of Justice for receiving financial payment by Russian state media network RT. (Source: Montpetit & Wong, 2024).

Although most foreign influence operations struggle to gain traction with domestic profiles, notable exceptions to this rule do exist. One prominent case involved the known Russian disinformation operation known as Matryoshka (VIGINUM, 2024), which impersonated the media outlet E! News, falsely claiming the U.S. Agency for International Development (USAID) paid celebrities millions in taxpayer dollars to visit Ukraine. The post was unwittingly amplified by high-profile accounts on X in pursuit of their own strategic interests, reaching millions before being debunked by the online community and the impersonated sources themselves (@antibot4navalny, 2025). Such amplification provides a high return on investment for influence operations and all but assures their continuation.

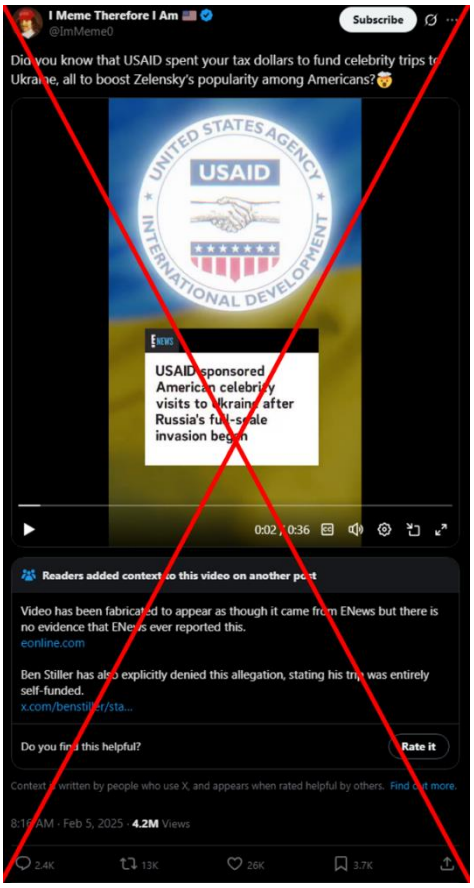

Figure 5 - A Matryoshka-linked post impersonated E! News to spread false claims that USAID misused taxpayer funds. The post was amplified by high-profile accounts on X, helping it surpass 4 million views (source: @antibot4navalny).

The Growing Use, and Capability, of Generative AI Within Influence Operations

Advancements in Generative AI have significantly lowered the barrier to entry for creating sophisticated disinformation and enables influence operations to operate automatically and at higher scale. This technology is increasingly used to quickly and more convincingly impersonate individuals and organizations (including news anchors, academics, and online communities like Taylor Swift fans) to hijack political narratives and sway audiences (Insikt Group, p.17, 2024; The Insider, 2024; Cohen, 2024). Beyond Generative AI, machine learning has also seen increased use to process vast volumes of data and generate detailed profiles of target audiences, enabling the tailoring of influence operations to specific demographics at scale (Rehagen, 2024).

- **Large Language Models (LLMs)** enable foreign actors to rapidly generate comments for inauthentic accounts and articles for impersonating news site that accurately mimic domestic voices, producing contextualized disinformation that reduces their chances of raising suspicion (OpenAI, p.7, 2024).
- **Audio Deepfakes**, such as the one seen in the 2023 Slovakian parliamentary election, have been used to fabricate recordings that falsely incriminate political figures (Appendix B(i)), but more recently are used to mimic political commentators to mislead their audiences.
- **Diffusion** technologies produce AI-generated images that are employed to create realistic profile pictures for inauthentic accounts that resemble the target audience, as well as emotionally charged images of politicians designed to provoke strong audience reactions.

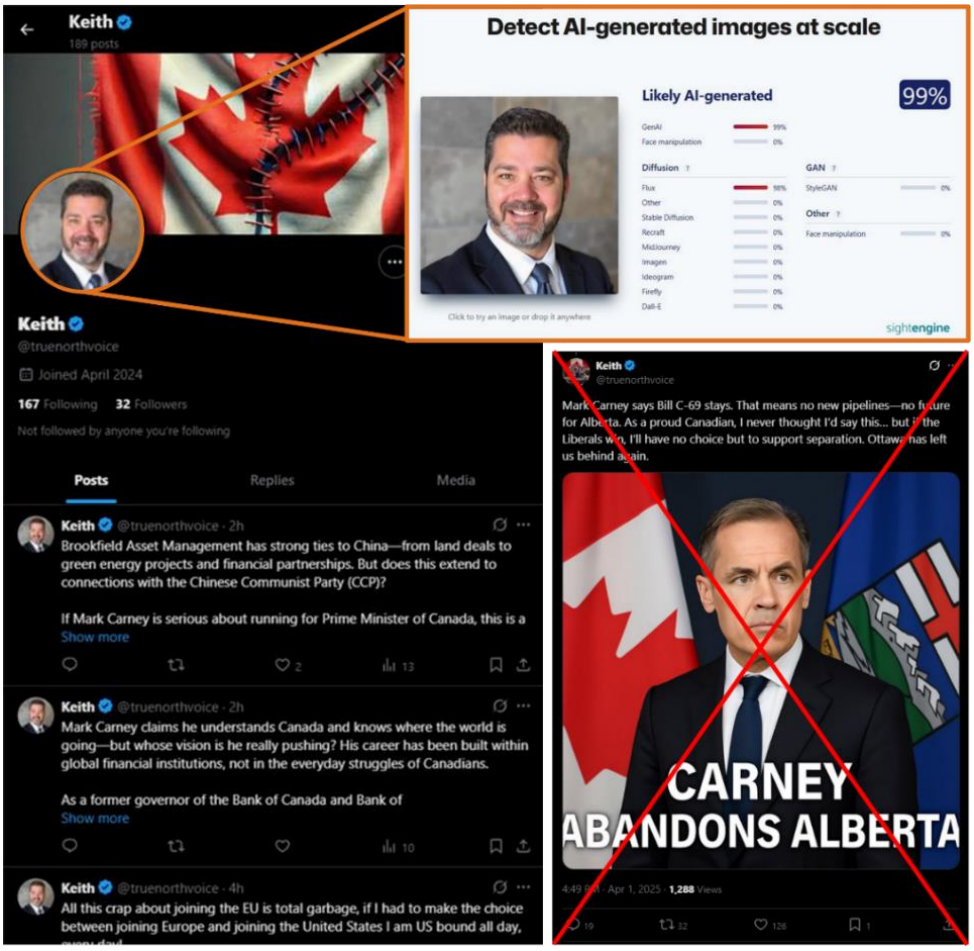

Figure 6 - An inauthentic account identified by CyberAlberta that used Generative AI to create a profile picture and subsequent posts targeting the Canadian federal government leveraging issues relevant to Alberta.

Despite this evolution, traditional methods such as doctored media and staged content remain widely exploited. Recent examples include:

- Russian actors spreading misleading videos claiming election malpractice during the 2024 U.S. presidential election (ODNI & FBI & CISA, 2024).
- Russian influence operations targeting former U.S. Vice President, Kamala Harris, with staged videos (MSTI, p.4, 2024b).
- Misappropriated content from European fashion influencers falsely endorsing the U.S. President, Donald Trump (Strick, 2024).
- Fabricated celebrity quotes promoting pro-Russian narratives (The Insider, 2023).

While conventional techniques persist, influence operations are poised to fully exploit advancements in Generative AI. This approach is almost certain to make discerning fact from fiction all the more challenging for voters in the future but will also continue to exhaust the resources of fact-checking teams and disinformation researchers.

In 2024, a Chinese influence operation, tracked by Microsoft Threat Intelligence (MSTI) as Storm-1376, launched a campaign harassing Canadian politicians on social media and circulating AI-generated videos promoting inflammatory rhetoric against the Canadian government (MSTI, p.7, 2024a). Canadian politicians were targeted again in April and May 2024 by inauthentic accounts using AI-generated avatars, this time with various Islamist related messages (Chenrose, 2024).

Specific Targeting of Diaspora in Political Organizations

Individuals who are both members of diaspora communities and political organizations face an elevated risk and may become the target of more focused and language-specific attacks. For example, Joe Tay, a Conservative Party candidate critical of China's stance on Hong Kong, ran in the Don Valley North riding in Toronto during the 2025 Canadian federal election. He was targeted by a Chinese-led influence operation aimed at Chinese-speaking audiences, seeking to undermine his candidacy and suppress criticism of the Chinese regime.

Figure 7 - An example Facebook post of the influence operation targeting Chinese speaking audiences undermining Joe Tay's candidacy (Privy Council Office, 2025)

A visual representation of influence operations and their targets within the current election interference threat landscape is provided below. This framework will be expanded throughout the report to include the remaining threats to elections.

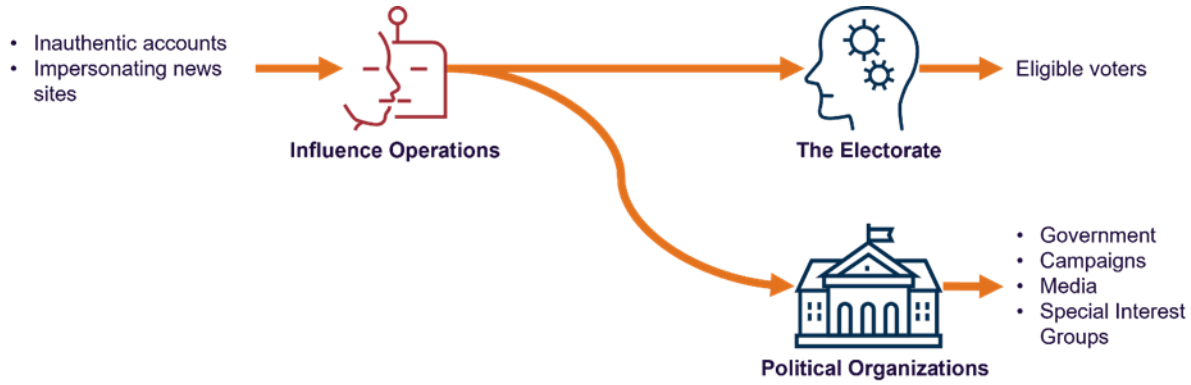

Figure 8 - First flow diagram of the current threat landscape of election interference, highlighting how influence operations are typically conducted and what they target.

Cyberattacks: Digital Threats to Election Integrity

While influence operations remain the most complex threat to elections, cyberattacks continue to be a major component of the threat landscape. Often launched in coordination with influence operations as a force multiplier, these attacks are designed to either uncover useful sensitive data, or to cause general disruption. Though not exclusive to election periods, cyberattacks frequently intensify in the lead-up to and during elections to maximize their impact (Appendix B(ii); Ilascu, 2024; An, 2024; Matishak, 2024).

The most prominent tactic in election-related cyberattacks is the **hack-and-leak** operation. Typically conducted by nation-state threat actors, these attacks target **political organizations** to exfiltrate sensitive data, which is then passed to influence operations to undermine public trust or discredit candidates. A defining case involved the Russian threat actor group linked to the General Staff Main Intelligence Directorate (GRU), known as APT28, which breached the internal mailboxes of the Clinton campaign ahead of the 2016 U.S. election, leaking them via other state groups and third-party actors (FireEye, p.5, 2017). Similar attacks have impacted elections in France in 2017, the UK in 2019, and the U.S. again in 2020) (O'Neill, 2017; GOV UK, 2023; Burt, 2020). Most recently, in August 2024, Iran was accused of leaking sensitive files related to then-U.S. Vice Presidential candidate JD Vance, likely aimed at disrupting the Republican re-election campaign (Isenstadt, 2024).

Nation-state actors also target **election infrastructure**, with the most common targets being voter registration databases, absentee ballot portals, and platforms for electoral communications. These attacks can serve dual purposes: enabling espionage (National Cyber Security Centre UK, 2024) and facilitating highly targeted influence operations. In 2020, an Iranian threat actor group linked to the Iranian Revolutionary Guard Corps (IRGC) compromised U.S. voter databases. The stolen data contained personally identifiable information (PII) that was used to send emails and social media messages containing threats of physical violence to intimidate voters and officials (U.S. Department of Justice, 2021).

Electronic voting machines are also part of election infrastructure, but are not currently in use in Alberta's provincial elections (Wearmouth, 2024), or in Canada's federal elections (Elections Canada, 2024). There are also no credible reports of their compromise leading to any changes in election outcomes.

Cybercriminals: A Burr Under the Saddle of Elections

Political organizations and election infrastructure are increasingly targeted by cybercriminals, particularly **ransomware** operators and **hacktivists**. Ransomware attacks are heavily directed at government entities, particularly at the municipal level, and pose an indirect yet significant threat to the election systems held by these organizations by encrypting critical data and disrupting access to essential networks. Hacktivists, meanwhile, often carry out Distributed Denial of Service (DDoS) attacks and deface websites to temporarily disable online services and damage the reputation of electoral institutions, preferring to target federal systems for increased notoriety. Both attacks risk undermining public trust in the systems supporting democratic processes.

While ransomware groups and hacktivists were traditionally viewed as separate from state operations, compromising organizations in pursuit of financial or political aims, they are increasingly co-opted by nation-state threat actors to bolster their ranks, leveraging them for cyber sabotage while providing plausible deniability of state involvement (CyberAlberta; 2025, Resecurity, 2024; ASERT Team, 2024; Jones, 2024).

Although cybercriminals cannot disrupt the core functions of voting or vote counting directly (FBI & CISA, 2024), their operations have interfered with critical election processes, including voter registration and absentee ballot verification (Abrams, 2020; National Intelligence Council, 2021; BBC, 2022). These attacks can also disrupt the flow of official updates, creating gaps that threat actors can exploit with false narratives, such as fake bomb threats intended to deter voter turnout in target regions (FBI, 2024). In environments where trust in elections is already fragile, these incidents further erode public confidence and place significant pressure on defenders of political organizations and election infrastructure to uphold cybersecurity.

Insider Threats: Interference Behind the Polling Curtain

Beyond external actors, cyberattacks on election infrastructure and political organizations can also emerge from insider threats. Individuals with privileged access can intentionally or negligently compromise the confidentiality of voter data (Layne, 2024), election integrity (CISA et al., 2024), or the availability of systems (Birkeland, 2024).

"The system is only as secure as the people who are entrusted to keep it secure" (Cross, 2022).

Following the 2020 U.S. election, disinformation regarding electoral fraud contributed to at least eight known insider incidents, involving the tampering of voting machines, data, or system access across several states (Ulmer & Layne, 2024). These cases demonstrate the potential impact of insider threat, but also underscore how influence operations not only polarize voters, but also radicalize election workers, forcing a requirement for robust vetting of members of staff in political organizations as well as strong physical security for election infrastructure.

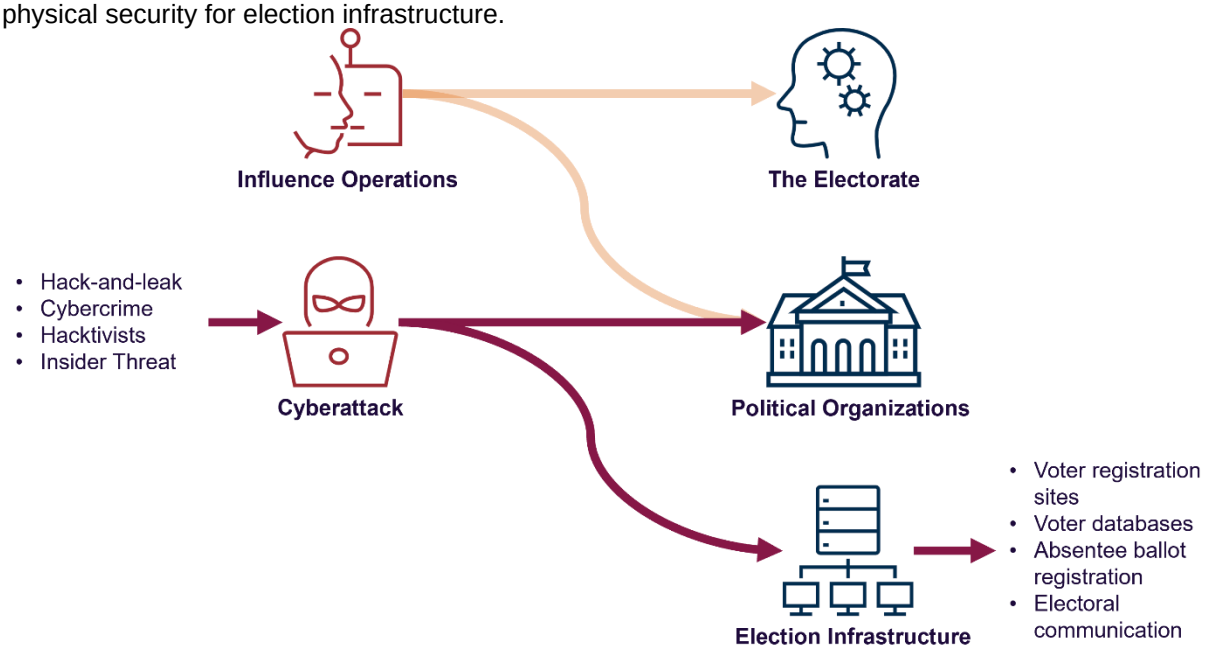

Figure 9 - Second flow diagram of the current threat landscape of election interference, highlighting the typical types of cyberattacks that are launched at political organizations and election infrastructure.

Covert Operations: Human Agents Subverting Democracy

The final major threat to elections is **covert operations**, which are clandestine activities carried out by human agents acting under the guise of legitimate roles including diplomats, embassy staff, or business personnel. These agents are tasked with influencing **the electorate** and members of **political organizations**, using deception or coercion to manipulate behaviour in favour of a foreign state's strategic interests.

Covert operations often focus on vulnerable members of **diaspora communities**, employing tactics such as financial incentives, revocation of rights, or even threats of physical violence to shape electoral outcomes. Members of political organizations are also targeted in similar ways, but in some cases, coercion is exerted through seemingly benign relationships that evolve into pressure to support preferred candidates or policies (Saito, 2024; Tang, 2024).

Testimonies presented during Canada's public inquiry into foreign interference highlighted intelligence-based allegations of covert operations involving China, India, and Pakistan targeting previous Canadian federal elections. According to the Commission's initial report, intelligence suggested that Indian actors may have offered financial support to Canadian politicians in an effort to influence Canada's position on Sikh separatism. Pakistan was similarly alleged to have mobilized members of the South Asian diaspora to promote candidates perceived as more aligned with its interests. While these claims were brought forward during the inquiry, the Commission noted that it was not in a position to independently verify the intelligence. In anticipation of such threats, Canada implemented a Threat Reduction Measure (TRM)

prior to the 2019 federal election, which helped mitigate risks by alerting targeted communities (Hogue, 2024b).

While no confirmed covert operations have been documented either targeting Albertans, or occurring in, Alberta, Canadian Security Intelligence Services (CSIS) has described “Canada and specifically Alberta [as a] very attractive target" for foreign agents conducting covert operations (Black, 2024). Alberta’s economic strength, energy resources, and sizable diaspora populations (including the second-largest Pakistani-Canadian community, and significant Russian, Chinese, Indian, and Iranian populations (Statistics Canada, 2021)) make it particularly attractive to foreign actors. Canada's geopolitical positions and vocal stance on sensitive global issues may also invite coercive pressure on diaspora communities. These communities should be made aware of covert tactics such as bribery, intimidation, or threats to family members, which may be used to sway voter behaviour.

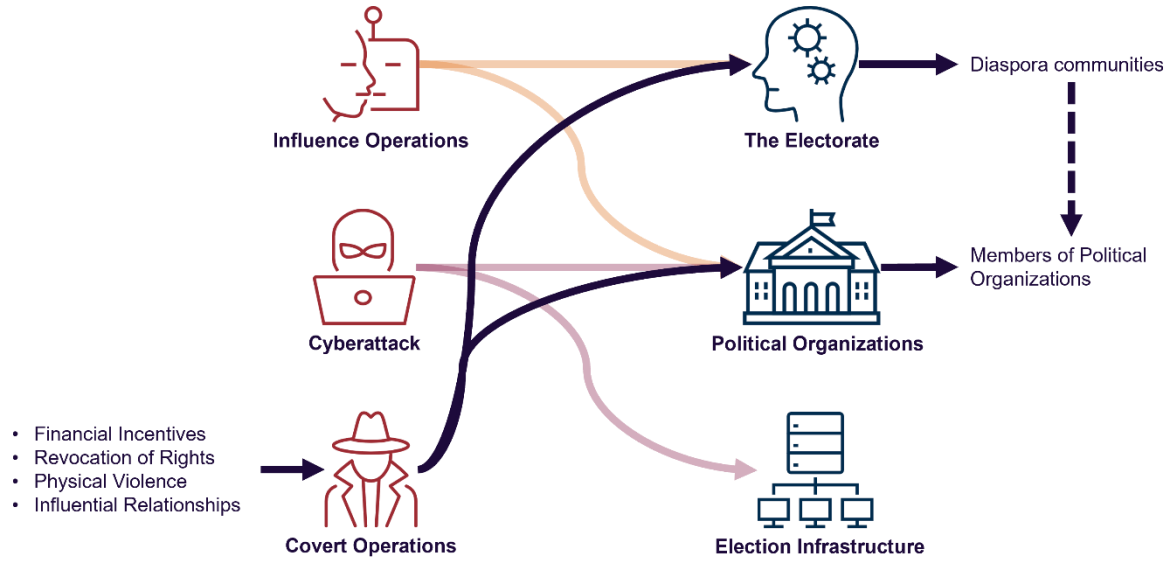

Figure 10 - Third flow diagram of the current threat landscape of election interference, highlighting the typical actors behind covert operations and their targets.

Recommendations for Combating Election Interference

Election interference poses risks to political stability, operational continuity, and public trust. Mitigating these threats requires a comprehensive, multi-layered approach, particularly against influence operations, which represent the most persistent and complex challenge.

Influence Operations

Increase Awareness and Resilience

- Media literacy must be strengthened to appropriately meet the modern and constantly evolving threat of disinformation.
- Pre-bunking can proactively educate voters ahead of elections on issues likely to be weaponized through emotionally charged narratives.
- Regularly monitoring trusted fact-checking services offers insights into the tactics, techniques, and procedures (TTPs) used in influence operations.
- Perspective-taking can help individuals trial alternative viewpoints on divisive issues, helping to reduce polarization and close societal divides.

Use Trusted Information Sources

- Refer to official election sites, such as Elections Alberta, as the primary source of provincial election information.
- If unavailable, verify election-related content through multiple reputable sources before sharing.

Measures to Mitigate the Spread of Disinformation

- Remove unused or inactive social media accounts to reduce risk of takeover and misuse.
- Report misleading or suspicious content to platform moderators if available, or to appropriate authorities.
- Support and participate in community-based education initiatives (e.g., workshops, awareness campaigns, online quizzes).

The Government of Canada provides additional guidance and resources for identifying online disinformation.

Cyberattacks

The US Cybersecurity & Infrastructure Security Agency (CISA) provides tips to help election networks protect and respond to cyberattacks. CISA, along with its partners, has also provided comprehensive guidance on mitigating insider threats.

Covert Operations

For further insight into covert threats targeting Canadian election, review the unclassified reports published by the SITE Task Force.

Conclusion

At a minimum, Alberta is likely to remain a secondary target of foreign influence operations aimed at undermining the federal government, an ongoing risk that threatens to degrade the province's societal cohesion. However, as an appealing target in its own right, Alberta faces the realistic possibility of direct interference in the 2027 provincial elections. Furthermore, as the province moves toward an uncertain political future, including the possibility of a formal separation referendum, the threat of election interference could intensify. A referendum would likely draw international attention, and with it, increased disingenuous influence.

Meanwhile, Generative AI is rapidly improving its capabilities, outpacing the development of governance and policy safeguards. This widening gap creates fertile ground for further misuse of Generative AI, enabling the production of divisive content that blurs the line between disinformation and truth. At the same time, social media algorithms, engineered for engagement over integrity, amplify emotionally charged and divisive content, with little to no incentive for reform. Together, these factors enable malicious actors, both foreign and domestic, to more effectively undermine democratic processes and overwhelm already strained fact-checkers and disinformation researchers.

In light of these risks, there is an urgent need to foster an informed electorate through enhanced media literacy. Voters must be equipped to critically assess digital content and resist manipulative narratives designed to deepen societal divides. At the same time, political organizations and election infrastructure must be secured against cyberattacks to ensure the confidentiality of voter data and uphold public trust in the integrity of democratic processes. Finally, Alberta’s most vulnerable communities must be protected from covert influence operations, ensuring free and fair elections remain accessible to all eligible voters.

Appendix A: Research Into Nation-States Targeted by Election Interference

To quantify the number of elections in 2024, data from the National Democratic Institute (NDI) and the International Foundation for Electoral Systems (IFES) was cross-referenced. It was determined that 65 nation-states, plus the European Parliament, had held elections in 2024.

To further profile likely targets of election interference, open-source data was investigated to identify which of the 65 nation-states were reportedly targeted by foreign interference, the type of election they held, and whether they belonged to a formal alliance group, specifically NATO or the EU.

The table below breaks down election interference by the type of election and by NATO or EU membership.

When analyzing all nation-states holding elections in 2024, it was found that 24 out of 65 (37%) had reportedly been targeted by foreign interference. This percentage stayed consistent when analyzing the reports of interference by election type:

- Head of state elections: 17 out of 41 (41%)
- Upper house of parliament: 2 out of 7 (28%)
- Lower house of parliament: 3 out of 11 (27%)
- Local government: 2 out of 6 (33%)

When analyzing election interference in nation-states that are members of either NATO, the EU, or both, it was found that 13 out of 16 (81%) nation-states in this group had reportedly been targeted by foreign interference. Analyzing this group of nation-states by election type considerably narrows the sample size, but does suggest that some elections are more likely than others to be targeted when it comes to NATO and EU members:

- Head of state elections: 7 out of 8 (88%)
- Upper house of parliament: data sample size of two considered too small.
- Lower house of parliament: 3 out of 3 (100%)
- Local government: 2 out of 3 (66%)

When analyzing election interference in nation-states that are not members of either NATO or the EU, it was found that 11 out of 49 (23%) nation-states in this group had reportedly been targeted by foreign interference, with the following variances observed among different types of elections:

- Head of state elections: 10 out of 33 (27%)
- Upper house of parliament: 1 out of 5 (20%)
- Lower house of parliament: 0 out of 8 (0%)
- Local government: 0 out of 3 (0%)

Appendix B: Case Studies of Notable Incidents Targeting Elections

Appendix B(i): Influence Operations - The Slovakian Slow Burn

Since as early as 2014, Russian state actors have compounded influence operations that have significantly misled the Slovak information landscape (Ružičková, 2023). Initially, the focus was on

spreading false narratives about Ukraine, portraying Russia as a victim of Western encroachment. This portrayal aimed to cultivate pro-Russian sentiments and undermine trust in Slovakian leadership.

Russian influence in Slovakia has been bolstered by local sympathizers who amplify Kremlin narratives, helping to legitimize Russia's actions. These domestic actors contribute to a fragmented information environment, making it easier for Russian disinformation to resonate with the Slovak electorate.

The Russian embassy in Slovakia has been particularly active in spreading disinformation, using its social media presence to push pro-Kremlin narratives. They attempted to distract from Russian war crimes by spreading false claims about local incidents, such as the alleged destruction of a Russian soldier cemetery in Ladomirova (Dubóczi, 2022).

Disinformation recently helped install Slovakian Prime Minister Robert Fico, who is considered to be more agreeable to Russia's interests. During the 2023 parliamentary elections, Russian influence operations amplified anti-Western sentiments, targeting Slovaks' skepticism towards NATO and the EU (Bonney, 2024). These narratives were leveraged by Fico with the Smer-SD party, helping secure a victory and implement policies that aligned more closely with Russian interests.

Just two days before the 2023 elections, AI generated audio was used to greatly undermine Fico's opponent, Michal Šimečka. In the fabricated recording, Šimečka's voice could be heard discussing election rigging strategies (Meaker, 2023). Although the recording was eventually discredited, its initial impact—fueled by widespread dissemination so close to election day—contributed to Fico's success.

"[S]ociety has two poles ... There are people who love [Fico] and there are others who hate him" ("Lenka", 2024, as quoted in Gyori, Stezycki, & Lopatka, 2024)

Russian influence operations continued into the new year, influencing the outcome of the 2024 Slovakian presidential election via disinformation. False claims about military conscription and involvement in Ukraine were spread to sway public opinion in favour of Peter Pellegrini, a candidate aligned with Fico's policies (Hockenos, 2024).

The polarization that Russian disinformation had aided up until this point boiled over on 15th May 2024, when Fico was shot and critically injured by Juraj Cintula, a 71-year-old man who claimed to have acted primarily due to Fico's opposition to Ukrainian assistance (Nicholson, 2024). The events in Slovakia underscore the profound impact disinformation can have on political landscapes and voter behaviour.

"Everyone is tense ... It's more and more aggressive, but I don't think it's only in Slovakia, but worldwide" ("Veronika", 2024, as quoted in Gyori, Stezycki, & Lopatka, 2024).

Appendix B(ii): Cyberattacks combine with Influence Operations to Impact the 2024 Romanian Presidential Election

In November 2024, Romania's election infrastructure was targeted by a wave of cyberattacks amidst the country's presidential election. Over 85,000 attacks began 19th November 2024 and ended the day after the first round of elections on 25th November 2024, targeting systems owned by the Permanent Electoral Authority (AEP). The widespread attacks originated from devices in 33 different countries and sought to compromise election data, deny access to systems, and contribute to an erosion of trust. While the Romanian Intelligence Service (SRI) did not formally attribute the attack, they noted that the scale and tactics are indicative of nation-state activity, with Russia identified as the likely culprit given its history of election interference in the region (Ilascu, 2024; SC Media, 2024).

The attackers had initially compromised a public facing server used for storing mapping data which was also connected to the AEP's internal network, providing the attackers the opportunity for lateral movement to more sensitive network environments. After gaining a foothold into the AEP's private systems, the attackers began targeting legitimate user accounts, exploiting vulnerabilities affecting other servers, and

launching SQL injection and cross-site scripting (XSS) attacks. In doing so, the attackers were able to gain access to further systems, and compromise credentials for multiple electoral websites, including those used to provide voter registration services and the Central Election Bureau.

SRI assess the intended impact of this campaign was to not only gain access to the election infrastructure, but to also deny its use by the public, and alter important public information regarding the electoral process. The compromised credentials were subsequently leaked on a cybercriminal forum that caters to a Russian speaking audience.

This large-scale cyberattack occurred in parallel to ongoing influence operations targeting the 2024 Romanian presidential election. SRI and Romania's Ministry of International Affairs (MAI) revealed that over 100 Romanian TikTok influencers were paid to promote the presidential candidate Călin Georgescu, a known NATO critic (Ilie, 2024). The operation used previously dormant accounts, with some registered as far back as 2016, to rapidly amplify narratives supporting Georgescu in the weeks leading up to the election, violating both TikTok's policies and Romanian election law. These efforts have been widely attributed to causing Georgescu's unexpected victory in the first round of the Romanian presidential election, despite his prior lack of political prominence.

Following the discoveries of interference, Romania's constitutional court ruled to annul the election, marking an unprecedented decision in response to influence operations and cyberattacks targeting elections (Martin, 2024; Lakshmanan, 2024). The decision has led to the entire election being rescheduled for May 2025 and prompted questions over how targeted nation-states should handle election interference. The European Commission also ordered TikTok to preserve election-related data to enable investigations, citing concerns over "systematic inauthentic activity" (Martin, 2024).

Although the influence operation had likely impacted the election outcome more significantly, the cyberattacks undoubtedly complicated matters and further undermined public trust in the election process. How the attackers progressed through the AEP's infrastructure is a reminder of the importance of network segmentation and removing internet access from systems that do not require it, thus limiting the attack surface of election infrastructure. The influence operation highlights the need to fully remove dormant accounts to reduce resources at the interferer's disposal. This case also highlights how cyberattacks and influence operations are increasingly deployed in tandem to manipulate election outcomes, and often ramp up in the immediate run up to an election.

Appendix B(iii): The Fox Guarding the Henhouse - Insider Threat in the 2020 U.S. Presidential Elections

One of the most significant incidents of insider threat election interference from the 2020 US presidential election was the case of Tina Peters, the former county clerk of Mesa County, Colorado. Peters was convicted on multiple counts related to tampering with election infrastructure (Looker, 2024).

The interference began when Peters allowed an unauthorized individual, Conan Hayes—an associate of conspiracy theorist Mike Lindell—access to Mesa County's election equipment. Peters used someone else's security badge to conceal Hayes' identity and facilitate this breach. Her actions included permitting the unauthorized copying of hard drives from voting machines during a software update, which were later posted online.

Peters gathered and distributed sensitive election data to promote false claims of election fraud that she believed to be true. Her actions were driven by disinformation regarding false claims of election fraud during the 2020 U.S. presidential election, fueling what was described as a "fixation" on proving these claims and gaining notoriety, as she became entangled with figures and narratives questioning the election's integrity.

This compromise led to a ban on using the tampered voting equipment for the fall 2021 election in Mesa County (Birkeland, 2021). Although there was no immediate evidence of altered election results, the breach contributed to the dissemination of confidential information and heightened concerns about the integrity of election processes.

Peters' case, resulting in her conviction on seven out of ten charges, highlights how individuals with access and influence within election systems can exploit their positions to further partisan agendas. This poses risks to both the integrity of elections and public confidence in their outcomes.

Glossary

Term	Definition
Artificial Intelligence (AI)	A broad field in computer science that involves the simulation of human or human-like knowledge, reasoning, synthesis, or inference by computers.
Breach	Unauthorized access, acquisition, or disclosure of sensitive or confidential information, including personal data, financial information, intellectual property, or other data intended to be kept private.
Covert Operations	Concealed activities conducted by human agents to influence the outcome of an election in favour of the sponsor of the operation.
Cyberattack	A deliberate attempt by a cyber threat actor to either disrupt or gain unauthorized access to digital systems.
Deepfake	The use of an AI algorithm to manipulate existing media (e.g., video, photos, audio) to create new media depicting events that did not take place or occurred differently.
Diaspora	Members of a national population who no longer reside in their homeland, sometimes referred to as expatriates or transnational communities.
Disinformation	False information shared with the intent to cause harm.
Distributed Denial of Service (DDoS)	A cyberattack where a server is flooded with internet traffic to render it inaccessible.
Election Interference	Deliberate efforts to manipulate the outcome of elections or undermine their integrity.
Espionage	The act of covertly infiltrating a target to gather intelligence.
Generative Artificial Intelligence	A form of AI that can produce various media such as text, images, audio, and video based on data provided by the owner or user of the model.
Hack-and-Leak Attack	A type of cyberattack where any data that is compromised as a result of the attack is disclosed to the public, typically with the intent to cause reputational

	damage to those implicated in the data, or it's custodians.
Hacktivist	A type of threat actor that uses cyberattacks to achieve politically motivated goals.
Influence Operations	Deliberate efforts to manipulate voter behavior with disinformation, subsequently influencing election outcomes, typically delivered online via social media.
Infrastructure	The combination of hardware and software elements that enable network connectivity.
Insider Threat	The potential for an insider to use their authorized access or understanding of an organization to harm that organization (CISA).
Nation-State Threat Actor	A threat actor that officially operates at the behest of a nation-state, typically known for having advanced capabilities.
Personally Identifiable Information (PII)	Information that is either related to or can identify and individual.
Ransomware	A specific type of malware designed to encrypt all files on a target system, preventing access until a payment is made to the attacker to acquire the decryption key.
Threat Reduction Measure (TRM)	A tool used by Canadian Security Intelligence Services (CSIS) to disclose classified information to potential targets to raise their awareness of a particular threat.