

Safeguarding Canadian Democracy: Confronting Foreign Interference and Disinformation

Acouamela Amandé and Kiara Yllescas

Issue

Safeguarding Canadian democracy requires urgent, coordinated strategies to counter threats posed by foreign interference — including disinformation and artificial intelligence (AI)-driven media manipulation, such as the use of algorithms, deepfakes, and automated bots to spread false or misleading content that undermine the integrity of Canadian elections.

Background

Foreign interference, utilizing media manipulation and AI now presents an unprecedented threat to Canada's democratic governance. Recent federal elections have exposed critical gaps in Canada's capacity to respond swiftly and effectively to these challenges. Hogue (2025,2) highlighted several shortcomings that impair Canada's ability to "deter, detect and counter" threats to electoral integrity (Hogue 2025, 2).

Canada is a democratic, open society renowned for its welcoming and tolerant stance. However, foreign states and proxies exploit this openness through deception in the information space to undermine Canadian democracy and advance strategic interests at Canadians' expense. This constitutes foreign interference and poses a serious national security threat.

The Canadian Security Intelligence Service (CSIS) continues to observe steady — and in some cases

intensifying — foreign interference by state actors against Canada (CSIS, 2025). These campaigns target all facets of society, with a particular focus on democratic institutions and processes. Wesley Wark (2024) explains the insidious nature of this threat: "Foreign interference targeting democratic societies works not by the classic Orwellian formula of ruthless powers limiting sources of information and knowledge...but by producing an opposite effect. The opposite effect is multiplying and amplifying chosen channels of information and attempting to corrupt the availability of true information in favor of that which is both false and harmful."

Such campaigns are designed to exploit societal divisions, erode public confidence in institutions, and influence political outcomes in ways that serve foreign interests. Recent media coverage — particularly allegations of interference by China — has heightened public awareness (Hogue, 2025). Research on the disinformation surrounding Kenny Chiu's 2021 Foreign Influence Registry Act demonstrates how its false framing as a measure targeting the Chinese community fostered confusion and suspicion within diaspora communities. The result was a weakening of trust in democratic processes and a suppression of informed public debate (Lee & Fung, 2022). This case illustrates how targeted disinformation can manipulate public perception, drive social polarization, and exploit vulnerabilities in a country's communication infrastructure. Canadians have often turned to mainstream media for clarity, as the Government of Canada has not

maintained a sufficiently visible or consistent role in public communication (ibid.). This gap reflects the inherent challenges of handling sensitive intelligence and the complexities of attribution.

Addressing these threats necessitates a proactive, transparent and coordinated response. One such tool is the Rapid Response Mechanism (RRM) — a Canadian-led Group of Seven (G7) initiative established in 2018 to monitor and counter foreign interference in democratic processes (Global Affairs Canada 2021). The RRM leverages open-source intelligence to raise awareness while protecting classified information. Enhancing and elevating the RRM's role could enable Canada to better inform citizens and strengthen resilience against foreign interference.

The Hogue Commission

In 2023, the Canadian government took a decisive step by establishing the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, led by the Honourable Marie-Josée Hogue. This marked Ottawa's formal acknowledgment of public concern over foreign meddling (Hogue 2024). The inquiry followed reports of interference by Russia in the 2016 US and French elections and, more recently, Chinese interference in Canada's 2019 and 2021 federal elections (ibid.; Runciman and Baker 2017).

The inquiry's mandate was to assess Canada's capacity to “detect, deter and counter” foreign interference, revealing significant gaps in the national security apparatus (Hogue 2025, 2). The 2019 election case study highlighted Chinese influence efforts, including allegations of Chinese officials pressuring students, influencing candidate nominations and indirect financial support for certain candidates. Interference efforts also involved the *Buffalo Chronicle* disinformation campaign. While these did not sway the overall election outcome, they likely influenced specific ridings and damaged public trust, especially among diaspora communities.

Similarly, the 2021 election case study identified interference involving China, India and Russia. Alleged activities included misinformation targeting the Conservative Party and MP Kenny Chiu, covert financial support and influence in key ridings. Again, these efforts did not alter the election outcome but did impact public confidence and community trust (ibid. 2025).

A key finding was the government's inadequate response capacity, especially via the RRM, which failed to serve as an effective alerting or coordination tool during critical periods (BBC 2022). Prime Minister Trudeau publicly acknowledged China's “aggressive games,” but the delayed response underscored a need for greater operational visibility and responsiveness.

The Hogue Report

On January 28, 2025, the Public Inquiry released its final report, confirming foreign interference in the 2019 and 2021 elections. It found that interference, while not altering the election results, posed an “existential threat” to Canada. The report identified bureaucratic shortcomings, including slow responses, fragmented intelligence sharing and insufficient public communication (Hogue 2025).

Other key findings include:

- No evidence of “traitors” in Parliament conspiring with foreign states.
- Some parliamentarians engaged in questionable conduct but not outright treason.
- The primary threat is the spread of misinformation and disinformation through media and social networks.
- Transnational repression against diaspora communities in Canada is a significant concern.
- The intelligence delivery system has been restructured but remains untested (ibid.).

2025 — Additional Developments

The *Cyber Threats to Canada's Democratic Process: 2023* (Canadian Security Establishment [CSE] 2023) report identified technological interference as an emerging threat to Canada's democratic processes. Since then, this threat has intensified with the rapid growth of generative AI. Between 2023 and 2024, the number of reported cases involving AI-driven election interference increased to 102 cases across 41 elections worldwide — up from just one case during 2021–2023 — driven by improvements in the quality, affordability and accessibility of AI technologies (CSE 2025, 3).

In their 2025 report, the CSE warned that foreign state actors are actively deploying AI for public opinion manipulation, disinformation and social polarization

(Government of Canada 2025). This development marks a dangerous escalation: AI enables the creation of quicker, more captivating content, which complicates detection and response efforts. Commissioner Hogue has described this manipulation as an “existential threat” to Canada. However, she also noted that Canada’s bureaucratic response remains too fragmented and slow. The widening gap between the agility of foreign adversaries and the institutional capacity of Canada jeopardizes the integrity of upcoming elections (Hogue, 2025).

Recommendations

RRM public attribution protocol. The federal government should develop a clear, evidence-based protocol for publicly attributing foreign interference, ensuring consistency across G7 states. It should create criteria and evidence standards to determine when and how to publicly attribute threats. The RRM should include a tiered attribution system: low-confidence threats are flagged internally, while high-confidence threats are disclosed publicly with evidence. Cautiously leveraging AI technologies, the RRM should analyze large data sets and assess threats, guided by a threat model (Blais-Savoie 2025). Given Canada’s leadership role in the RRM, it can spearhead the development of international attribution standards.

Education and public awareness strategy. The Government of Canada should establish a non-partisan oversight body (for example, ombudsman) to validate attribution claims before public release, ensuring transparency and credibility. The body should incorporate media literacy education into school curricula and higher education programs, focusing on foreign tactics, AI disinformation and election security. It should also launch a public education campaign modelled after successful initiatives such as TVO’s *Big [If True]* television series, which effectively communicate complex threats in an engaging manner (TVO Media Education Group, 2024).

About the Authors

Acouamela Amandé is a student in Wilfrid Laurier University’s Master of International Public Policy program, based at the Balsillie School of International Affairs.

Kiara Yllescas is a student in Wilfrid Laurier University’s Master of International Public Policy program, based at the Balsillie School of International Affairs

Acknowledgements

The authors would like to thank Justin Dell and Professor Wesley Wark for their guidance and mentorship throughout the course of the fellowship program.

Works Cited

- BBC. 2022. “Trudeau accuses China of ‘aggressive’ election interference.” November 8. www.bbc.com/news/world-us-canada-63551134.
- Blais-Savoie, Fabrice. 2025. “Algorithmic Intelligence: A Solution to Canada’s Capacity Constraints?” Unpublished Manuscript.
- CSIS. 2022. *CSIS Public Report 2022*. www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2022.html.
- CSIS. 2025. *Foreign interference threats to Canada’s democratic process*. Government of Canada. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html>
- CSE. 2023. *Cyber threats to Canada’s democratic process: 2023 update*. <https://www.cyber.gc.ca/sites/default/files/cyber-threats-canada-democratic-process-2023-update-v1-e.pdf>
- CSE. 2025. *Cyber Threats to Canada’s Democratic Process*. www.cyber.gc.ca/sites/default/files/tdp-2025-e-v1.pdf.
- Hogue, Marie-Josée, 2025. *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions – Final Report*. Privy Council Office, Government of Canada. https://foreigninterferencecommission.ca/fileadmin/report_volume_1.pdf.

Global Affairs Canada. 2021. *G7 Rapid Response Mechanism Annual Report 2021*. www.international.gc.ca/transparency-transparence/assets/pdfs/rapid-response-mechanism-mecanisme-reponse-rapide/g7-rrm-2021-annual-report-en.pdf.

Lee, S.-F. and Fung, B. 2022. “Misinformation and Chinese interference in Canada’s affairs.” *Policy Options*. <https://policyoptions.irpp.org/magazines/january-2022/misinformation-and-chinese-interference-in-canadas-affairs/>

Runciman, Bob and George Baker. 2017. *Controlling Foreign Influence in Canadian Elections*. Report of the Standing Senate Committee on Legal and Constitutional Affairs. https://sencanada.ca/content/sen/committee/421/LCJC/reports/Election_Report_FINAL_e.pdf.

TVO Media Education Group. (2024). *TVO’s new show ‘Big [If True]’ tackles mis- and disinformation with award-winning journalist Molly Thomas*. TVO. <https://tvo.me/tvos-new-show-big-if-true-tackles-mis-and-disinformation-with-award-winning-journalist-molly-thomas/>

Wark, Wesley. 2024. “Foreign Interference Online: Where Disinformation Infringes on Freedom of Thought.” In *Legitimate Influence or Unlawful Manipulation*, 1-8. Waterloo, ON: CIGI. www.cigionline.org/publications/foreign-interference-online-where-disinformation-infringes-on-freedom-of-thought/