Democracy and You: A Handbook for Detecting and Preventing Foreign Interference in Canadian Elections

Marcus Kolga

Foreign Interference Resilience & Education
An initiative by Digital Public Square

disinfowatch

DIGITAL
PUBLIC
SQUARE

About

Digital Public Square is a Toronto-based not-for-profit whose objective is to rethink and redesign the way technology is used to support communities worldwide. We find ways for communities to engage in healthy debate, share knowledge, and co-create solutions to their most pressing challenges. Over the past decade, Digital Public Square has created space for tens of millions of people around the world to interact with our platforms. Our products have been deployed in a wide range of contexts, from countering misinformation in North America to increasing knowledge of labor rights in Asia and strengthening election integrity in Africa.

Marcus Kolga is the founder and director of DisinfoWatch, a leading Canadian platform dedicated to monitoring and debunking foreign disinformation. As an expert in digital communications, global human rights, sanctions, disinformation, and cybersecurity, Marcus leverages his expertise to combat foreign influence operations. DisinfoWatch relies on open-source data, contributions from an international network of journalists, civil society organizations, analysts, and some automated tools. This information is analyzed and exposed to raise awareness about foreign operations and to build long-term resilience against foreign information and influence campaigns. The platform's core mission is to enhance public understanding of foreign information operations by uncovering who produces it, who amplifies it, why it is created, how to recognize it, and how to prevent its spread.

Research for this report was supported by Heritage Canada's Digital Citizen Contribution Program.

This project has been made possible in part by the Government of Canada. Ce projet a été rendu possible en partie grâce au gouvernement du Canada.

Canada

What is Foreign Interference?

Foreign interference in Canadian democracy and elections happens when foreign governments try to manipulate public opinion and influence how people vote to advance their own interests. This includes spreading false or misleading information online, hacking political parties or election systems, and even pressuring members of some ethnic communities to vote a certain way through threats or intimidation.

Countries like China, Russia, and Iran are the most prominent governments to use these tactics to manipulate Canadian democracy and push their own agendas. The government of Canada and civil society groups are working to address foreign interference to strengthen the resilience of our democracy, fight disinformation, and protect vulnerable communities from foreign influence.

In Canada, foreign interference efforts have targeted federal, provincial, and even municipal elections.

Maintaining the integrity of our elections is fundamental to ensure a healthy and functioning democracy. It is essential for voters, activists, journalists, candidates, and political parties to recognize interference tactics and take steps to counter them. This handbook provides an overview of key interference tactics, real-life case studies, and practical steps for spotting, reporting, and defending against these threats.

How Actors Interfere in Our Democracy & How to Respond

Disinformation & Information Manipulation

Disinformation is false and misleading information that is intentionally created to manipulate public opinion, often by foreign governments or actors aligned with them in Canada. These actors may also amplify false or misleading information through state-controlled media, social media, bots, inauthentic users, and influencers. Their goal may be to discredit certain political parties or candidates, sow confusion and division, or shift policy discussions and debates in favour of foreign regimes.

Where You Might Encounter It:

Here is a **combined, concise list** of where a Canadian voter might commonly encounter foreign disinformation—including Russian, Iranian, and Chinese state-controlled content—as well as fringe extremist websites:

Social Media Platforms

- Large networks (e.g. Facebook, X [Twitter], TikTok, YouTube) can be used by foreign actors or fringe groups to spread disinformation, sometimes via fake accounts, bots, or targeted ads.
- State-controlled websites and their social media channels such as RT (Russia), Press TV (Iran), and CGTN/Global Times (China) may share disinformation or misleading content on their platforms.

Messaging Apps and Private Groups

- Encrypted or closed platforms like **Telegram**, **WhatsApp**, and **WeChat** can host disinformation in semi-private spaces, making it harder for authorities or civil society to monitor.
- Community group chats can further amplify false narratives.

Foreign State-Controlled Traditional and Online Media

- Russian (RT, Sputnik), Iranian (Press TV), and Chinese (CGTN, Xinhua) outlets often push narratives aligned with their respective governments' interests.
- Content from these sources may appear on cable, satellite, or via search engines without clearly indicating state affiliation.

Inauthentic or Partisan Websites (Including Fringe Extremist Sites)

- Websites mimicking legitimate news sources can be funded or controlled by foreign or extremist interests, publishing articles designed to look locally sourced.
- Fringe extremist websites often host conspiratorial or inflammatory content that foreign actors can exploit or amplify to sow division.

Targeted Ads and Aggregation Platforms

- Paid ads on social media, search engines, or aggregator sites can be micro-targeted to specific voter segments, spreading tailored disinformation.
- Manipulative headlines or "clickbait" stories can funnel readers to state-backed or extremist-endorsed propaganda.

By recognizing these common channels—especially those tied to Russian, Iranian, Chinese, or extremist sources—Canadian voters can be more critical of what they read and share, and rely on verified, fact-based reporting.

How Can You Identify It:

- **Check the Source**
  Is the information coming from a credible news organization, an anonymous social media account, or a foreign state-linked outlet? Be cautious of sources with no verifiable reputation.
- **Look for Emotional Manipulation**
  Disinformation often uses inflammatory language, fear, or outrage to provoke strong reactions rather than inform. If a post or headline seems designed to anger or divide, verify before sharing.
- **Verify with Multiple Reliable Sources**
  If major news outlets are not reporting the same claim, it may be false or misleading. Always cross-check information with trusted media and fact-checking organizations.
- **Be Wary of Screenshots & Edited Media**
  Misinformation can spread through fake social media posts, manipulated images, or deepfake videos. If something seems suspicious, search for the original source.
- **Watch for "Too Good (or Too Bad) to Be True" Stories**
  Disinformation often exploits bias by crafting stories that perfectly fit a political agenda. If a claim seems exaggerated or one-sided, investigate further before believing or sharing.

What to Do If You Encounter It:

- Verify sources and check for fact-checking reports before sharing political content.
- Report misleading content on social media platforms and raise awareness of false claims.
- Political parties and candidates should proactively counter false narratives with accurate information.

CASE STUDY: Disinformation Targeting MPs Critical of China

During Canada's 2021 federal election, a coordinated disinformation campaign attempted to discredit MPs seen as critical of the Chinese government. Fake social media accounts spread misleading claims that these MPs were engaging in "anti-Asian racism," an effort aimed at discouraging voters from supporting them while positioning Beijing-friendly candidates as more "inclusive" options.

Covert Funding & Candidate Sponsorship

Foreign states covertly support candidates sympathetic to their interests through undeclared financial contributions, business networks, or community mobilization efforts. Such tactics can give foreign regimes significant influence over Canadian policy decisions. When conducted during an election such support may give a selected target an advantage over their opponents.

What to Do If You Encounter It:

- Political parties must report donations - check the rules.
- If you suspect a violation, report it to Elections Canada, or your local election authorities and your local law enforcement.
- Journalists and researchers should investigate and expose suspicious funding networks.

CASE STUDY: Alleged Covert Foreign Support for Canadian Federal Candidates

A National Security and Intelligence Committee of Parliament report in 2024 stated that members of Parliament "accepted knowingly, or through willful blindness, funds or benefits from foreign missions or their proxies which have been layered or otherwise disguised to conceal their sources". The report included a section about a Liberal Party nomination candidate in the Greater Toronto area who had allegedly received support from the Chinese Consulate. The report states that the candidate's supporters "arrived in buses ... supported by the PRC: between 175 and 200 international Chinese students arrived in several buses. The Consulate reportedly told the students that they must vote for [the candidate] if they want to maintain their student visas."

Harassment & Intimidation of Candidates

Foreign actors use disinformation, threats, doxxing, and smear campaigns to discourage or discredit candidates who criticize their governments. These tactics are often directed at diaspora politicians or MPs advocating for human rights in China or Russia.

What to Do If You Encounter It:

- Candidates should document and report threats to law enforcement and Elections Canada.
- Social media platforms should be used to call out coordinated harassment efforts.
- Political parties must ensure security support for targeted candidates.

CASE STUDY: Chinese Government Pressure on Conservative MP Kenny Chiu

In the 2021 federal election, Conservative MP Kenny Chiu, known for his support of a foreign influence transparency registry, became the target of an online disinformation and intimidation campaign. WeChat messages falsely claimed he was anti-Chinese, leading to a decline in his support among Chinese-Canadian voters. He eventually lost his seat.

Cyber Espionage & Hacking

State-sponsored hackers target political parties, candidates, and government institutions to steal sensitive data, manipulate election outcomes, or discredit public figures.

What to Do If You Encounter It:

- Political parties and election agencies must assess and reinforce cybersecurity measures.
- Use multi-factor authentication and encrypted communication for sensitive campaign work.
- Report suspicious cyber activity to security agencies.

CASE STUDY: Russian Cyber Operations Against Canada's 2019 Election

Ahead of the 2019 federal election, Canadian intelligence officials warned that Russia-linked hackers attempted to breach political party databases and government networks. Although no major breach was confirmed, the attempt reflected the Kremlin's efforts to undermine democratic elections in Western nations.

Transnational Repression Targeting Candidates and Their Supporters

Foreign regimes may target elected officials, candidates, and their prominent supporters with smear campaigns, sanctions, or threats to discourage criticism and influence Canada's foreign policy.

What to Do If You Encounter It:

- Officials should publicly document and denounce these attacks.
- Voters should recognize foreign efforts to discredit Canadian politicians as a form of interference.

CASE STUDY: Russia's Targeting of Chrystia Freeland & China's Targeting of Michael Chong

Deputy Prime Minister Chrystia Freeland has been a frequent target of Russian disinformation, with state-controlled media and online trolls falsely portraying her as a Nazi sympathizer due to her Ukrainian heritage.

Canadian MP Michael Chong was targeted by a Chinese government transnational repression campaign after advocating for Uyghur human rights. Beijing sanctioned him in 2021, and in 2023, reports revealed that a Chinese diplomat in Canada sought to intimidate Chong by gathering information on his family in Hong Kong.

Tip Sheet: How to Counter Foreign Electoral Interference

For Voters: Protecting Your Vote & Recognizing Interference

- **Verify Before You Share** – Disinformation can spread quickly. Always fact-check political claims, especially if they come from unknown sources or foreign media.
- **Be Wary of Divisive Content** – Foreign actors often amplify social and political divisions. If a story is designed to provoke outrage, double-check its accuracy and source.
- **Scrutinize Political Messaging on Private or Semi-Private Chat Apps** – Be cautious of political endorsements or messaging on WeChat, WhatsApp, Telegram, and other closed-group apps where foreign states may influence narratives.
- **Report Suspicious Activity** – If you see clear disinformation, foreign-backed campaigning, or unusual voting pressure in your community, report it to Elections Canada or independent watchdog organizations.
- **Encourage Election Integrity** – Encourage friends and family to stay informed and be aware of attempts to manipulate our information environment by foreign actors.

For Candidates & Political Campaigns: Securing Your Election Effort

- **Secure Your Digital Presence** – Use strong passwords, multi-factor authentication, and encrypted communications for campaign-related work.
- **Vet Your Donors & Supporters** – Be cautious of large donations or offers of campaign assistance from groups with potential foreign ties. Conduct due diligence before accepting support. If you're not sure, check with Elections Canada.
- **Prepare for Disinformation & Smear Campaigns** – Have a strategy to quickly counter false narratives about the candidate or the election platform. Work with fact-checkers and journalists to set the record straight.
- **Engage with Ethnic Communities Directly** – Don't let foreign-controlled messaging dominate the conversation. Proactively and directly reach out to diaspora groups with accurate information.
- **Report Threats & Harassment** – If you or your team are targeted with threats or intimidation, document everything and report it to law enforcement and Elections Canada.
- **Educate Your Team** – Train staff to recognize foreign influence tactics, from social media manipulation to cyber threats.

Tip Sheet: How to Counter Foreign Electoral Interference

For Journalists & Media: Investigating & Reporting Responsibly

- **Identify Foreign-Sourced Narratives** – If a political story is being amplified by foreign state media (e.g. CGTN, RT, Sputnik), investigate its origins before reporting.
- **Fact-Check Viral Political Claims** – Be cautious when covering sensational political accusations that lack verifiable evidence. Check if the claim has been promoted by known disinformation networks.
- **Monitor Targeted Attacks on Candidates** – Be aware of smear campaigns against politicians critical of known perpetrators of foreign interference, such as China or Russia. Report on these tactics as part of a broader foreign interference strategy.
- **Use Open-Source Intelligence (OSINT) Tools** – Investigate social media trends and coordinated amplification using tools whenever possible.
- **Protect Your Own Security** – Journalists covering foreign interference are often targeted by cyberattacks and harassment. Use encrypted communication tools and secure your accounts.
- **Hold Social Media Platforms Accountable** – Push for transparency from platforms about how they handle disinformation and foreign influence operations.

Digital Public Square is a Toronto-based not-for-profit whose objective is to rethink and redesign the way technology is used to support communities worldwide. We find ways for communities to engage in healthy debate, share knowledge, and co-create solutions to their most pressing challenges.

digitalpublicsquare.org
hello@digitalpublicsquare.org

DIGITAL
PUBLIC
SQUARE