

For Public Release



Government
of Canada

Gouvernement
du Canada

Unclassified



SECURITY AND INTELLIGENCE THREATS TO THE ELECTIONS TASK FORCE (SITE TF)

Foreign Interference:
A Threat to Canada's National Security

Canada

For Public Release



Unclassified

Purpose

To provide political parties with a comprehensive and up to date briefing on foreign interference.

Objectives

To provide an overview of:

- SITE TF and posture for by-elections;
- the threat of foreign interference;
- why Canada and who are the targets;
- the prominent threat actors;
- known foreign interference opportunities;
- cyber threat activities;
- risks of violence / violent extremism; and
- how to protect yourselves.

**Canada**

For Public Release





Unclassified



SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE

WHAT ARE WE TALKING ABOUT?
Covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada



	MANDATE/ROLE	ACTIVITIES
 CSE Communications Security Establishment	Information Technology Security <ul style="list-style-type: none"> Providing advice, guidance, and services to help ensure the protection of electronic information and of systems of importance Foreign Intelligence <ul style="list-style-type: none"> Collection of foreign intelligence for Government of Canada on threat actors Supporting CSIS and RCMP <ul style="list-style-type: none"> Providing assistance on technical operations 	<ul style="list-style-type: none"> Providing intelligence and cyber assessments on the intentions, activities, and capabilities of foreign threat actors Protecting Government systems and networks related to elections through cyber defence measures Providing cyber security advice and guidance to political parties, provinces and other institutions involved in democratic processes
 CSIS Canadian Security Intelligence Service	Intelligence and Threat Reduction <ul style="list-style-type: none"> Collection of information about foreign influenced activities that are detrimental to the interest of Canada and are clandestine or deceptive or involve a threat to any person Countering such activities through threat reduction measures Intelligence Assessment <ul style="list-style-type: none"> Providing advice, intelligence reporting and intelligence assessments to Government of Canada about foreign influenced activities 	<ul style="list-style-type: none"> Providing threat briefings and intelligence reporting to Elections Canada and the Commissioner of Elections Providing an assessment of hostile state activity methodologies and capabilities to Government of Canada decision makers
 GAC Global Affairs Canada	Mandate/Role <ul style="list-style-type: none"> Open source research on global trends and data on threats to democracy Partnership with G7 countries to share information and coordinate responses to threats as appropriate 	<ul style="list-style-type: none"> Providing research on disinformation campaigns targeting Canada by foreign actors Reporting on global trends, metrics, and incidents Coordinating attribution of incidents
 RCMP Royal Canadian Mounted Police	Mandate/Role <ul style="list-style-type: none"> The primary responsibility for preventing, detecting, denying and responding to national security-related criminal threats in Canada Investigates criminal offenses arising from terrorism, espionage, cyber attacks, and foreign influenced activities The key investigatory body for Elections Canada if criminal activity is suspected 	<ul style="list-style-type: none"> Investigates any criminal activity related to interference or influence of Canada's electoral processes Works closely in partnership with intelligence, law enforcement and regulatory agencies



For Public Release

Unclassified



Toronto-St. Paul's By-Election: Current posture



- SITE TF stands up for federal by-elections
- Collective monitoring of threat activity
- Internal mechanisms to report and brief (i.e. Deputy Ministers' Intelligences Response and Electoral Security Coordinating Committee)
- Activation of the 24/7 Hotline Service available to political parties throughout the by-election period
- Publication of an unclassified report post by-election

The word "Canada" in a serif font, with a red maple leaf icon above the letter 'a'.

For Public Release



What is foreign interference?

Unclassified

The Government of Canada defines **foreign interference** as malign activities undertaken by states, or their proxies, to advance their own strategic objectives to the detriment of Canada's national interests. It includes activities that fall below the threshold of armed conflict, yet are clandestine, deceptive, threatening and/or illegal.

What is the aim?

- Foreign states engage in FI activities in Canada for:
- strategic, military, intelligence and economic gain;
 - regime preservation; or
 - discrediting democratic institutions.

Foreign interference is **distinct from normal activities to exert influence**, which are legitimate, legal and an integral part of conventional and rules-based international relations.



Canada

For Public Release



Risk of Violence/Violent Extremism

Unclassified

- Global trends and incidents manifest domestically more quickly and deeper than previously seen
- Threat actors are driven by a range of grievances that are amplified by mis/disinformation
- Threatening rhetoric has been normalized against public figures and threats to parliamentarians are known to peak during election cycles.
- The risk of protests leading to violence is driven by multiple factors: demographics, ideologues, candidates, riding history, etc.



Canada

For Public Release



Why Canada?

Unclassified

Characteristics that make Canada an attractive target:

- membership in multilateral and bilateral defence and trade agreements;
- abundance of natural resources;
- leadership in many sectors;
- rich diversity and multiculturalism; and
- open society.



Canada

For Public Release



SITE TF

Targets of FI: Elected and Public Officials

Unclassified

- Elected officials include:

- members of Parliament,
- members of provincial legislatures,
- municipal officials, and
- representatives of Indigenous governments.



- Public servants, ministerial and political staff, and others with input into, or influence over, the public policy decision-making process
- Electoral candidates and their staff



Canada

For Public Release



What FI actors want from you?

Unclassified

- Compel you to **advocate or suppress specific policy positions.**
- Use you to obtain **access to policy makers and other high-value targets.**
- Obtain **privileged information** from you that would help them achieve their goals, such as:
 - Information about government policies and plans;
 - Information about people in power positions; and
 - Information about security protocols.



Canada

For Public Release



Who are the prominent perpetrators?

Unclassified

Some prominent foreign states conducting FI activities against Canada to promote their strategic interests include:



People's Republic of China (PRC)



Government of India (GoI)



Russia



Government of Pakistan (GoP)



Canada

For Public Release

Unclassified



Known Foreign Interference Opportunities



Financing

- GE43 – 2019
- GE44 – 2021



Community groups

- Greater Vancouver, GE43 – 2019



Candidates Nomination

- DVN



Coercive measures

- DVN



Mis/Disinformation

- GE44, late August 2021
- Steveston-Richmond East, BC & Bill C-282
- Wellington-Halton Hills MP, May 4-13, 2023
- Spamouflage



For Public Release



Cyber and Digital Threats to Parliamentarians

Unclassified

Cyber Attacks - Hacking

- **Tactics and Techniques:**
 - Ransomware
 - DDoS,
 - Cyberespionage
 - Social engineering (e.g.: spearphishing, tracking pixels).
- **Targets:**
 - Voter and/or party databases
 - Corporate networks and resources
 - Email accounts
- **Goals:**
 - Access and/or manipulate sensitive information
 - Disrupt party operations and campaigns
 - Inflict reputational damage

Social Media Impersonation

- **Tactics and Techniques:**
 - Social engineering (e.g.: spearphishing, tech support scams)
 - Credential compromise
 - Deepfakes
 - Account and website defacement.
- **Targets:**
 - Official party accounts and websites
 - Candidate accounts
 - Party executive accounts
- **Goals:**
 - Discredit or embarrass target.
 - Influence public opinion

Information Campaigns

- **Tactics and Techniques:**
 - Misinformation, disinformation and malinformation
 - Hack-and-leak operations
 - Blackmail operations (e.g.: sextortion)
- **Targets:**
 - Canadian public
 - Party members
 - Candidates
- **Goals:**
 - Inflict reputational damage
 - Influence public opinion and election results
 - Coerce/control candidates.



For Public Release



How to protect yourself

Unclassified

- Be aware and keep track of “unnatural” social interactions.
- Be aware of inappropriate requests that involve money, suspicious donations, free trips, personal benefits, or “gifts.”
- Follow protocols on the security of information.
- Be diligent with information sharing and partnerships.
- Practice good password etiquette and use Two-factor identification whenever possible.
- Apply updates to your mobile devices, computers and applications.
- Secure your social media account.
- Be on guard for phishing and spear-phishing messages.
- Store your data securely and know your back-up procedures.
- Set up social media and web monitoring, as well as alerting services for identifying and tracking fake news and deep fakes related to your brand and organizations.
- Be wary of connecting devices to unsecured or free Wi-Fi networks.

**Canada**

For Public Release



How to report

Unclassified

- If you or your family believe they are in immediate danger, call 9-1-1 or contact the local police.
- To report non-urgent potential national security threats or suspicious activities, contact CSIS at 613-993-9620, or 1-800-267-7685, or by completing the [web form](#).
- Contact CSE's Canadian Centre for Cyber Security for tailored cyber security assistance: **1-833-CYBER-88** or contact@cyber.gc.ca.
- Contact RCMP Protective Operations Coordination Centre (POCC): phone 1-833-226-7622 or by email protective_policing@rcmp-grc.gc.ca.



Canada

For Public Release



SITE TF

Extra Guidance for Parliamentarians

Unclassified

- [Foreign Interference and You](#)
- [Cyber Security Guide for Campaign Teams](#)
- [Cyber Security Advice for Political Candidates](#)
- [Five Practical Ways to Protect your Campaign](#)
- [Fact Sheet for Canadian Political Campaigns: Protect Yourself Online](#)
- [Social Media Account Impersonation](#)
- [Cyber Security Briefing for Canadian Elections \(ITLC 612, Course Training\)](#)
- [Cyber Security for Political Party IT Decision Makers and IT Staff \(ITLC 616\)](#)
- See the Cyber Centre's [Cyber Threats and Elections](#) webpage and the [Cyber Threats to Canada's Democratic Process Update](#) for additional information.



Canada

For Public Release



Unclassified

Questions?



This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSIS, given its role as SITE TF Chair in 2023-2024.

