

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 Parliamentarians and their staff 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;
- the roles and responsibilities within the GoC in countering foreign interference;
- who are the targets;
- the prominent threat actors;
- the common FI tools and tactics; and
- how to protect yourselves.

The word "Canada" is written in a red, serif font, with a small red maple leaf positioned above the letter 'a'.

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



Durham 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' 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 above the letter 'a'.

For Public Release



Unclassified

What is foreign interference?

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.

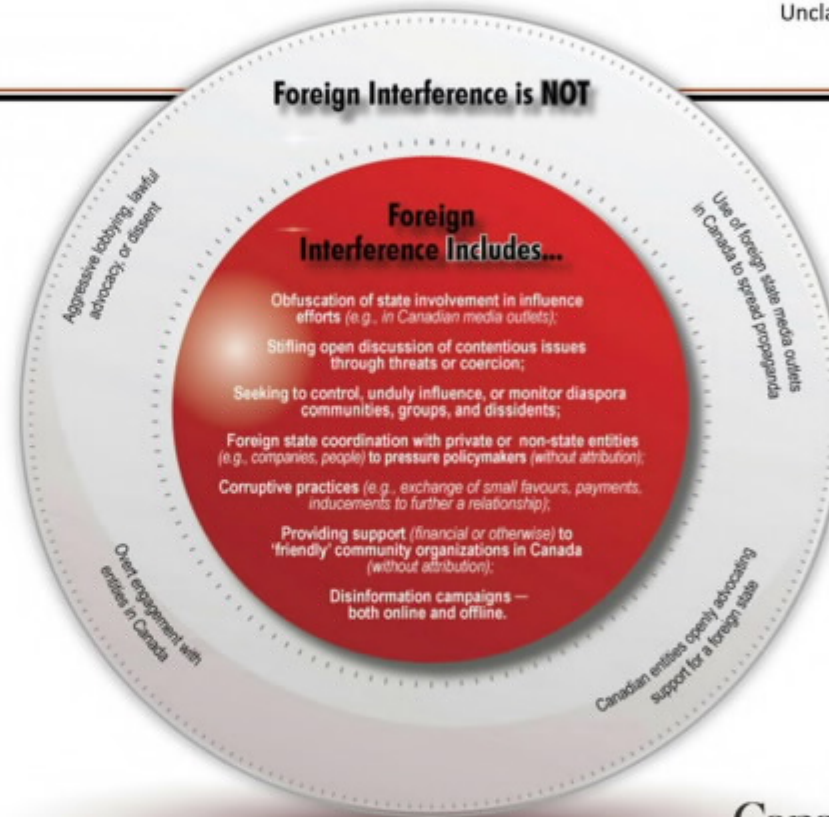
**Canada**

For Public Release

Unclassified



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



Unclassified

Why Canada?

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



Unclassified

What is the GoC doing to protect against FI?

- Security and Intelligence Threats to Elections (SITE) Task Force
- Ongoing whole-of-government approach to defend against FI threats:
 - National Counter Foreign Interference Coordinator (PS)
 - Canadian Security Intelligence Service (CSIS)
 - Communications Security Establishment (CSE) and the Canadian Centre for Cyber Security (CCCS)
 - Royal Canadian Mounted Police (RCMP)
 - Global Affairs Canada (GAC)

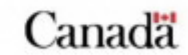
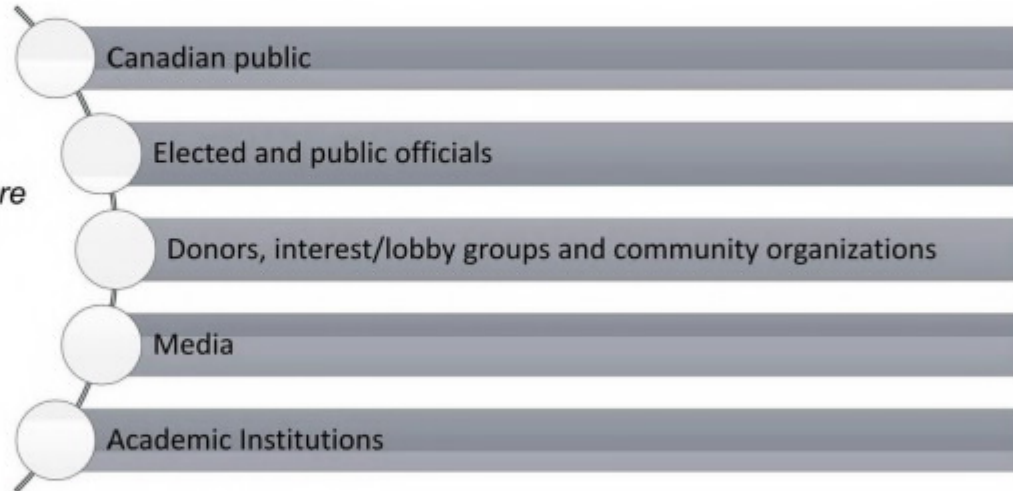


The word "Canada" in a bold, sans-serif font, with a red maple leaf above the letter 'a'.



Who are the targets?

Foreign interference activities are persistent, multi-faceted, and target all areas of Canadian society





Targets of FI: Elected and Public Officials

- 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



Unclassified

What threat actors want from you?

- 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



Unclassified

Who are the prominent perpetrators?

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

- China
- Russia
- Iran
- India

**Canada**



Common FI tactics and techniques

FI can take multiple forms, employ diverse techniques, and target many different Canadians and their communities.



Elicitation



Illicit and corrupt financing



Social Media Manipulation



Cultivation



Cyber attacks



Blackmail/Threats



Canada

For Public Release

Unclassified



Cultivation and Financing: Christine Lee & UK MP

SECURITY SERVICE MS

Security Service Interference Alert

Christine Ching Kui LEE

The purpose of this Security Service Interference Alert (SSIA) is to draw attention to an individual knowingly engaged in political interference activities on behalf of the United Front Work Department (UFWD) of the Chinese Communist Party (CCP).

State Threat Actors

- The UFWD identifies and cultivates individuals with the goal of promoting the CCP's agenda and challenging those that do not subscribe to its policies. This activity can be both overt and covert.
- UFWD actors have been known to be involved in political interference activity, seeking to deceive, corrupt or coerce politicians and high profile individuals into making statements or taking action in support of the objectives of the CCP, and to silence voices which are critical of the CCP.



Christine LEE

Affiliations:

- China Overseas Friendship Association; and,
- British-Chinese Project.

LEE has acted covertly in coordination with the UFWD and is judged to be involved in political interference activities in the UK.

The purpose of this SSIA is to inform you that Christine Ching Kui LEE is working in coordination with the United Front Work Department (UFWD) of the Chinese Communist Party (CCP). We judge that the UFWD is seeking to covertly interfere in UK politics through establishing links with established and aspiring Parliamentarians across the political spectrum. The UFWD seeks to cultivate relationships with influential figures in order to ensure the UK political landscape is favourable to the CCP's agenda and to challenge those that raise concerns about CCP activity, such as human rights.

LEE has been engaged in the facilitation of financial donations to political parties, Parliamentarians, aspiring Parliamentarians and individuals seeking political office in the UK, including facilitating donations to political entities on behalf of foreign nationals. LEE has publicly stated that her activities are to represent the UK Chinese community and increase diversity; however, the aforementioned activity has been undertaken in covert coordination with the UFWD, with funding provided by foreign nationals located in China and Hong Kong. LEE has extensive engagement with individuals across the UK political spectrum, including through the now disbanded All-Party Parliamentary Chinese in Britain Group, and may aspire to establish further APPGs to further the CCP's agenda.

Anyone contacted by LEE should be mindful of her affiliation with the Chinese state and remit to advance the CCP's agenda in UK politics. If you receive any concerning or suspicious contact or would like any further information, please contact the Parliamentary Security Director (PSD).

Point of Contact [\[Redacted\]](#)

Handling Information

This report should be used to raise awareness of the potential threat posed by the individual it describes, and is aimed at those who are most likely to encounter them. We would welcome any feedback or comments on the activities of the individuals concerned, particularly from those that have already encountered this individual or will do so in the future.

RESTRICTED - SECURITY



For Public Release

Unclassified



Cultivation and Elicitation: Senator Feinstein & her driver

San Francisco Chronicle

Subscribe Sign In

BAY AREA

Feinstein had a Chinese spy connection she didn't know about — her driver

By **Hallier & Ross**

Updated Aug 1, 2018 9:07 a.m.



U.S. Sen. Dianne Feinstein (D-Calif.) addresses the 2018 California Democratic State Convention on February 24, 2018, in San Diego. (Brian Cahn/TWIST Images)



Canada

For Public Release



Social Media Manipulation: MP Chong & Spamouflage campaign

Unclassified

- *Disinformation campaign against Mr. Chong (between May 4 and 13, 2023):*
 - a coordinated network of WeChat news accounts featured, shared and amplified false or misleading narratives about Mr. Chong's identity, including commentary and claims about his background, political stances and family heritage.

GAC judges it highly probable China played a role in the information operation based on indicators such as:

- o coordinated content and timing;
- o highly suspicious and abnormal shifts in volume and scope of engagement; and
- o the concealment of state involvement.

- *Spamouflage (August 2023):*
 - Spamouflage is a well studied tactic or technique using networks of spam social media accounts.
 - This activity targeted dozens of MPs from across the political spectrum and included "Deepfake" videos of a Canada based critic of Chinese Communist Party (CCP) criticizing the Prime Minister.
 - Very low engagement/reach to audiences but observed on multiple western social media platforms.

GAC judges it highly probable that it is connected to China based on previous reporting from industry and academia.

Indicators to look for: Anonymous networks spreading false narratives, posting at the same or near same time, which then get amplified by state media or officials.



Canada

For Public Release



Unclassified

How to protect yourself

- 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.



Canada

For Public Release



Unclassified

Cyber and Digital Threats to Parliamentarians

Cyber Attacks - Hacking

- Cyber threat actors use a variety of techniques to target the websites, e-mail, social media accounts, as well as the networks and devices of political parties, candidates and their staff, to access private information.

Impersonations on Social Media

- Tactics including deepfake technologies, have been used to target politicians and journalists, primarily women, to silence and discredit them. Threat actors can also target voters using AI-generated audio to mimic the tone, inflection and idiosyncrasies of candidates.

Information campaigns

- Parliamentarians may be targeted by misinformation, disinformation and malinformation to inflict reputational damage and may influence much larger groups.



Canada

For Public Release



SITE TF

Unclassified

How to protect your digital self

- 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



Unclassified

How to report

- 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.
- RCMP Protective Operations Coordination Centre (POCC): phone 1-833-226-7622 or by email protective_policing@rcmp-grc.gc.ca.



Canada

For Public Release



Unclassified

Extra Guidance for Parliamentarians

- [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.

Canada