

For Public Release

Protected B | Protégé B



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**PROTECTED B**

DATE:2023-11-07

File No.: PS-041739

GCDOCS: 34034126

**MEMORANDUM FOR THE MINISTER OF PUBLIC SAFETY, DEMOCRATIC  
INSTITUTIONS AND INTERGOVERNMENTAL AFFAIRS**

**BRIEFING PARLIAMENTARIANS ON FOREIGN INTERFERENCE**

(For Signature)

**ISSUE**

Your signature is requested by 13 November 2023, in order to approve material (**TABS A & B**) which will be used by national security officials to brief Members of Parliament (MPs) and their staff on foreign interference (FI).

**BACKGROUND**

With the high level of attention around FI, notably the threat to democratic institutions, it would be advisable that MPs be invited to an unclassified threat briefing on FI. The briefing would provide information on the FI threat and practical advice for MPs and their staff to protect themselves. It would also create a more regularized avenue for engagement on FI with MPs. The practice of providing briefings on specific issues to MPs, particularly by the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP), is not new, but a comprehensive level-setting briefing on FI appears necessary at this point. Pursuing these briefings would align, among others, with:

1. Recommendations made by the National Security and Intelligence Committee of Parliamentarians (NSICOP) in its Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018: *"In the interest of national security, members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada"*;
2. Recommendations made by the Standing Committee on Access to Information, Privacy and Ethics in its 2023 report on "Foreign Interference and the Threats to the Integrity of Democratic Institutions, Intellectual Property and the Canadian State":

For Public Release

Protected B | Protégé I

- 2 -

*“That the Government of Canada ensure that the Canadian Security Intelligence Service provide more training and information to Canadian parliamentarians and public servants on the threats posed by foreign interference in Canada, the various tactics used by foreign actors and the means to counter them”*; and

3. Commitments made in the Government of Canada report on “Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada’s Democratic Institutions” wherein *“New briefings will be offered to Members of Parliament and Senators”*.

PS held conversations with the Sergeant-at-Arms of the House of Commons of Canada and the Director of Corporate Security of the Senate on the proposed briefings, both of whom accepted to help facilitate the offer, and to work with party caucuses to set up briefings.

To support this brief, PS, CSIS, RCMP and the Communications Security Establishment (CSE) have developed an English (**TAB A**) and French (**TAB B**) FI deck. This has also previously been consulted with the Privy Council Office and the Prime Minister’s Office and is attached for your approval. The briefings would be delivered by PS, in collaboration with CSIS, the RCMP and CSE.

### **CONSIDERATIONS**

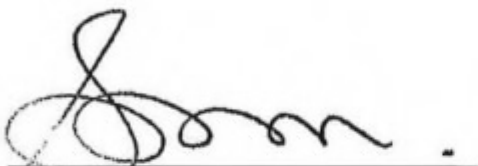
FI is a non-partisan issue, and it is the collective responsibility of MPs and their staff to be aware of best practices. Recent examples of attempts by foreign states or their proxies to interfere in Canadian electoral processes highlight the need to keep MPs informed on an on-going basis (e.g., the Spamouflage campaign targeting the Prime Minister, several members of Cabinet, the leader of the Official Opposition, and dozens of other MPs on popular social media platforms such as Facebook, X (formerly Twitter), and YouTube; and the activity on WeChat against MP Michael Chong and his family – who was consequently called to speak to his experience during a United States congressional hearing on transnational repression).

Your colleague, and former Minister of Public Safety (PS), the Honourable Bill Blair, addressed a letter to MPs in December 2020 that discussed FI, and what the Government of Canada was doing to actively address these threats. The letter was expansive and provided MPs with a briefing on the threat environment, the government agencies responsible for safeguarding the nation, and other government actions to further strengthen our institutions and citizenry against FI. The English (**TAB C**) and French (**TAB D**) versions of that letter are attached for your reference.

**RECOMMENDATION**

It is recommended you approved the enclosed English (**TAB A**) and French (**TAB B**) decks and authorize PS, in coordination with the Sergeant-at-Arms and the Director of Corporate Security of the Senate, to establish a schedule of briefings, as well as provide briefings on a ad-hoc basis as required.

Should you require additional information, please do not hesitate to contact me or Sébastien Aubertin-Giguère, Assistant Deputy Minister, National and Cyber Security Branch, at 613-614-4715.



Shawn Tupper  
Deputy Minister

I concur

I do not concur

I concur with changes



\_\_\_\_\_  
The Honourable Dominic LeBlanc, P.C., K.C., M.P.

Date: \_\_\_\_\_

Attachments (4):

- Tab A: FI Deck to Parliamentarians (EN)
- Tab B: FI Deck to Parliamentarians (FR)
- Tab C: FI Letter - Min PS Blair Dec 2020 (EN)
- Tab D: FI Letter - Min PS Blair Dec 2020 (EN)

Prepared by: NSOD-NCSB



Public Safety  
Canada

Sécurité publique  
Canada

UNCLASSIFIED

**BUILDING A SAFE AND RESILIENT CANADA**  
**BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT**



# Foreign Interference

## Briefing to Canadian Parliamentarians

Date

# Purpose and Objectives

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

- **Purpose**
  - Provide Parliamentarians and their staff with a comprehensive and up to date briefing on foreign interference
- **Objectives**
  - Define the threat of foreign interference.
  - Define roles and responsibilities in countering foreign interference
  - Provide concrete examples of foreign interference.
  - Provide tools and resources to help protect yourselves.



Public Safety  
Canada

Sécurité publique  
Canada

# What is foreign interference?

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

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.

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.

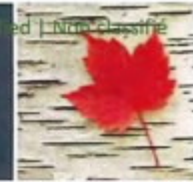


For Public Release

Public Safety  
CanadaSécurité publique  
Canada

# Roles and Responsibilities in countering foreign interference

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

## Public Safety / National Counter Foreign Interference Coordinator

- Public Safety Canada coordinates the Government's efforts to combat foreign interference, to give Canada's existing and future efforts greater focus, coherence and effect.

## Canadian Security Intelligence Service (CSIS)

- Investigates threats to the national security of Canada, advises the Government of Canada on intelligence matters, and takes threat reduction measures.

## Communications Security Establishment (CSE) and the Canadian Centre for Cyber Security (CCCS)

- CSE leverages its authorities including cyber security, the collection of foreign signals intelligence, and the conduct of active and cyber defensive operations to enhance our security posture against foreign interference, and to disrupt the activities of malign actors that target Canadian systems of importance.

## Royal Canadian Mounted Police (RCMP)

- As Canada's Federal law enforcement agency, the RCMP leverage its mandates and authorities to investigate foreign interference as a threat to the security of Canada.



Public Safety  
Canada

Sécurité publique  
Canada

3  
Unclassified | Non classifié

# Some FI Actors

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

Foreign states with a history of FI activity in Canada include:

- China
- Russia
- Iran
- India



For Public Release



# Why Canada?

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

- 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.



Public Safety  
Canada

Sécurité publique  
Canada

5  
Unclassified | Non classifié

# Who are the targets?

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

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



Canadian public



Media



Elected and public officials



Academic institutions and think tanks



Donors, interest/lobby groups, NGOs and community organizations



Private/business sector



Public Safety  
Canada

Sécurité publique  
Canada

# Elected and Public Officials

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

- 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.



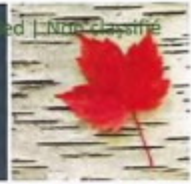
Public Safety  
Canada

Sécurité publique  
Canada

7  
Unclassified | Non classifié

# What threat actors want from you

Unclassified | Non classifié



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉILIENT

- 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.
  - Information about government policies and plans.
  - Information about people in power positions.
  - Information about security protocols.



Public Safety  
Canada

Sécurité publique  
Canada

8  
Unclassified | Non classifié

# Methods used by threat actors

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT



Elicitation



Illicit and Corrupt Financing



Cyber attacks

## Threat actors can, for example:

- Threaten to **use compromising information** about you, your family or your close associates;
- **Harass or threaten** to use violence against you or your family;
- Conduct **social media campaigns** against you;
- Befriend you, creating a **feeling of indebtedness** towards the threat actor, or making you an unwitting participant;
- **Promise personal benefits** (i.e., money, status, access, votes, supporters); or
- **Access your digital information** without your consent.



Cultivation



Coercion



Disinformation



Espionage



Public Safety  
Canada

Sécurité publique  
Canada

# Cyber Threats to Parliamentarians

Unclassified | Non-Classifié



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

## 1. Cyber Attacks - Hacking

- Accessing your information through a range of illicit means.

## 2. Impersonated on Social Media

- Including the use of deepfake technologies, which 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.

## 3. Information campaigns against you

- Parliamentarians may be targeted by mis-and disinformation to inflict reputational damage and may influence much larger groups.
- 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. They may steal information and then release it to the public for the purpose of embarrassing or discrediting the political party or candidate.



Public Safety  
Canada

Sécurité publique  
Canada

10  
Unclassified | Non classifié

## Case Study: Encrypted Messaging Apps

Unclassified | Non classifié



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

- Encrypted Messaging Apps (EMAs) like WhatsApp, Signal and Telegram make it difficult to trace and curb the spread of false information
- The closed nature of EMAs means that most users are communicating with people they consider trustworthy
- Presents users with the ability to forward information to large groups of people, thereby increasing the chances of false information to be misrepresented as fact
- Key distribution channel for misinformation and other hoaxes
- Online foreign influence activity very likely also targets linguistic minorities and diaspora communities in Canada.
  - E.g., WeChat (Chinese social media app) has been used to spread misinformation, disinformation, and malinformation (MDM) and propaganda specific to the Chinese diaspora.



Public Safety  
Canada

Sécurité publique  
Canada

11  
Unclassified | Non classifié

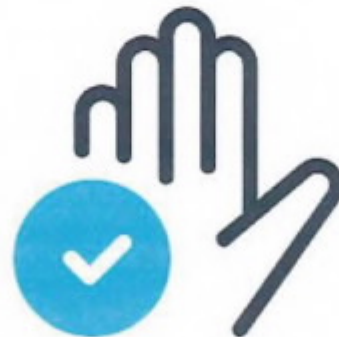
UNCLASSIFIED



## How to protect your social self

BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

- 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



Public Safety  
Canada

Sécurité publique  
Canada

12  
Unclassified | Non classifié



# How to protect your digital self

Unclassified | Non classifié



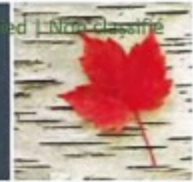
BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

- Practice good password etiquette and use Two-factor identification whenever possible
- Apply updates to your mobile devices, computers and application
- 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



# New Ministerial Direction

UNCLASSIFIED



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT

In accordance with the Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians, CSIS will continue to:

- Investigate all threats (as defined in the *CSIS Act*) that **target Parliament and parliamentarians**.
- Pursue the appropriate **lawful methods** in response to such threats.
- Ensure that **parliamentarians are informed** of these threats directed at them **wherever possible within the law** while protecting the security and integrity of national security and intelligence operations and investigations.
- Inform **Minister of Public Safety** of all instances of threats directed at Parliament or parliamentarians in a timely manner.

CSIS will create a framework to codify implementation of the Directive



Public Safety  
Canada

Sécurité publique  
Canada

14  
Unclassified | Non classifié

# RCMP

Unclassified | Non classifié



**BUILDING A SAFE AND RESILIENT CANADA**  
**BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT**

- The RCMP's Federal Policing National Security (FPNS) program has a multidisciplinary team dedicated to counter foreign interference.
- Collaborates with domestic and international law enforcement and security and intelligence partners to counter foreign interference threats.

## Investigations:

- FPNS provides leadership, subject matter expertise, and governance on investigations.
- NS criminal investigations are conducted by regional investigative teams by using various investigative methods and techniques.
- Engagement and outreach with at-risk communities and sectors.



Public Safety  
Canada

Sécurité publique  
Canada

# SITE Task Force





Unclassified | Non classifié


**BUILDING A SAFE AND RESILIENT CANADA**  
**BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT**



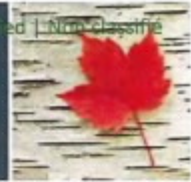
**SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE**

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

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

## Where to turn to

Unclassified | Non classifié



**BUILDING A SAFE AND RESILIENT CANADA**  
**BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT**

- 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](mailto:contact@cyber.gc.ca).
- RCMP Protective Operations Coordination Centre (POCC):  
phone **1-833-226-7622** or by email [protective\\_policing@rcmp-grc.gc.ca](mailto:protective_policing@rcmp-grc.gc.ca).



Public Safety  
Canada

Sécurité publique  
Canada

17  
Unclassified | Non classifié

UNCLASSIFIED

Unclassified | Non classifié



**BUILDING A SAFE AND RESILIENT CANADA**  
**BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT**

# Questions ?

For Public Release



Public Safety  
Canada

Sécurité publique  
Canada

18  
Unclassified | Non classifié

## Annex – Additional Resources

Unclassified | Non classifié



BUILDING A SAFE AND RESILIENT CANADA  
BÂTIR UN CANADA SÉCURITAIRE ET RÉILIENT

### 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.



Public Safety  
Canada

Sécurité publique  
Canada

19  
Unclassified | Non classifié