

For Public Release

Clerk of the Privy Council and
Secretary to the CabinetOttawa, Canada
K1A 0A3Greffier du Conseil privé et
Secrétaire du Cabinet

PCO - BCP Records Operations

DEC 17 2019

Gestion des documents

SECRET
Canadian Eyes Only

DEC 16 2019

MEMORANDUM FOR THE PRIME MINISTER**BRIEFING TO PARLIAMENTARIANS ON
FOREIGN INTERFERENCE AND EXTREMISM IN CANADA**

(Decision Sought / Signature Required)

SUMMARY

- o In its 2018 special report on your trip to India in February 2018, the National Security and Intelligence Committee of Parliamentarians (NSICOP) recommended that Members of Parliament (MPs) and senators be briefed upon being sworn in and regularly thereafter on the risks of foreign interference and extremism in Canada. The recommendation was reiterated in the NSICOP's 2019 annual report, which was submitted to you in August 2019.
- o Parliamentarians can be targeted by foreign interference activities that seek to exploit their role as legislators and the influence they can exert on government policy and on Canada's democratic institutions. It is possible that parliamentarians could come into contact with individuals who hold violent extremist views or who are proxies covertly advancing the interests of foreign state actors.
- o The Canadian Security Intelligence Service (CSIS) has prepared an unclassified, introductory briefing and placemat on foreign interference risks faced by parliamentarians (**Tab A**). The briefing could be delivered to MPs and senators in sessions offered by the Leader of the Government in the House of Commons (Government House Leader) and the Government Representative in the Senate in the early weeks of the 43rd Parliament.
- o Following this initial briefing, the Government House Leader and the Government Representative in the Senate could engage with House and Senate leaders on opportunities to integrate the briefings into orientation activities organized by House and Senate administration.
- o In the interim, PCO is working with partners in the national security community to establish a process for identifying additional briefings on issues related to foreign interference and extremism in Canada that could be provided to parliamentarians.
- o **Do you agree?**

PCO Evidentiary Id / No. de preuve, BCP



N000049873

Canada

Background

- o The *Canadian Security Intelligence Service Act* describes foreign interference as "foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."
- o Foreign states target parliamentarians and their staff for foreign interference activities because they are decision-makers in the legislative process and because they are in a position to influence government policy on issues of interest to foreign states.
- o In their role as parliamentarians, MPs and senators regularly engage with constituents and Canadians, which could potentially bring them into contact with individuals who hold violent extremist views or who may be covertly acting in the interests of a foreign power.
- o On December 3, 2018, the NSICOP's special report on your trip to India in February 2018 was tabled in Parliament. Among other issues, the special report examined the circumstances surrounding allegations of foreign interference in the context of the trip and recommended that, in the interest of national security, MPs and senators be briefed upon being sworn in and regularly thereafter on the risks of foreign interference and extremism in Canada.
- o The NSICOP's 2019 Annual Report, which was submitted to you in August 2019 and must be tabled in Parliament within the first 30 sitting days of the 43rd Parliament, reiterates the recommendation.
- o Countering foreign interference was also a key objective of Canada's plan to safeguard the recent general election. As part of this plan, classified briefings were offered to security-cleared representatives of the major political parties throughout the pre-election period, in order to encourage them to take preventative measures within their party organizations.

PCO Comments

- o Providing a briefing to parliamentarians on the risks of foreign interference could raise awareness of the issue and provide strategies to mitigate the risk and thereby protect Canada's interests.
- o The risks that parliamentarians face with respect to extremism in Canada is also a growing concern given the increased assertiveness of various ideologically motivated violent extremists. Though these individuals usually engage in the online space, there has been an emergence and, in some cases, a re-emergence of a cadre of ethno-nationalist as well as racially and religiously motivated individuals in

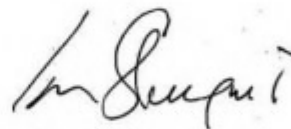
For Public Release

- 3 -

SECRET//CEO

Canada. Some of these individuals and groups are supported by foreign state and non-state actors.

- o CSIS has prepared an unclassified, introductory briefing for parliamentarians that raises awareness on foreign interference activities, highlights tactics used to carry out these activities, and proposes measures to mitigate the risk. A placemat has been developed to support the briefing (**Tab A**). Introductory remarks for the briefing will provide a general warning about the risks of extremism in Canada.
- o The Government House Leader and the Government Representative in the Senate could engage with House and Senate leaders to offer the briefings to MPs and senators. Offering the briefings in the early weeks of the 43rd Parliament may be well received by former NSICOP members who reiterated the recommendation in their 2019 Annual Report.
- o Following the initial briefings, the Government House Leader and the Government Representative in the Senate could also engage with House and Senate leaders to explore the potential for integrating the briefings into existing orientation sessions provided to new MPs and senators by House of Commons and Senate administration.
- o Going forward, PCO will work with the national security community to identify additional topics that could be addressed in future briefings on foreign interference and extremism in Canada. When providing the briefings, CSIS will also solicit the input of parliamentarians on potential future briefing topics in these areas.
- o **Do you agree?**

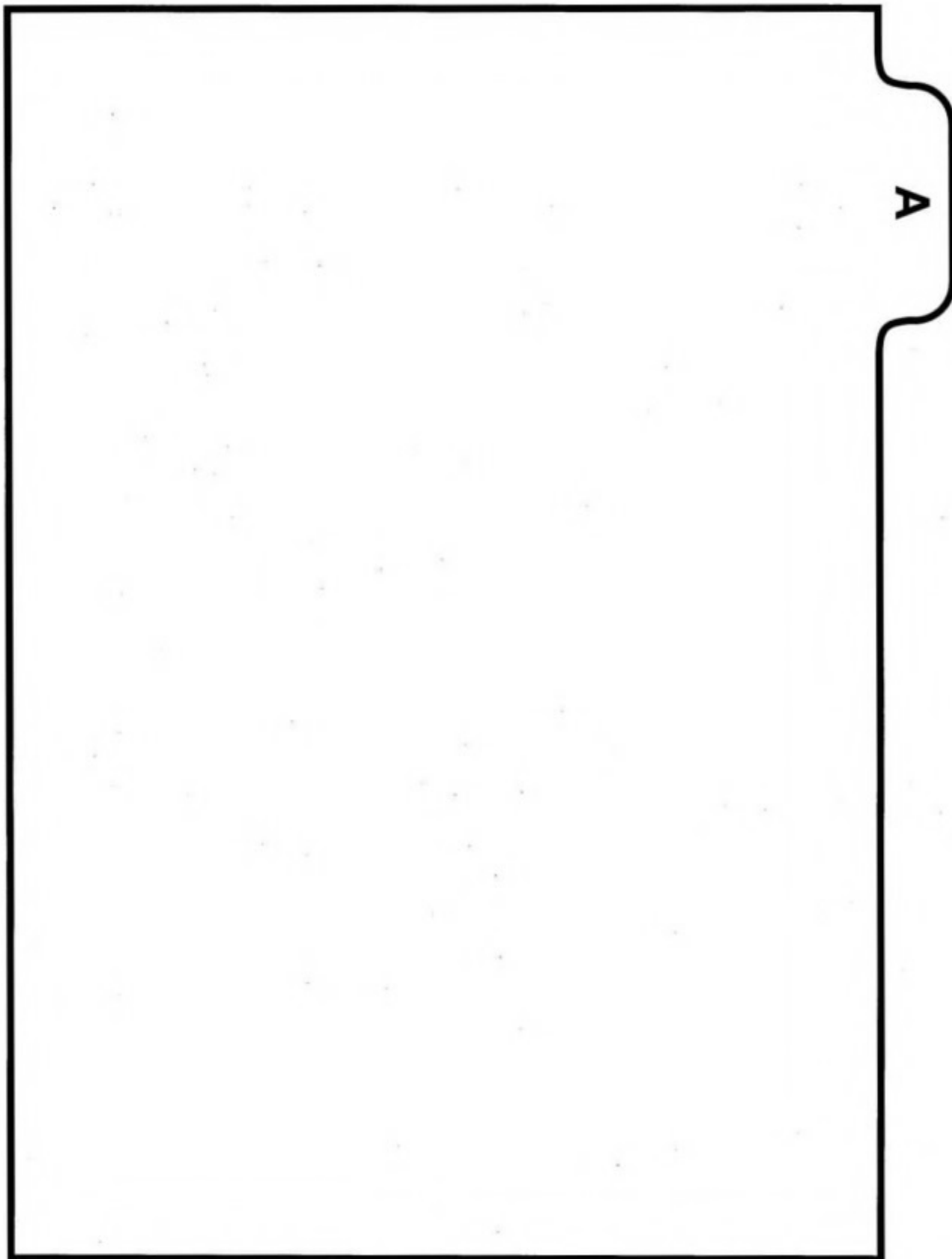


Ian Shugart

Attachment

/Cintrat/Khanna

For Public Release





The Canadian Security Intelligence Service Act describes **Foreign-Influenced Activities** as: "activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person."

Foreign-Influenced Activities, or Foreign Interference (FI) is extensive and aggressive activity undertaken by foreign states, typically covert, against Canadians and Canadian institutions, to advance their strategic interests to the detriment of Canada.

- FI differs from normal diplomatic conduct or acceptable foreign state-actor lobbying.
- Active, overt diplomacy and lobbying are healthy parts of democracy. **Clandestine or deceptive** foreign interference is not.

States conduct Foreign Interference to further their own strategic national interests, for:

- Strategic, military, intelligence and economic gain;
- regime preservation; or
- discrediting liberal-democratic institutions.

Foreign Interference in Canada – BE ALERT



CANADA IS A TARGET. FI is a significant threat to the integrity of our political system, democratic institutions, economy, and fundamental rights and freedoms.

PERSON-TO-PERSON FOREIGN INTERFERENCE REMAINS COMMON PRACTICE, PERPETRATED BY:

- Foreign government officials; Intelligence officers; Proxies and individuals purposefully selected (both witting and unwitting) - community members, office staff.

TARGETS OF FOREIGN STATES INCLUDE:

- The general population and specific communities; political parties; candidates; parliamentarians and their paid and volunteer staff.
- Government and elected officials are targeted because of their access to privileged information, contacts, and decision-makers.

FOREIGN STATES OR THEIR PROXIES MAY TARGET YOU, DIRECTLY OR INDIRECTLY, BECAUSE:

- You possess information they want;
- You have access to information they want;
- You are in a position to influence government policy.

FI HAS BEEN OBSERVED AT ALL LEVELS OF GOVERNMENT IN CANADA: MUNICIPAL, PROVINCIAL AND FEDERAL

YOU AND YOUR STAFF HAVE A KEY ROLE TO PLAY IN PROTECTING CANADA'S DEMOCRACY AND INSTITUTIONS.

Common FI Techniques: HOW CAN YOU PROTECT YOURSELF?

ELICITATION

Elicitation results when a targeted person is manipulated into sharing valuable information through a casual conversation.

For example, a threat actor could knowingly seek to provide you with incorrect information, in the hope that you will correct them, thereby providing information they were actually looking for.

Be discrete, avoid "over-sharing", and assume public conversations are monitored.

CULTIVATION

Effective threat actors seek to build long-lasting, deep relationships with targeted persons. These relationships enable the manipulation of targets when required, for example, through requests for inappropriate and special favours.

To establish a relationship, targets must first be cultivated. Cultivation begins with a simple introduction, with the end goal of recruitment over time. Shared interests and innocuous social gatherings are often leveraged for cultivation.

Be aware and keep track of all social interactions, frequent requests to meet privately, and out of place introductions or engagements.

BLACKMAIL/THREATS

The use of blackmail and/or threats represents one of the most aggressive forms of recruitment and coercion.

If a threat actor becomes aware of compromising or otherwise embarrassing details regarding your life, they can seek to blackmail you.

Sometimes, blackmail or threats may occur after a long period of cultivation and relationship-building. A threat actor may also seek to place you in a compromising situation in an effort to blackmail you later.

Avoid sharing compromising details about your life with untrusted individuals, both in-person and online. Avoid placing yourself in compromising situations.

ILLICIT FINANCING

Threat actors may seek to use you as a proxy to conduct illicit financing on their behalf.

Inducements may occur innocuously via a simple request for a favour. For example, a threat actor may ask you to "pay someone back" or relay money to a third party on their behalf.

Be aware of inappropriate requests which involve money, and question the source of strange donations or gifts.

CYBER TOOLS

Your electronic devices can be compromised through a range of methods. Socially-engineered e-mails (i.e., "phishing" emails) can trick you into clicking a specific link and sharing details about your devices, or can potentially introduce harmful malware into your systems.

Use strong passwords, enable two-factor authentication, and do not click on links from attachments unless you are certain of who sent them and why.

These cyber tools enable threat actors to collect potentially useful information that can be used in a foreign influence operation (e.g. voter data, compromising information about a candidate).

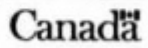
SOCIAL MEDIA MANIPULATION

Threat actors can manipulate social media to spread disinformation, amplify a particular message, or "troll" users, when appropriate.

By using specific manipulation tactics, threat actors can potentially impact voter opinions and degrade the reputations of elected officials.

Be careful in what you share on-line (or in-person) - just have others, take note of and active interactions and content.

For Public Release



For Public Release

Government of Canada / Privy Council Office
Gouvernement du Canada / Bureau du Conseil privé

Security / Sécurité (with attachment(s) / avec pièce-jointe(s))

Secret // CEO

Transmittal Note / Bordereau de transmission

To / Pour : Ian Shugart	Date : Nov 25, 2019
-----------------------------------	-------------------------------

Subject / Objet:
Briefing to Parliamentarians on Foreign Interference and Extremism in Canada

From / De :		Via:	
Name / Nom	Office / Bureau	Name / Nom	Office / Bureau
+ Mala Khanna <i>MK</i>	1-ASPA / 1-SAAP F.BCP	+ Ian McCowan	1-DSG / 1-SSG F.BCP
- Allen Sutherland <i>AS</i>	1-ASMOGD/1-SAAGR F.BCP	- Caroline Xavier <i>CP</i>	A Sec SI
Approved By / Approuvé par : <i>DEC 11 2019</i>		Drafting Officer / Rédacteur	
Name / Nom	Office / Bureau	Admin typist	
+ Jean Cintrat <i>JC</i>	1-DLHP / 1-DAP F. BCP		
+ Greta Bossenmaier <i>GB</i>	NSIA <i>DEC 13 2019</i>		

Action Requested / Mesure de suivi :

- Your Signature / Votre signature
- Your Comments / Vos commentaires
- Your Meeting / Votre réunion
- Your Decision / Votre décision
- Your Information / À titre d'information

For the attention of / A l'attention du:

- Prime Minister / Premier Ministre
- Clerk / Greffier
- Minister / Ministre

Janica Dec-13

Remarks / Observations :

Reference Numbers / Numéros de référence :

WEBCIMS # 2019-LHP-00239 InfoXpress Transmittal Note / Bordereau de transmission
 InfoXpress Briefing Note / Note de breffage
 GCDOCS # 7154901 InfoXpress Other Numbers / Autres numéros

In consultation with / En consultation avec :

- SD / PDS
- ERDP / PDER
- P&P / PP
- LSMP / SLPM
- COMMS / COMMS
- IGA / AI
- MOG / AG
- Leg. Couns. / CJ
- Parl Affairs / LPP
- F & DP / PED
- S&I / SR
- IAS / LDR
- SPS / PS
- PSR / RFP
- RDU / RL
- NSIA / CSNRA
- Corp / SM
- Youth / SJ
- Other / Autre :

Distribution after signature / Distribution après signature :

- David Morrison
- Ken MacKillop
- Thao Pham
- Ian McCowan
- Greta Bossenmaier
- Matthew Mendelsohn
- Christiane Fox
- Janine Sherman
- Philip Jennings
- Jodie van Dieen
- Matthew Shea
- Catherine Blewett
- Other / Autre :

Rec'd - Reçu
 0930
 DEC 12 2019
 NSA to PM - PCO
 CNS au FM - BCP

