Public Safety Canada | Sécurité publique 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":

Canada

"*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 Unites 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**

_____ Date:_____
The Honourable Dominic LeBlanc, P.C., K.C., M.P.

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

Canada

Purpose and Objectives

- **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.

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.

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.

Roles and Responsibilities in countering foreign interference

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.

Some FI Actors

- Foreign states with a history of FI activity in Canada include:
  - China
  - Russia
  - Iran
  - India

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.

Who are the targets?

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

Canadian public

Media

Elected and public officials

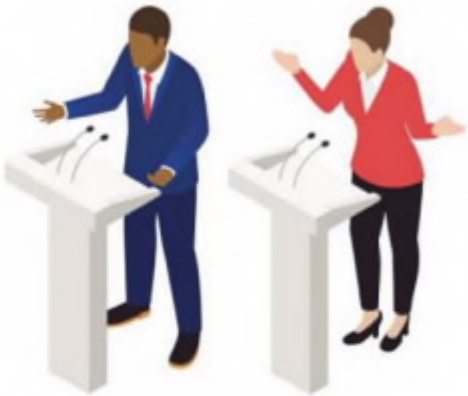
Academic institutions and think tanks

Donors, interest/lobby groups, NGOs and community organizations

Private/business sector

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.

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

Methods used by threat actors

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

Cyber Threats to Parliamentarians

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

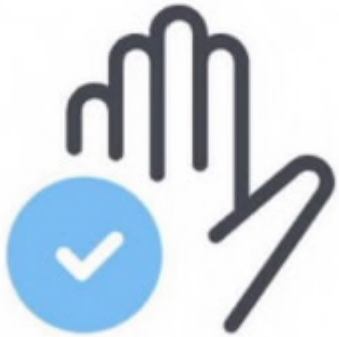
- Parliamentarians may be targeted by mis-and disinformation to inflict reputational damage and may influence much larger groups.
- Cyber threat actors use a variety of techniques to target the websites, e-mail, social media accounts, as well as the networks and devices of political parties, candidates 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.

Case Study: Encrypted Messaging Apps

- 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.

How to protect your social self

- 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



How to protect your digital self

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

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

Canada

RCMP

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.

Canada

SITE Task Force

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
CSE Communications Security Establishment	**Information Technology Security** • Providing advice, guidance, and services to help ensure the protection of electronic information and of systems of importance **Foreign Intelligence** • Collection of foreign intelligence for Government of Canada on threat actors **Supporting CSIS and RCMP** • Providing assistance on technical operations	• 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** • 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** • Providing advice, intelligence reporting and intelligence assessments to Government of Canada about foreign influenced activities	• 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** • 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	• 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** • 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	• 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

Where to turn to

- 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**.

Questions ?

Annex – Additional Resources

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

SANS CLASSIFICATION

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

Ingérence étrangère

Information à l'intention des parlementaires canadiens

date

Canada

But et objectifs

SANS CLASSIFICATION

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

- **But**
  - Fournir aux parlementaires et à leur personnel de l'information complète et à jour sur l'ingérence étrangère

- **Objectifs**
  - Définir la menace que représente l'ingérence étrangère
  - Définir les rôles et les responsabilités liés à la lutte contre l'ingérence étrangère
  - Fournir des exemples concrets de l'ingérence étrangère
  - Fournir des outils et des ressources pour vous aider à protéger vos activités

Qu'est-ce que l'ingérence étrangère?

SANS CLASSIFICATION

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

Le gouvernement du Canada définit **l'ingérence étrangère** comme les activités malveillantes que mènent des États ou leurs mandataires pour faire avancer leurs propres objectifs stratégiques au détriment des intérêts du Canada. L'ingérence étrangère comprend les activités qui se situent sous le seuil des conflits armés, mais qui sont clandestines, trompeuses, menaçantes et/ou illégales.

L'ingérence étrangère **n'est pas la même chose que les activités normales qui visent a exercer une influence**, lesquelles sont légitimes et légales et font partie intégrante des relations internationales conventionnelles et fondées sur des règles.

Rôles et responsabilités liés à la lutte contre l'ingérence étrangère

SANS CLASSIFICATION

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

Sécurité publique / Coordonnateur national de la lutte contre l'ingérence étrangère

- Sécurité publique Canada coordonne les efforts du gouvernement en matière de lutte contre l'ingérence étrangère, pour faire en sorte qu'ils soient mieux ciblés, plus cohérents et plus efficaces.

Service canadien du renseignement de sécurité (SCRS)

- Enquêter sur les menaces à la sécurité du Canada, donner des conseils au gouvernement du Canada sur les enjeux liés au renseignement et prendre des mesures de réduction de la menace.

Centre de la sécurité des télécommunications (CST) et Centre canadien pour la cybersécurité (CCCS)

- Le CSE utilise ses pouvoirs, notamment en matière de cybersécurité, de collecte de renseignements étrangers d'origine électromagnétique, et de réalisation de cyberopérations actives et défensives pour améliorer notre position en matière de sécurité contre l'ingérence étrangère et imposer des coûts aux acteurs malveillants qui ciblent les systèmes importants du Canada.

Gendarmerie royale du Canada (GRC)

- En tant qu'organisme fédéral d'application de la loi au Canada, la GRC tire parti de son mandat et de ses pouvoirs pour enquêter sur les activités d'ingérence étrangère qui constituent une menace pour la sécurité du Canada.

Quelques acteurs

- Les États étrangers qui mènent des activités d'ingérence étrangère contre le Canada inclut :
  - la Chine;
  - la Russie;
  - l'Iran.
  - l'Inde

Pourquoi le Canada?

SANS CLASSIFICATION

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

- Caractéristiques du Canada qui en font une cible attrayante:
  - signataire d'accords bilatéraux et multilatéraux en matière de commerce et de défense;
  - abondance de ressources naturelles;
  - leadership dans de nombreux secteurs;
  - riche diversité et multiculturalisme; et
  - société ouverte.

Qui sont les cibles?

SANS CLASSIFICATION

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

Les activités menées à des fins d'ingérence par des intérêts étrangers sont persistantes, comportent de multiples facettes et ciblent toutes les sphères de la société canadienne

Public canadien

Médias

Élus et fonctionnaires

Établissements d'enseignement et groupes de réflexion

Donneurs, groupes d'intérêt ou de pression, ONG et organisations communautaires

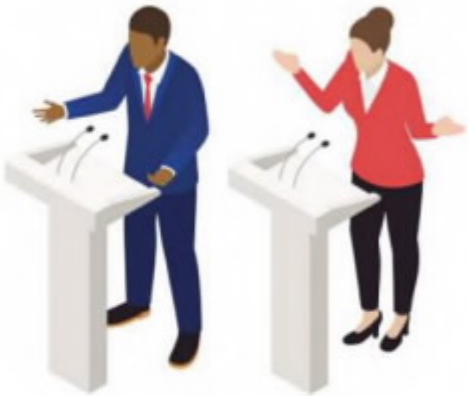
Secteur privé/entreprises

Élus et fonctionnaires

SANS CLASSIFICATION

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

- On compte parmi les élus :
  - les députés fédéraux;
  - les députés provinciaux;
  - les représentants municipaux;
  - les représentants de gouvernements autochtones.



- Les fonctionnaires, le personnel ministériel et politique et d'autres personnes qui contribuent au processus décisionnel en matière de politique publique ou l'influencent.

- Les candidats aux élections et leur personnel.

Ce que les auteurs de menace veulent obtenir

- Vous forcer à **défendre ou à abandonner des positions stratégiques particulières.**
- Se servir de vous pour avoir **accès aux décideurs politiques ou à d'autres cibles très importantes.**
- Obtenir de vous des **renseignements confidentiels** qui les aideront à atteindre leurs objectifs.
  - Renseignements sur les politiques et les plans du gouvernement.
  - Renseignements sur les personnes en position d'autorité.
  - Renseignements sur les protocoles de sécurité.

Méthodes utilisées par les auteurs de menace

SANS CLASSIFICATION

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

Subtilisation

Financement illégal et corruption

Cyberattaques

Les auteurs de menace peuvent, par exemple :

- Menacer d'utiliser des **renseignements compromettants** vous concernant ou concernant votre famille ou vos proches;
- **Vous harceler ou menacer de recourir à la violence** à votre endroit ou à l'endroit de votre famille;
- Mener des **campagnes** contre vous **dans les médias sociaux**;
- Lier des liens d'amitié avec vous, créant un **sentiment de dette** envers eux ou entraînant votre participation involontaire;
- **Vous promettre des avantages** (p. ex., argent, statut, accès, votes, appuis);
- **Accéder à vos renseignements électroniques** sans votre consentement.

Relations

Coercition

Désinformation

Espionnage

Cybermenaces pour les parlementaires

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

1. Cyberattaques - piratage

- Accéder à vos renseignements par divers moyens illégaux.

2. Identité usurpée dans les médias sociaux

- Notamment le recours à des technologies d'hypertrucage, qui ont été utilisées à l'endroit de politiciens et de journalistes, principalement des femmes, pour les réduire au silence et les discréditer. Les auteurs de menace peuvent également cibler des électeurs au moyen d'enregistrements audio générés par l'IA qui imitent le ton, l'intonation et les traits caractéristiques d'un candidat.

3. Campagne d'information contre vous

- Les parlementaires peuvent être la cible de campagnes de mésinformation et de désinformation qui visent à miner leur réputation et peuvent influencer de très grands groupes.
- Les auteurs de cybermenaces ont recours à une gamme de techniques pour cibler les sites Web, les courriels, les comptes de médias sociaux, de même que les réseaux et les appareils des partis politiques, des candidats et de leur personnel. Ils peuvent voler des renseignements et ensuite les révéler au public dans le but de mettre le parti politique ou le candidat dans l'embarras ou de le discréditer.

Étude de cas : applications de messagerie chiffrée

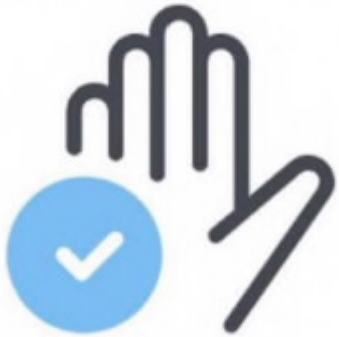
- Les applications de messagerie chiffrée (AMC) comme WhatsApp, Signal et Telegram rendent la diffusion de faux renseignements difficile à repérer et à contrer.
- Comme les AMC ne sont pas de nature ouverte, la plupart des utilisateurs y communiquent avec des gens qu'ils estiment dignes de confiance.
- Elles permettent aux utilisateurs de transmettre des renseignements à de grands groupes, ce qui accentue le risque que de faux renseignements soient communiqués comme s'ils étaient des faits.
- Moyen de diffusion clé pour la mésinformation et d'autres canulars.
- Les activités d'influence étrangère en ligne ciblent fort probablement des minorités linguistiques et les diasporas présentes au Canada.
  - P. ex., WeChat (média social chinois) a servi à diffuser de la mésinformation, de la désinformation et de la malinformation (MDM), ainsi que de la propagande ciblant la diaspora chinoise.

Comment protéger son image sociale

SANS CLASSIFICATION

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

- Restez aux aguets et prêtez attention aux interactions sociales « inhabituelles ».
- Soyez à l'affût de demandes inappropriées portant sur de l'argent, des dons suspects, des voyages gratuits, des avantages personnels ou des « cadeaux ».
- Suivez les protocoles sur la sécurité de l'information.
- Soyez prudents lorsque vous partagez des renseignements ou formez des partenariats.



Comment protéger votre identité numérique

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

- Suivez un protocole efficace au moment de choisir vos mots de passe et utilisez l'authentification à deux facteurs.
- Appliquez les mises à jour à vos appareils mobiles, ordinateurs et applications.
- Sécurisez vos comptes de médias sociaux.
- Soyez à l'affût pour détecter les tentatives de hameçonnage et de harponnage.
- Stockez vos données de façon sécuritaire et établissez des procédures de sauvegarde.
- Mettez en place un contrôle des médias sociaux et du Web, ainsi que des services d'alerte pour détecter et suivre les fausses nouvelles et l'hypertrucage concernant votre image de marque et votre organisation.
- Évitez de connecter vos appareils à des réseaux sans fil non sécurisés ou gratuits.

Nouvelles directives ministérielles

SANS CLASSIFICATION

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

Conformément aux Directives ministérielles sur les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires, le SCRS continuera :

- d'enquêter sur toutes les menaces (selon la définition donnée dans la *Loi sur le Service canadien du renseignement de sécurité*) **dirigées contre le Parlement et les parlementaires**;
- d'appliquer les **méthodes légales** appropriées pour répondre à ces menaces;
- de veiller à ce que les **parlementaires soient informés** des menaces à la sécurité du Canada qui sont dirigées contre eux, et ce, **dans la mesure du possible et dans le respect de la loi**, tout en protégeant la sécurité et l'intégrité des opérations et des enquêtes de sécurité nationale et de renseignement;
- de faire en sorte que le **ministre de la Sécurité publique** soit informé en temps opportun de toutes les menaces dirigées contre le Parlement et les parlementaires.

Le SCRS créera un cadre pour codifier la mise en œuvre des directives.

Canada

GRC

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

- Le programme de la Sécurité nationale de la Police fédérale (SNPF) de la GRC a une équipe multidisciplinaire qui se consacre à la lutte contre l'ingérence étrangère.
- La SNPF collabore avec les partenaires nationaux et internationaux chargés de l'application de la loi, de la sécurité et du renseignement pour lutter contre les menaces d'ingérence étrangère.

Enquêtes :

- La SNPF assure un rôle de chef de file, d'expert en la matière et de gouvernance dans le cadre des enquêtes.
- Les enquêtes criminelles en matière de sécurité nationale sont menées par des équipes d'enquête régionales qui utilisent diverses méthodes et techniques d'enquête.
- Activités de mobilisation et de sensibilisation auprès de secteurs et de collectivités à risque.

Canada

Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections

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

GROUPE DE TRAVAIL SUR LES MENACES EN MATIÈRE DE SÉCURITÉ ET DE RENSEIGNEMENTS VISANT LES ÉLECTIONS

DE QUOI PARLONS-NOUS?

Il s'agit d'activités secrètes, clandestines ou criminelles qui entravent ou influencent les processus électoraux du Canada.

	MANDAT/RÔLE	ACTIVITÉS
CST Centre de la sécurité des télécommunications	**Sécurité de la technologie de l'information** • Fournir des conseils, de l'orientation et des services pour aider à assurer la protection de l'information électronique et des systèmes importants. **Renseignements étrangers** • Recueillir des renseignements étrangers destinés au gouvernement du Canada sur les auteurs de menaces. **Soutien au Service canadien du renseignement de sécurité (SCRS) et à la Gendarmerie royale du Canada (GRC)** • Fournir de l'assistance pour les opérations techniques.	• Fournir des renseignements et des cyber-évaluations sur les intentions, activités et capacités des auteurs étrangers de menaces. • Protéger les systèmes et les réseaux du gouvernement liés aux élections à l'aide de mesures de cyber-défense. • Fournir des conseils et une orientation en matière de cybersécurité aux partis politiques, aux provinces et aux autres institutions qui contribuent aux processus démocratiques.
SCRS Service canadien du renseignement de sécurité	**Renseignements et réduction des menaces** • Recueillir des renseignements sur les activités influencées par l'étranger qui nuisent aux intérêts du Canada, sont clandestines ou trompeuses, ou représentent une menace pour quiconque. • Contrecarrer de telles activités par des mesures de réduction des menaces. **Évaluation des renseignements** • Fournir des conseils, des rapports de renseignement et des évaluations de renseignements au gouvernement du Canada sur les activités influencées par l'étranger.	• Fournir des comptes rendus de menaces et des rapports de renseignement à Élections Canada et au commissaire aux élections fédérales. • Fournir aux décideurs du gouvernement du Canada une évaluation des méthodes et des capacités utilisées pour mener des activités hostiles à l'État.
AMC Affaires mondiales Canada	**Mécanisme de réponse rapide du G7** • Effectuer des recherches en libre accès sur les tendances et les données mondiales concernant les menaces pour la démocratie. • Établir des partenariats avec les pays du G7 afin d'échanger des renseignements et de coordonner les réponses aux menaces, au besoin.	• Effectuer des recherches sur les campagnes de désinformation ciblant le Canada et menées par des acteurs étrangers. • Rendre compte des tendances, des mesures et des incidents mondiaux. • Coordonner l'attribution des incidents.
GRC Gendarmerie royale du Canada	**Sécurité nationale** • Principale organisation chargée de prévenir, de détecter et de repousser les menaces criminelles liées à la sécurité nationale au Canada et d'y répondre. • Enquêter sur les actes criminels liés au terrorisme, à l'espionnage, aux cyberattaques et aux activités influencées par l'étranger. • Constituer, pour Élections Canada, le principal organe d'enquête si une activité criminelle est suspectée.	• Enquêter sur toute activité criminelle visant à entraver ou à influencer les processus électoraux du Canada. • Travailler en étroite collaboration avec les organismes de renseignement, d'application de la loi et de réglementation.

Public Safety Canada | Sécurité publique Canada

Ressources

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

- Si vous ou un membre de votre famille croyez être en danger immédiat, composez le 911 ou le numéro d'urgence de votre ville.
- Pour signaler des menaces non urgentes à la sécurité nationale ou des activités suspectes, communiquez avec le SCRS au **613-993-9620** ou au **1-800-267-7685**, ou remplissez un **formulaire Web**.
- Communiquez avec le Centre canadien pour la cybersécurité du CST obtenir de l'aide particulière en matière de cybersécurité : **1-833-CYBER-88** ou **contact@cyber.gc.ca**.
- Centre de coordination des missions de protection (CCMP) de la GRC : Téléphone : **1-833-226-7622** ou courriel : **protective_policing@rcmp-grc.gc.ca**.

Des questions?

Annexe – Ressources supplémentaires

Conseils supplémentaires à l'intention des parlementaires

- Ingérence étrangère et vous
- Guide de sécurité à l'intention des équipes chargées des campagnes électorales
- Conseils en matière de cybersécurité pour les intervenants politiques
- Cinq moyens pratiques pour protéger votre campagne
- Fiche de renseignements relative aux campagnes politiques canadiennes : Protégez vos activités en ligne
- Faux comptes de médias sociaux
- Exposé sur la cybersécurité liée aux élections au Canada (Cours ITLC 612)
- La cybersécurité à l'intention des décideurs et du personnel des TI travaillant pour un parti politique (Cours ITLC 616)
- Veuillez consulter la page Les cybermenaces et les élections et la page Cybermenaces contre le processus démocratique du Canada (mise à jour) du Centre canadien pour la cybersécurité pour obtenir de plus amples renseignements.

Minister
of Public Safety
and Emergency Preparedness

Ministre
de la Sécurité publique
et de la Protection civile

Ottawa, Canada K1A 0P8

DEC 18 2020

Colleagues,

Foreign interference has recently been a topic of interest and discussion in the House of Commons.

In response to the motion that passed in the House on November 18th, 2020, I am writing to provide you with an overview of what the Government of Canada is doing to address these threats to the security, prosperity and democratic institutions of our country.

As we have adjourned for the winter break, I want to ensure you have something in writing before the session restarts in 2021.

I am happy to formally table the contents of this letter next month.

First-and-foremost, our Government does not, and will never, tolerate these types of activities.

Before I explain some of the ways in which the Government works to protect Canadians and counter these threats, I would like to emphasize that regarding this motion, particularly clause (b), the Government of Canada is always working to refine and further its plans to address foreign interference in Canada.

Work in this area has been longstanding and remains ongoing. This motion provides an opportunity to inform Canadians of what steps have been taken while assuring them that our agencies will always adapt to meet evolving threats.

We understand foreign interference to be hostile activity undertaken by foreign states that is purposely covert, malign, clandestine and deceptive. It can include threats, harassment and intimidation. These activities can be directed at Canadians, or residents of Canada, or against Canadian institutions to advance their strategic interests at the expense of our national interest and values. Hostile foreign states cross a line anytime they go beyond standard diplomacy to conduct activities against Canada that attempt to threaten our citizens, compromise our way of life, undermine our democratic processes, or damage our economic prosperity.

Canada

Modern foreign interference represents a complex threat. It poses a significant threat to the integrity of our political system, democratic institutions, social cohesion, academic freedom, economy and long-term prosperity as well as fundamental rights and freedoms. It can also affect the safety of our citizens and those who live here. This is not new. But it remains unacceptable as it targets all orders of government – federal, provincial and territorial, and municipal, as well as Canadian communities.

Foreign threat actors can use human intelligence operations, state-sponsored or foreign-influenced media, and sophisticated cyber tools, among others, to achieve their objectives. These include advancing their interests, sometimes at our expense, in an effort to achieve geopolitical influence, increase their economic advantages, access sensitive research, technology or information, revise the rules-based international order, enhance their domestic stability, and gain military advantage.

The 2019 Canadian Security Intelligence Service (CSIS) Public Report states that foreign interference activities are directed at Canadian entities both inside and outside of Canada, and directly threaten Canada's national security and strategic interests. Further, the Annual Report of the National Security and Intelligence Committee of Parliamentarians (NSICOP) outlined foreign interference activities, including the targeting of Canadian institutions and certain communities.

I will note that the Prime Minister took the important step of permitting the unclassified, publicly-released version of the NSICOP report to, for the first time, specifically name the People's Republic of China (PRC) and Russia as being particularly active in Canada. This was intended to raise public awareness of the threats posed by these countries. Additionally, the Canadian Centre for Cyber Security Report on National Cyber Threat Assessment 2020 also included reference to these countries as well as Iran and North Korea. Recently, the Standing Committee on Public Safety and National Security heard testimony from Mr. Scott Jones who declared that decisions about whether to list countries in these publications are not easy, but ultimately we need to acknowledge that these countries pose a risk while working to raise Canadians' awareness.

With an open and stable economy, skilled workforce, and advanced infrastructure, Canada is an attractive destination for foreign investors. The vast majority of foreign investment in Canada is conducted in an open and transparent manner and is beneficial to Canada's economy. However, the Government of Canada is increasingly concerned that certain types of investment transactions undertaken by foreign adversaries can harm national security. Foreign investments that give these entities control over, or access

to, sensitive technologies, critical infrastructure or the sensitive personal data of significant numbers of Canadians are of particular concern.

Certain governments, and their proxies, are prepared to use illicit means to obtain goods, sensitive information and technology. These proxies could include state-owned enterprises, individuals engaged with academic institutions and trade organizations, or other entities that are not directly linked to a state itself but may still serve its interests.

For example, talent programs are an acceptable part of the modern research enterprise, however some foreign threat actors can use them for malicious purposes. The requirement to transfer or replicate research, requirements to attribute research to foreign institutions, or to conceal affiliations to foreign military or intelligence services, are ways in which foreign actors, including the PRC, use talent programs to acquire sensitive technology and knowledge to further their economic and security interests to the detriment of Canada's. For instance, CSIS actively investigates threats of foreign interference and espionage and supports the Government of Canada's collective effort to respond, including acting to reduce the threat of specific foreign espionage activities through its lawful mandate.

In addition, foreign states, including the PRC, attempt to threaten and intimidate individuals around the world, including in Canada, through various state entities and non-state proxies. We strongly denounce this behavior wherever it may occur. We know that states may attempt to threaten and intimidate individuals in order to pursue fighting alleged corruption or to bring alleged criminals to justice. However, we are aware that these tactics can also be used as cover for silencing dissent, including on university campuses, pressuring political opponents and instilling a general fear of state power no matter where a person is located. The PRC's *Operation Fox Hunt* is one such example. The PRC uses this program as a means to identify and try to repatriate to China individuals who they allege are corrupt. The PRC has conducted this operation in Canada since 2014. I will note that as per the 2019 NSICOP report, initially the response was often to work with Chinese officials to "support their investigations of corrupt officials." However, "increasingly stringent criteria" on the People's Republic of China investigators involved in this program has been added as time passed following 2015.

When foreign states target Canadians, persons residing in Canada, or their families, they are seeking to deprive members of Canadian communities of their fundamental rights and freedoms. Such actions are unacceptable. If anyone feels intimidated or threatened it is of the utmost importance to

contact your local police, and I can assure you that your concerns will be dealt with in a serious and appropriate manner.

Foreign interference and COVID-19

The COVID-19 pandemic has accelerated these trends by providing foreign threat actors with unique opportunities to pursue their hostile activities. The impacts of disinformation, coercive use of trade and economic-based threats to national security, and threats to Canada's supply chain are ongoing concerns.

This past year, we have observed state-sponsored information manipulation, or disinformation by certain regimes against Canada and our allies. These campaigns aim to sow doubt about the origins of the COVID-19 virus and the means required to counter it; discredit responses to COVID-19 while casting their own as superior; and erode confidence in our shared values of democracy and human rights.

Canada's security and intelligence community, which is at the forefront of Canada's efforts to combat foreign interference, is taking coordinated and integrated action to protect the safety, security and strategic interests of Canadians. I would like to provide you with an overview of these efforts.

CANADA'S RESPONSE TO FOREIGN INTERFERENCE

There is no more fundamental role for the Government than to keep Canadians and communities safe. The Government takes this responsibility seriously. Though I am unable to share operational information regarding ongoing counter foreign interference activities, Canadians can be confident that the Government of Canada applies a whole-of-government approach to protect Canadians from national security threats, including threats to institutions that play a key role in Canada's response to the COVID-19 pandemic.

Investigations and monitoring

CSIS has longstanding investigations into foreign interference threat activities that target Canada, and uses the full mandate of the *CSIS Act* to investigate, advise the government and take action to reduce the threat. CSIS works closely with other government partners, inside and outside the security and intelligence community, to address clandestine, deceptive or threatening interference activities that can pose significant harm to Canada's democratic institutions and processes.

The Royal Canadian Mounted Police (RCMP) have a broad, multi-faceted mandate that allows them to investigate, and disrupt threats from foreign actors by drawing upon various legislation, including investigations with a view to laying charges under the *Criminal Code of Canada*.

The Communications Security Establishment (CSE) provides intelligence and cyber assessments to the Government of Canada on the intentions, activities and capabilities of foreign threat actors, and can also carry out active cyber operations to degrade, disrupt, respond to or interfere with the capabilities, intentions or activities of foreign individuals, states, and organizations. CSE also provides advice, guidance, and services to help protect electronic information and information infrastructures of federal institutions and of systems of importance to the Government of Canada.

In addition, in an effort to counter foreign interference against the 2019 Federal Election, the Government created the Security and Intelligence Threats to Elections (SITE) Task Force, composed of officials from CSE, CSIS, RCMP and Global Affairs Canada (GAC). Throughout the 2019 Federal Election, the SITE Task Force raised awareness and assessed foreign interference threats, briefing members of the Government of Canada's Critical Election Incident Public Protocol on any threat activities to ensure nothing affected Canada's ability to have a free and fair election. The SITE Task Force continues to monitor and advise the Government of Canada on foreign interference-related threats to federal elections.

The Canada Border Services Agency (CBSA) works closely with its partners to ensure that individuals that pose a security threat to Canada, including those who engage in acts of espionage or acts of subversion against democratic governments, do not gain entry into Canada. Those who have previously entered and are deemed inadmissible will be removed from Canada. Through its robust Intelligence and National Security Screening programs, the CBSA aims to detect such inadmissible persons at various points in the travel continuum and advise other security and intelligence partners of possible threats.

Through investigations and monitoring, we continue to identify and shed light on the multiple ways foreign interference manifests itself in Canada, allowing us to be well-armed with the knowledge needed to deploy our tools to counter it.

Protecting against economic-based threats to national security

The Government has never and will never compromise Canada's national security, and will take action where necessary to protect it. As reported in the 2018-19 *Investment Canada Act* Annual Report, for the four fiscal years 2015-16 to 2018-19 the Governor in Council issued eight 25.4 final orders:

six blocking or ordering the foreign investor to divest of its investment and two imposing conditions that protect national security while allowing those investments to proceed.

To protect Canadians in this current economic environment shaped by COVID-19, the Government of Canada announced in April 2020 that it is applying increased scrutiny to all foreign direct investments, controlling or non-controlling, into Canadian businesses that are vital to public health and the security of supply of critical goods and services to Canadians or to the Government of Canada. The Government also announced that all foreign investments by state owned enterprises, or private investors assessed as being closely tied to or subject to direction from foreign governments, would be subject to enhanced scrutiny under the national security provisions of the *Investment Canada Act*. Innovation, Science and Economic Development (ISED) and Public Safety Canada work together, in conjunction with 18 other federal departments, to meet the legislative requirements of this *Act* on behalf of the Government of Canada and Canadians.

The Government of Canada purchases approximately $22B worth of goods and services each year. The potential exists for foreign threat actors to exploit procurement processes to their advantage. State-owned enterprises use their vast resources as a competitive advantage that allows them to underbid Canadian companies, and insert themselves into our infrastructure and services, and undermine our security. The Government is committed to addressing procurement-based national security threats. For example, we are working to enhance risk awareness and ensure due diligence throughout the procurement process. This has included the development of national security guidance material, which has been distributed to employees of departments and agencies with duties that include, or may be impacted by, procurement activity, as well as to Provinces and Territories, and the Canada City Alliance, which represents 12 of Canada's largest cities.

The Government is aware of the ongoing attempts by some foreign states to undermine our economy for their own benefit. Our many efforts to counter these threats help protect Canadians' prosperity and maintain Canada as an economic leader.

Protecting our democracy

In January 2019, the Government announced its plan to defend Canadian democracy from threats ahead of the 43rd General Election. This plan was built on four mutually supporting pillars:

1. *Enhancing Citizen Preparedness* by supporting an informed and engaged citizenry;

2. *Improving Organizational Readiness* by strengthening coordination to identify threats, emerging tactics and systems vulnerabilities;

3. *Combatting Foreign Interference* by preventing covert, clandestine or criminal activities by foreign actors aimed at interfering in our democratic processes; and

4. *Expecting Social Media Platforms to Act* by guiding social and digital platforms to ensure integrity, transparency and authenticity.

The plan was internationally recognized as illustrating Canada's leadership in countering foreign interference in democratic processes, and key components are being evaluated for on-going implementation.

In addition, the *Canada Elections* Act contains provisions that aim to protect the federal electoral process, including strong regulations related to financial and non-financial contributions to political actors, and prohibitions against bribing or intimidating electors. The *Elections Modernization* Act, which received Royal Assent in December 2018, further strengthened protections against foreign interference through amendments that:

- Prohibit third parties from using foreign funds for their partisan activities and advertising, irrespective of when it takes place;
- Prohibit foreign entities from spending any money to influence federal elections;
- Require registered third parties to have a Canadian bank account; and,
- Prohibit any organizations – online or offline – that sell advertising space from knowingly running election advertisements paid for with foreign funds.

A pre-election period was also established, extending spending limits for third parties and subjecting third parties to enhanced reporting obligations. To improve transparency, the amended law also requires online platforms such as social media sites to publish a registry of all partisan or other political advertising they have carried, including who authorized the advertisements, and to keep that information available for a minimum of two years after the advertisements are posted.

As democratic processes were being targeted in multiple countries around the world by foreign threat actors, it was clear Canada needed to take action

here at home. As a result, we took these key measures to bolster the robustness of our democratic and electoral institutions to tackle this threat head on.

Reaching out to Canadians

What the Government does to counter foreign interference is often done behind the scenes, given the sensitivity of the tools and techniques involved. But in light of the breadth of foreign interference and its impact on so many areas of society, our agencies have been engaging with Canadians to assist with the signs of what to look for, and who to call when they encounter it.

In this respect, CSIS provides briefings to private companies, universities and research institutions to help them better understand how to protect their work. In the context of the pandemic, Canada's security and intelligence agencies moved quickly to work with the life sciences sectors involved in Canada's response to COVID-19 to help protect them from foreign interference activities. As an example, CSIS has undertaken a national outreach campaign aimed at sensitizing these sectors from the threat they could face from foreign interference.

The RCMP also engages with the Canadian Association of Chiefs of Police to help inform local law enforcement agencies of threats from foreign interference and to establish mechanisms for reporting foreign interference incidents.

With respect to foreign interference and other cyber threats, CSE's Canadian Centre for Cyber Security (Cyber Centre) recently released the *National Cyber Threat Assessment 2020* report, which highlights cyber threats facing individuals and organizations in Canada in order to help Canadians shape and sustain our nation's cyber resilience. This includes threats from activities sponsored by countries such as the PRC, covering cyber espionage, intellectual property theft, online influence operations, and disruptive cyber incident. The Cyber Centre also provides cyber security guidance and best practices, including through CSE's Get Cyber Safe public awareness and education campaign.

The Government is committed to continued engagement with Canadians on the issue of foreign interference to build awareness and bolster resilience.

Protecting Canadian Knowledge and Research

The Government of Canada is committed to an open and collaborative environment for science and research, and recognizes the importance of Open Science as essential for research discoveries and innovation. At the

same time, espionage and foreign interference activities pose real threats to Canadian research integrity, intellectual property, and business interests.

Universities, government departments, the federal granting councils, and national security agencies are regularly in contact as part of ongoing engagement activities, and collaborate to understand, identify and respond to potential threats to research security. This dialogue includes a joint Government of Canada-Universities Working Group which facilitates the identification, sharing and promotion of best practices to minimize security risks, protect data and intellectual property.

As part of this work, the Government of Canada and the academic sector worked collaboratively to develop and launch an online resource portal called "Safeguarding Your Research." The portal provides information, best practices and tools to help researchers identify and mitigate potential security risks to their work. Earlier this year CSIS gave a briefing to the Canadian Chamber of Commerce which flagged China and Russia as countries actively involved in commercial espionage.

Recognizing the elevated threat of foreign actors targeting COVID-19 related research in Canada, the Government of Canada also released a policy statement on research security – signed by the Minister of Innovation, Science and Industry, the Minister of Health, and myself – in September 2020. The statement identifies the potential threats to research security and the need to take appropriate measures to safeguard research and innovation, particularly in the context of COVID-19.

Furthermore, the Government has instructed federal research funding agencies, including the Canada Foundation for Innovation, the Canadian Institutes of Health Research, the Natural Sciences and Engineering Research Council, and the Social Sciences and Humanities Research Council, to review their security policies and processes and to promote awareness of the best practices and tools available to the Canadian researchers and innovators they fund, so that Canada, rather than our adversaries, maximizes benefits from the Government's significant investments in science and research.

Additionally, direct engagement between Canadian universities, federal laboratories and security institutions on the risks posed by foreign interference has been ongoing since 2016 through the Safeguarding Science initiative led by Public Safety Canada, in partnership with 10 other federal departments.

This initiative aims to raise awareness within Canada's research communities of the risks of proliferation; dual-use technology; research security; and cybersecurity. The initiative informs participants about tools to help recognize and mitigate the risks Canadian institutions are facing, including those posed

to their research and development. Thus far, Safeguarding Science presentations have been delivered to 33 institutions and 5 federal labs across the country. Expansion efforts are also underway to deliver additional tools and guidance to the research community, along with more workshops from coast-to-coast and within the private sector and with Provincial/Territorial partners.

Public Safety Canada has also established a Federal, Provincial and Territorial Community of Practice on Economic-based National Security Threats to bring together key officials across these jurisdictions to discuss national security threats that arise through certain economic activities.

Canada's multi-disciplinary research community is world-renowned. With the right tools and awareness of the potential risks, we can ensure that Canada continues to maximize benefits from our significant investments in science and research.

I will note that just this week it was reported that CSIS has been engaging with, and briefing government partners and companies in the vaccine and other medical supply chains. I can assure you that our agencies will continue to work closely with our partners to ensure that as many businesses and orders of government have the information they need to implement pre-emptive security measures to identify and mitigate all threats.

International collaboration

Canada cannot tackle foreign interference alone. Our international allies and partners face similar threats. And so, by working together, we bring our collective resources to bear in countering threats from foreign actors. Canada has always stood up for a rules-based international order, one in which all countries abide by international norms. Consistent with these principles, Canada actively shares information and coordinates responses with allies through numerous multilateral bodies and relationships.

As a member of the Five Country Ministerial, I have committed to collaborating with my counterparts in the United States, the United Kingdom, Australia and New Zealand on the issue of foreign interference, to share information about our respective approaches and to coordinate responses and attribution as deemed appropriate.

Security and intelligence partners also collaborate to share information in an effort to counter foreign interference, including state-sponsored disinformation, through a number of fora. The security and intelligence community, for example, work with domestic and international partners to share information that can help detect, investigate, and prevent foreign interference in Canada.

Global Affairs Canada leads the G7 Rapid Response Mechanism. In 2018, G7 leaders committed to working together to strengthen G7 coordination to identify and respond to diverse and evolving foreign threats to G7 democracies, including through sharing information and analysis and identifying opportunities for coordinated response. The G7 RRM's focus includes, but is not limited to, threats to democratic institutions and processes; disinformation and media; and fundamental freedoms and human rights. The mechanism has since expanded to include Australia, the Netherlands and New Zealand. G7 RRM information sharing was tested and proven in the COVID-19 context. The mechanism quickly shifted its focus to the pandemic, supporting a real-time exchange of analysis of foreign threats that included industry and civil society organization partners, particularly with respect to evolving foreign state-sponsored information manipulation.

Working with our international partners, we have also taken measures to publicly attribute foreign interference activities when appropriate. For example, in December 2018, Canada again joined partners in calling out the Chinese Ministry of State Security for the compromise of Managed Service Providers (MSPs). The Cyber Center reached out to MSPs in Canada to inform them of the threat and offer assistance.

The Government of Canada is committed to working with our partners and allies to share the critical information necessary to understand and counter the full spectrum and threat of foreign interference.

Protecting our citizens and our communities

Canada does not tolerate harassment or intimidation of its citizens. Any allegation of harassment or intimidation is taken seriously by the Government of Canada and will be dealt with appropriately.

Any Canadian who feels threatened or intimidated by a person acting on behalf of a foreign country is encouraged to contact their local police at the earliest possible opportunity. In instances where this threat rises to a level where individuals are concerned for their personal safety and security, it is essential that they report this information to local law enforcement agencies for their immediate action.

Through Integrated National Security Enforcement Teams our national security agencies investigate national security matters domestically and internationally. CSIS collects evidence and provides intelligence advice. The Police of Jurisdiction, including the RCMP, has the authority and expertise to investigate cases whereby the evidence supports it. Canadians who are concerned that they are being targeted by state and non-state actors for the purposes of foreign interference should contact the RCMP's National Security

Information Network at 1-800-420-5805, or by email at RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Canadians may also report information related to foreign interference to CSIS by contacting 613-993-9620, or by completing the web form at: www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html.

Our law enforcement and security agencies are actively engaged in protecting Canadians from these threats. Canadians should feel confident that they have the skills, resources and capabilities to do what it takes to keep them safe.

Moving Forward

Colleagues, I welcome the interest you and other members of the House of Commons have shown in how the Government of Canada addresses foreign interference. Bringing these issues to the attention of Canadians and raising awareness amongst stakeholders is key to countering this threat.

It is only through raising awareness, building resilience, forging partnerships with key stakeholders and seeking innovative ways of responding to threats that we will be successful in countering the evolving and complex nature of foreign interference. We are therefore always looking for new ways of doing things, and meeting this challenge head on.

This Government values above all the wellbeing and safety of Canadians. Whenever malign foreign states seek to harm our communities, undermine our values or jeopardize the very institutions on which our country is built, we will take action. We cannot always make Government actions public in this sphere, but our sustained efforts make a difference in the lives of Canadians.

Sincerely,

The Honourable Bill Blair, P.C., C.O.M., M.P.

Ministre
de la Sécurité publique
et de la Protection civile

Minister
of Public Safety
and Emergency Preparedness

Ottawa, Canada K1A 0P8

18 DEC. 2020

Chers collègues,

L'ingérence étrangère a été un sujet d'intérêt et de discussion à la Chambre des communes récemment.

Afin de répondre à la motion passée par la Chambre des communes le 18 novembre 2020, je vous écrit pour vous donner un aperçu des mesures que le gouvernement du Canada prend pour répondre aux menaces à la sécurité, à la prospérité, et aux institutions démocratiques de notre pays.

Puisque la Chambre est ajournée pour les vacances d'hiver, je veux m'assurer que vous avez quelque chose par écrit avant que la session recommence en 2021.

Il me fera plaisir de déposer le contenu de cette lettre de manière formelle le mois prochain.

D'abord et avant tout, le gouvernement ne tolère pas, et ne tolérera jamais, ce type d'activités.

Avant de vous expliquer quelques-unes des façons dont le gouvernement travaille à protéger les Canadiens et à contrer ces menaces et, je tiens à souligner qu'en ce qui concerne cette motion, en particulier l'alinéa b), le gouvernement du Canada s'efforce toujours à raffiner et à approfondir ses plans pour lutter contre l'ingérence étrangère au Canada.

Les travaux dans ce domaine durent depuis longtemps et se poursuivent. Cette motion donne l'occasion d'informer les Canadiens des mesures qui ont été prises tout en les assurant que nos agences s'adapteront toujours pour faire face à des menaces en évolution constante.

L'ingérence étrangère est une activité hostile menée par des États étrangers qui est délibérément secrète, malveillante, clandestine et trompeuse. Ces activités peuvent inclure des menaces, du harcèlement et de l'intimidation. Elles peuvent viser les Canadiens, ou les résidents du Canada, ou les institutions canadiennes pour promouvoir leurs intérêts stratégiques de ces États étrangers au détriment de nos intérêts et de nos valeurs nationaux. Les États étrangers hostiles dépassent les bornes chaque fois qu'ils vont au-delà la diplomatie standard pour mener des activités contre le Canada qui tentent de menacer nos citoyens, de compromettre notre mode de vie, de miner nos processus démocratiques ou de nuire à notre prospérité économique.

Canada

L'ingérence étrangère moderne représente une menace complexe. Elle constitue une menace importante pour l'intégrité de notre système politique, de nos institutions démocratiques, de notre cohésion sociale, de la liberté académique, de notre économie et de notre prospérité à long terme, ainsi que de nos droits et libertés fondamentaux. Elle peut aussi affecter la sécurité de nos citoyens et de ceux qui vivent ici. Ceci n'est pas nouveau, mais elle demeure inacceptable, puisqu'elle cible tous les ordres de gouvernement – fédéral, provinciaux et territoriaux, et municipaux, ainsi que les communautés canadiennes.

Les auteurs étrangers de la menace peuvent utiliser des opérations d'intelligence humaine, des médias parrainées par l'État ou sous influence étrangère, et des cyberoutils sophistiqués, entre autres, pour réaliser leurs objectifs. Ces objectifs comprennent la promotion de leurs intérêts, parfois à nos dépens, en vue d'obtenir une influence géopolitique, d'accroître leurs avantages économiques, d'avoir accès à la recherche, à la technologie ou à l'information de nature délicate, de réviser l'ordre international fondé sur des règles, d'accroître leur stabilité nationale, ou d'obtenir un avantage militaire.

Selon le rapport publique de 2019 du Service canadien du renseignement de sécurité (SCRS), les activités d'ingérence étrangère visent les entités canadiennes tant à l'intérieur qu'à l'extérieur du Canada et elles menacent directement la sécurité nationale et les intérêts stratégiques du Canada. De plus, le Rapport annuel du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) a donné un aperçu des activités d'ingérence étrangère, y compris comment elles ciblent les institutions canadiennes et certaines communautés.

Je note que le premier ministre a pris la décision importante de permettre la version déclassifiée et rendue publique de nommer, pour la première fois, spécifiquement la République populaire de Chine (RPC) et la Russie comme étant particulièrement actifs au Canada. L'intention était de sensibiliser le public aux menaces posées par ces pays. De plus, le rapport *Évaluation des cybermenaces nationales 2020* du Centre canadien pour la cybersécurité inclut aussi des références à ces pays, en plus de l'Iran et la Corée du Nord. Récemment, le Comité permanent de la sécurité publique et nationale a reçu le témoignage de M. Scott Jones, qui a déclaré que la décision de nommer ces pays dans les rapports n'est pas facile, mais qu'ultimement, il faut reconnaitre que ces pays posent un risque tout en travaillant à sensibiliser les Canadiens à ce sujet.

Grâce à une économie ouverte et stable, une main d'œuvre qualifiée et une infrastructure de pointe, le Canada est une destination attrayante pour les investisseurs étrangers. La grande majorité des investissements étrangers au Canada sont effectués de manière ouverte et transparente et sont bénéfiques pour l'économie canadienne. Toutefois, le gouvernement du Canada se préoccupe de plus en plus du fait que certains types d'opérations d'investissement effectués par des adversaires étrangers peuvent nuire à la sécurité nationale. Les investissements étrangers qui donnent à ces entités le contrôle ou l'accès à des technologies sensibles, des infrastructures essentielles ou des renseignements personnels de nature sensibles de plusieurs Canadiens sont particulièrement préoccupants.

Certains gouvernements et leurs mandataires sont prêts à utiliser des moyens illicites pour obtenir des biens, des technologies et des informations sensibles. Ces mandataires pourraient inclure des entreprises d'État, des particuliers associés aux institutions universitaires ou aux organisations commerciales ou à d'autres entités qui ne sont pas directement liées à un État lui-même, mais qui peuvent quand même servir ses intérêts.

Par exemple, les programmes de talents constituent une partie acceptable de l'entreprise de recherche moderne. Cependant certains auteurs étrangers de menaces peuvent les utiliser à des fins malveillantes. L'obligation de transférer ou de reproduire la recherche, ou l'obligation d'attribuer la recherche à des institutions étrangères, ou à dissimuler les associations à des services militaires ou du renseignement étrangers, constituent des exemples de moyens dont les intervenants étrangers, y compris la RPC, utilisent les programmes de talents pour acquérir des technologies et connaissances sensibles pour avancer leur intérêts économiques et de sécurité au détriment du Canada. Par exemple, le SCRS enquête activement sur les menaces d'ingérence étrangère et sur l'espionnage, et appuie l'effort collectif du gouvernement du Canada pour intervenir, y compris en prenant des mesures pour réduire la menace que posent des activités d'espionnage spécifiques, par l'entremise de son mandat légal.

De plus, certains États étrangers, y compris la RPC, tentent de menacer et d'intimider les individus partout dans le monde, y compris au Canada, par l'intermédiaire de diverses entités étatiques et de mandataires non étatiques. Nous dénonçons fortement ces actes, peu importe où ils ont lieu. Nous savons que les États peuvent chercher à menacer et à intimider les individus sous prétexte de lutter contre la corruption alléguée ou de traduire les criminels allégués en justice. Toutefois, nous savons que ces tactiques servent également de couverture pour réduire au silence la dissidence y compris sur des campus universitaires, pour exercer une pression sur les opposants politiques et pour provoquer une crainte générale du pouvoir de l'État, peu importe où se trouve une personne. L'opération *« Chasse aux renards »* de la RPC en est un exemple. La RPC utilise ce programme comme moyen d'identifier et d'essayer de rapatrier en Chine des particuliers qu'elle allègue être corrompus. La RPC a mené cette opération au Canada depuis 2014. Je note que selon le rapport de 2019 du CPSNR, la réponse initiale était souvent de travailler avec les autorités chinoises pour « appuyer leurs enquêtes sur les représentants corrompus. » Cependant, depuis 2015, des critères « de plus en plus rigoureux » ont été ajoutés pour les investigateurs de la République populaire de Chine impliqué dans ce programme.

Lorsque les États étrangers ciblent les Canadiens, des personnes qui résident au Canada ou leur famille, ils cherchent à priver les membres des collectivités canadiennes de leurs droits et libertés fondamentaux. De telles mesures sont inacceptables. Si quelqu'un se sent intimidé ou menacé, il est de la plus haute importance de contacter votre police locale, et je peux vous assurer que vos préoccupations seront traitées de manière sérieuse et appropriée.

Ingérence étrangère et la COVID-19

La pandémie de la COVID-19 a accéléré ces tendances en offrant aux auteurs de menaces étrangers des occasions uniques de poursuivre leurs activités hostiles. Les répercussions de la désinformation, de l'utilisation coercitive de menaces commerciales et économiques à la sécurité nationale et de menaces à la chaîne d'approvisionnement du Canada constituent des préoccupations continues.

Au cours de la dernière année, nous avons observé une manipulation de l'information par des États ou une désinformation par certains régimes contre le Canada et nos alliés. Ces campagnes visent à semer le doute quant aux origines du virus de la COVID-19 et aux moyens nécessaires pour le contrer; à discréditer les interventions à la COVID-19 tout en présentant les leurs comme étant supérieures; et à miner la confiance dans nos valeurs communes de démocratie et de droits de la personne.

La communauté canadienne de la sécurité et du renseignement, qui est à l'avant-garde des efforts déployés par le Canada pour lutter contre l'ingérence étrangère, prend des mesures coordonnées et intégrées pour protéger la sécurité et les intérêts stratégiques des Canadiens. Je tiens à vous donner un aperçu de ces efforts.

INTERVENTION CANADIENNE À L'INGÉRENCE ÉTRANGÈRE

Il n'y a pas de rôle plus fondamental pour le gouvernement que celui de protéger les Canadiens et les communautés. Le gouvernement prend cette responsabilité au sérieux. Même si je ne suis pas en mesure de faire part des renseignements opérationnels concernant les activités de lutte contre l'ingérence étrangère en cours, les Canadiens peuvent être assurés que le gouvernement du Canada adopte une approche pangouvernementale pour protéger les canadiens contre les menaces à la sécurité nationale, y compris les menaces aux institutions qui jouent un rôle clé dans l'intervention du Canada à la pandémie de la COVID-19.

Enquêtes et surveillance

Le SCRS mène depuis longtemps des enquêtes sur les activités de menace d'ingérence étrangère qui ciblent le Canada et utilise le mandat intégral de la *Loi sur le SCRS* pour enquêter, conseiller le gouvernement et prendre des mesures pour atténuer la menace. Le SCRS collabore étroitement avec d'autres partenaires gouvernementaux, à l'intérieur et à l'extérieur du milieu de la sécurité et du renseignement, pour lutter contre les activités d'ingérence clandestines, trompeuses ou menaçantes qui peuvent nuire considérablement aux institutions et aux processus démocratiques du Canada.

La Gendarmerie royale du Canada (GRC) a un mandat vaste et multidimensionnel qui lui permet d'enquêter les menaces provenant d'intervenants étrangers et de les neutraliser en s'appuyant sur diverses lois, y compris des enquêtes en vue de porter des chefs d'accusation en vertu du *Code criminel* du Canada.

Le Centre de la sécurité des télécommunications (CST) offre au gouvernement du Canada des renseignements et des cyberévaluations sur les intentions, les activités et les capacités des auteurs de menaces étrangers et il peut également mener des cyberopérations actives pour dégrader, perturber, réagir à ou interférer avec les capacités, les intentions ou les activités des particuliers, des États et des organisations étrangers. Le CST offre également des conseils, une orientation et des services pour assurer la protection des renseignements électroniques et des infrastructures d'information des institutions fédérales et des systèmes importants pour le gouvernement du Canada.

En outre, afin de contrer l'ingérence étrangère dans les élections fédérales de 2019, le gouvernement a mis sur pied le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, composé de représentants du CST, du SCRS, de la GRC et d'Affaires mondiales Canada (AMC). Tout au long de l'élection fédérale de 2019, le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections a sensibilisé au sujet des menaces d'ingérence étrangère et a évalué celles-ci, en informant les membres du Protocole public en cas d'incident électoral majeur du gouvernement du Canada au sujet de toute activité de menace afin de s'assurer que rien ne pourrait nuire à la capacité du Canada de tenir des élections libres et équitables. Le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections continue de surveiller les menaces liées à l'ingérence étrangère aux élections fédérales et de conseiller le gouvernement du Canada à ce sujet.

L'Agence des services frontaliers du Canada (ASFC) collabore étroitement avec ses partenaires pour veiller à ce que les particuliers qui représentent une menace pour la sécurité du Canada, dont ceux qui se livrent à des actes d'espionnage ou de subversion contre les gouvernements démocratiques, n'entrent pas au Canada. Les personnes qui sont déjà entrées et qui sont jugées interdites de territoire seront expulsées du Canada. Grâce à ses programmes rigoureux de renseignement et de la vérification de sécurité nationale, l'ASFC vise à détecter de telles personnes interdites de territoire à divers points du continuum des déplacements et à informer d'autres partenaires en matière de sécurité et du renseignement des menaces possibles.

Grâce aux enquêtes et à la surveillance, nous continuons de cerner et d'éclairer les multiples façons dont l'ingérence étrangère se manifeste au Canada, ce qui nous permet d'être bien armés, munis des connaissances nécessaires pour déployer nos outils pour la contrer.

Protection contre les menaces économiques à la sécurité nationale

Le gouvernement n'a jamais compromis et ne compromettra jamais la sécurité nationale du Canada et prendra les mesures pour la protéger, le cas échéant. Tel que cela est signalé dans le Rapport annuel 2018-2019 de la *Loi sur l'investissement Canada*, en ce qui concerne les quatre exercices de 2015-2016 à 2018-2019, le gouverneur en conseil a émis huit décrets définitifs en vertu de l'article 25.4 : six ont bloqué ou ont ordonné à l'investisseur étranger de se départir de son investissement, et deux imposaient des conditions qui protègent la sécurité nationale, tout en autorisant ces investissements.

Afin de protéger les Canadiens dans ce contexte économique actuel façonné par la COVID-19, le gouvernement du Canada a annoncé en avril 2020 qu'il examinerait de plus près tous les investissements étrangers directs, qu'ils soient contrôlés ou non, dans les entreprises canadiennes qui sont essentielles à la santé publique et à la sécurité de l'approvisionnement de biens et de services essentiels aux Canadiens ou au gouvernement du Canada. Le gouvernement a également annoncé que tous les investissements étrangers effectués par des entreprises d'État ou des investisseurs privés considérés comme ayant des liens étroits à des gouvernements étrangers ou comme étant assujettis aux directives de ces derniers, seraient assujettis à un examen plus approfondi en vertu des dispositions de la *Loi sur investissement Canada* portant sur la sécurité nationale.

Chaque année, le gouvernement du Canada achète des biens et des services d'une valeur d'environ 22 milliards de dollars. Il existe un potentiel pour les auteurs de menaces étrangers d'exploiter les processus d'approvisionnement en leur faveur. Les entreprises d'État utilisent leurs vastes ressources comme un avantage concurrentiel qui leur permet de présenter des soumissions moins élevées de celles des entreprises canadiennes et de s'insérer dans notre infrastructure et nos services et de compromettre notre sécurité. Le gouvernement est résolu à lutter contre ces menaces à la sécurité nationale liée à l'approvisionnement. Par exemple, nous travaillons à accroître la sensibilisation au risque et à assurer la diligence raisonnable tout au long du processus d'approvisionnement. Ces travaux ont compris l'élaboration de documents d'orientation sur la sécurité nationale, lesquels ont été distribués aux employés des ministères et des organismes dont les fonctions comprennent les activités d'approvisionnement ou qu'elles sont touchées par ces dernières, ainsi qu'aux provinces et aux territoires, et à l'Alliance des villes Canada, qui représentent 12 des plus grandes villes du Canada.

Le gouvernement du Canada est au courant des tentatives que font actuellement certains États étrangers pour miner notre économie à leur propre profit. Nos nombreux efforts pour contrer ces menaces contribuent à protéger la prospérité des Canadiens et à maintenir le Canada en tant que chef de file économique.

Protéger notre démocratie

En janvier 2019, le gouvernement a annoncé son plan de défense de la démocratie canadienne contre les menaces avant la 43e élection générale. Ce plan est fondé sur quatre piliers de soutien communs :

1. *Améliorer l'état de préparation des citoyens* en appuyant une population informée et mobilisée;

2. *Renforcer la préparation organisationnelle* en renforçant la coordination en vue de cerner les menaces, les nouvelles tactiques et les vulnérabilités des systèmes;

3. *Lutter contre l'ingérence étrangère* en empêchant les activités secrètes, clandestines ou criminelles exercées par les intervenants étrangers visant à perturber nos processus démocratiques;

4. *Compter sur les plateformes des médias sociaux pour qu'elles agissent* pour orienter les plateformes sociales et numériques pour assurer l'intégrité, la transparence et l'authenticité.

Le plan a été reconnu à l'échelle internationale pour illustrer le leadership du Canada dans la lutte contre l'ingérence étrangère dans les processus démocratiques et les éléments clés sont en cours d'évaluation aux fins de leur mise en œuvre continue.

De plus, la *Loi électorale du Canada* contient des dispositions visant à protéger le processus électoral fédéral, y compris des règlements rigoureux concernant les contributions financières et non financières aux intervenants politiques et les interdictions de corrompre ou d'intimider les électeurs. La *Loi sur la modernisation des élections*, qui a reçu la sanction royale en décembre 2018, a renforcé davantage la protection contre l'ingérence étrangère au moyen de modifications qui :

- interdissent à des tiers d'utiliser des fonds étrangers pour leurs activités partisanes et leurs publicités, quel que soit le moment où elles ont lieu;
- interdisent aux entités étrangères de dépenser de l'argent pour influencer les élections fédérales;
- exigent que des tiers enregistrés aient un compte bancaire canadien;
- interdissent à toute organisation – en ligne ou hors ligne – qui vend de l'espace publicitaire de publier sciemment des publicités électorales payées avec des fonds étrangers.

Une période préélectorale a également été fixée, établissant des plafonds de dépenses pour les tiers et a soumis les tiers à des obligations accrues en matière d'établissement de rapports. Afin d'améliorer la transparence, la loi modifiée exige également que les plateformes en ligne, comme les sites de médias sociaux publient un registre de toutes les publicités partisanes ou politiques qu'ils ont affichées, y compris qui a autorisé les publicités et de veiller à ce que les renseignements soient disponibles pendant au moins deux ans après la publication des publicités.

Alors que les processus démocratiques étaient ciblés dans de nombreux pays par des auteurs de menaces étrangers, il était clair que le Canada devait prendre des mesures ici au pays. En conséquence, nous avons pris ces mesures clés pour renforcer le caractère rigoureux de nos institutions démocratiques et électorales afin de lutter directement contre cette menace.

Communiquer avec les Canadiens

Les mesures que le gouvernement prend pour contrer l'ingérence étrangère sont souvent prises en coulisses, étant donné le caractère délicat des outils et des techniques utilisés. Toutefois, compte tenu de l'ampleur de l'ingérence étrangère et de ses répercussions sur tant de secteurs de la société, nos organismes se sont engagés auprès des Canadiens pour les aider à reconnaître les signes qu'il faut rechercher et savoir qui appeler lorsqu'ils surviennent.

À cet égard, le SCRS mène des séances d'information destinées aux entreprises privées, aux universités et aux établissements de recherche pour les aider à mieux comprendre comment protéger leur travail. Dans le contexte de la pandémie, les organismes canadiens de sécurité et du renseignement ont rapidement collaboré avec les secteurs de sciences de la vie participant à l'intervention du Canada à la COVID-19 pour aider à les protéger contre les activités d'ingérence étrangère. Par exemple, le SCRS a entrepris une campagne nationale de sensibilisation visant à renseigner ces secteurs à la menace à laquelle ils pourraient être confrontés en raison de l'ingérence étrangère.

La GRC collabore également avec l'Association canadienne des chefs de police pour aider à informer les organismes locaux d'application de la loi des menaces provenant de l'ingérence étrangère et à établir des mécanismes pour signaler les incidents d'ingérence étrangère.

En ce qui concerne l'ingérence étrangère et d'autres cybermenaces, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) du CST a récemment publié le rapport *Évaluation des cybermenaces nationales 2020*, qui met en évidence les cybermenaces auxquelles sont confrontés les particuliers et les organisations au Canada afin d'aider les Canadiens à façonner et à maintenir la cyberrésilience de notre nation. Cela comprend les menaces d'activités parrainées par des pays comme la RPC, visant le cyberespionnage, le vol de propriété intellectuelle, les opérations d'influence en ligne et les cyberincidents perturbateurs. Le Centre pour la cybersécurité offre également des conseils et des pratiques exemplaires en matière de cybersécurité, y compris par l'entremise de la campagne de sensibilisation et d'éducation publique de Pensez cybersécurité du CST.

Le gouvernement est résolu à continuer de collaborer avec les Canadiens sur la question de l'ingérence étrangère afin d'accroître la sensibilisation et de renforcer la résilience.

Protéger les connaissances et la recherche canadiennes

Le gouvernement du Canada s'est engagé à créer un environnement ouvert et collaboratif pour la science et la recherche, et à reconnaître l'importance de la science ouverte comme essentielle aux découvertes et à l'innovation en recherche. En même temps, les activités d'espionnage et d'ingérence étrangère constituent une menace réelle pour l'intégrité de la recherche, la propriété intellectuelle et les intérêts commerciaux du Canada.

Les universités, les ministères, les conseils subventionnaires fédéraux et les organismes de sécurité nationale sont régulièrement en contact dans le cadre des activités de mobilisation continues et collaborent en vue de comprendre et de cerner les menaces possibles à la sécurité de la recherche et d'y répondre. Ce dialogue comprend un groupe de travail mixte du gouvernement du Canada et des universités qui facilite la détermination, l'échange et la promotion des pratiques exemplaires afin de réduire au minimum les risques pour la sécurité, de protéger les données et la propriété intellectuelle.

Dans le cadre de ce travail, le gouvernement du Canada et le secteur universitaire ont collaboré à l'élaboration et au lancement d'un portail de ressource en ligne intitulé « Protégez votre recherche ». Le portail fournit des renseignements, des pratiques exemplaires et des outils pour aider les chercheurs à cerner et à atténuer les risques possibles pour la sécurité de leur travail. Cette année, le SCRS a offert une séance d'information à la Chambre de Commerce du Canada qui a souligné que la Chine et la Russie étaient particulièrement actives en activités d'espionnage économique.

Reconnaissant la menace élevée que représentent les intervenants étrangers qui ciblent la recherche liée à la COVID-19 au Canada, le gouvernement du Canada a également publié un énoncé de politique sur la sécurité de la recherche – signé par le ministre de l'Innovation, des Sciences et de l'Industrie, la ministre de la Santé et moi-même – en septembre 2020. L'énoncé fait état des menaces possibles pour la sécurité de la recherche et de la nécessité de prendre les mesures appropriées pour protéger la recherche et l'innovation, surtout dans le contexte de la COVID-19.

De plus, le gouvernement a chargé les organismes fédéraux de financement de la recherche, y compris, la Fondation canadienne pour l'innovation, les Instituts de recherche en santé du Canada, et le Conseil de recherches en sciences naturelles et en génie et le Conseil de recherches en sciences humaines, d'examiner leurs politiques et leurs processus de sécurité et de promouvoir la sensibilisation aux pratiques exemplaires et aux outils à la disposition des chercheurs et des innovateurs canadiens qu'ils financent, afin que le Canada, plutôt que nos adversaires, maximise les avantages des investissements importants du gouvernement dans les sciences et la recherche.

De plus, une mobilisation directe entre les universités canadiennes, les laboratoires fédéraux et les établissements de sécurité au sujet des risques que présente l'ingérence étrangère est en cours depuis 2016 dans le cadre de l'initiative Science en sécurité dirigée par Sécurité publique Canada, en partenariat avec 10 autres ministères fédéraux.

Cette initiative vise à sensibiliser les milieux de la recherche du Canada aux risques de prolifération; de la technologie à double usage; à la sécurité de la recherche; et à la cybersécurité. L'initiative informe les participants des outils qui permettent de reconnaître et d'atténuer les risques auxquels sont confrontées les institutions canadiennes, y compris ceux concernant leur recherche et développement. Jusqu'à présent, des présentations de Science en sécurité ont été données à 33 institutions et à cinq laboratoires fédéraux partout au pays. Des efforts d'expansion sont également en cours pour fournir des outils et des conseils supplémentaires au milieu de la recherche,

ainsi que d'autres ateliers d'un océan à l'autre et au sein du secteur privé et avec des partenaires provinciaux et territoriaux.

Sécurité publique Canada a également mis sur pied une Communauté de pratique fédérale, provinciale et territoriale sur les menaces à la sécurité nationale fondées sur l'économie afin de réunir des représentants clés de ces juridictions pour discuter des menaces à la sécurité nationale qui découlent de certaines activités économiques.

Le milieu de la recherche multidisciplinaire du Canada est reconnu à l'échelle mondiale. Grâce aux bons outils et à la sensibilisation aux risques possibles, nous pouvons nous assurer que le Canada continue de tirer profit de nos investissements importants dans la science et la recherche.

Je note que cette semaine, il a été rapporté que le SCRS s'est entretenu avec des partenaires gouvernementaux et des entreprises impliqués dans la chaîne d'approvisionnement en vaccins et d'autres produits médicaux et a mené des séances d'information destinées à ces derniers. Je peux vous assurer que nos organismes continueront de travailler en étroite collaboration avec nos partenaires pour veiller à ce que le plus grand nombre possible d'entreprises et d'ordres de gouvernement disposent des informations dont ils ont besoin pour mettre en œuvre des mesures de sécurité préventives permettant d'identifier et d'atténuer toute menace.

Collaboration internationale

Le Canada ne peut pas lutter seul contre l'ingérence étrangère. Nos alliés et partenaires internationaux sont confrontés à des menaces semblables. Par conséquent, en collaborant, nous rassemblons donc nos ressources collectives pour contrer les menaces provenant d'intervenants étrangers. Le Canada a toujours défendu un ordre international fondé sur des règles, dans lequel tous les pays respectent les normes internationales. Conformément à ces principes, le Canada partage activement de l'information et coordonne les réponses avec ses alliés par l'intermédiaire de nombreux organismes multilatéraux et de relations.

En tant que membre de la réunion ministérielle des cinq pays, je me suis engagé à collaborer avec mes homologues des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande relativement à la question de l'ingérence étrangère, afin d'échanger des informations sur nos approches respectives et de coordonner les interventions et l'attribution, selon ce qui convient.

Les partenaires de la sécurité et du renseignement collaborent également pour échanger des renseignements dans le but de contrer l'ingérence étrangère, y compris la désinformation parrainée par l'État, à l'aide de plusieurs forums. Par exemple, le milieu de la sécurité et du renseignement collabore avec des partenaires nationaux et internationaux pour échanger des renseignements qui peuvent contribuer à détecter, à enquêter et à prévenir l'ingérence étrangère au Canada.

Affaires mondiales Canada dirige le Mécanisme de réponse rapide du G7. En 2018, les dirigeants du G7 se sont engagés à collaborer en vue de renforcer la coordination du G7 afin de déterminer les diverses menaces étrangères et en évolution aux démocraties du G7 et d'y répondre, notamment en partageant des renseignements et des analyses et en déterminant des possibilités d'une intervention coordonnée. L'objectif du MRR du G7 comprend, sans toutefois s'y limiter, les menaces aux institutions et aux processus démocratiques; la désinformation et les médias; ainsi que les droits de la personne et les libertés fondamentaux.

Le mécanisme a depuis été élargi en vue d'inclure l'Australie, les Pays-Bas et la Nouvelle-Zélande. L'échange de renseignements du MRR du G7 a été mis à l'essai et a fait ses preuves dans le contexte de la COVID-19. Le mécanisme a modifié rapidement son objectif afin de se concentrer sur la pandémie, en appuyant un échange en temps réel d'analyse des menaces étrangères qui comprenait les partenaires de l'industrie et des organisations de la société civile, surtout en ce qui concerne l'évolution de la manipulation de l'information parrainée par les États étrangers.

En collaboration avec nos partenaires internationaux, nous avons également pris des mesures pour attribuer publiquement les activités d'ingérence étrangère, le cas échéant. Par exemple, en décembre 2018, le Canada a de nouveau collaboré avec ses partenaires pour accuser le ministère chinois de la Sécurité d'État d'avoir compromis les fournisseurs de services gérés. Le Centre pour la cybersécurité a communiqué avec les fournisseurs de services gérés au Canada pour les informer de la menace et pour leur offrir de l'aide.

Le gouvernement du Canada est résolu à collaborer avec nos partenaires et nos alliés afin d'échanger les renseignements essentiels nécessaires pour comprendre et contrer l'éventail complet et la menace d'ingérence étrangère.

Protéger nos citoyens et nos communautés

Le Canada ne tolère ni le harcèlement ni l'intimidation de ses citoyens. Toute allégation d'un tel harcèlement ou d'une telle intimidation est prise au sérieux par le gouvernement du Canada et sera traitée de manière appropriée.

Tous les Canadiens qui se sentent menacés ou intimidés par une personne agissant au nom d'un pays étranger sont encouragés à communiquer le plus tôt possible avec la police locale. Pour les cas où cette menace atteint un niveau tel que les personnes s'inquiètent de leur sécurité personnelle, il est essentiel de communiquer toute information aux organismes locaux d'application de la loi pour qu'ils puissent prendre des mesures immédiates.

Par l'entremise des Équipes intégrées de la sécurité nationale, nos organismes de sécurité nationale enquêtent sur les questions de sécurité nationale au niveau national et international. Le SCRS entreprend la collecte de preuves et offre des conseils reliés aux renseignements. Les services de police compétents, y compris la GRC, ont l'autorité et l'expertise pour enquêter les cas où les preuves le justifient. Les Canadiens qui craignent être ciblés par des intervenants étatiques et non-étatiques aux fins d'ingérence étrangère

devraient communiquer avec le Réseau info-sécurité nationale de la GRC au 1-800-420-5805 ou par courriel à l'adresse RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Les Canadiens peuvent également signaler des renseignements liés à l'ingérence étrangère au SCRS en composant le 613-993-9620 ou en remplissant le formulaire Web à l'adresse suivante : https://www.canada.ca/fr/service-renseignement-securite/organisation/signaler-des-informations-relatives-a-la-securite-nationale.html.

Nos organismes d'application de la loi et de sécurité s'emploient activement à protéger les Canadiens contre ces menaces. Les Canadiens devraient être assurés que ces derniers ont les compétences, les ressources et les capacités nécessaires pour faire ce qu'il faut afin de les protéger.

À l'avenir

Chers collègues, je me réjouis de l'intérêt que vous et d'autres députés de la Chambre des communes avez manifesté relativement à la façon dont le gouvernement du Canada lutte contre l'ingérence étrangère. Il est essentiel de porter ces questions à l'attention des Canadiens et de sensibiliser les intervenants pour contrer cette menace.

Ce n'est qu'en sensibilisant, qu'en renforçant la résilience, qu'en établissant des partenariats avec des intervenants clés et qu'en cherchant des moyens novateurs de répondre aux menaces que nous réussirons à contrer la nature évolutive et complexe de l'ingérence étrangère. Nous sommes donc toujours à la recherche de nouvelles façons de faire les choses et de relever ce défi de manière directe.

Le gouvernement privilégie d'abord et avant tout le bien-être et la sécurité des Canadiens. Lorsque des États étrangers malveillants cherchent à causer des préjudices à nos collectivités, à miner nos valeurs ou à compromettre les institutions sur lesquelles notre pays est bâti, nous prendrons des mesures. Nous ne pouvons pas toujours rendre publiques les mesures que le gouvernement prend dans ce domaine, mais nos efforts soutenus font une différence dans la vie des Canadiens.

Veuillez accepter mes meilleures salutations.

L'honorable Bill Blair, C.P., C.O.M., député