FI Briefing to Parliamentarians – Script

UPDATED June 11, 2024

[APG]

Intro (PS LEAD)

- Good (morning/evening) everyone.

- We are honoured to be here today to discuss the threat of foreign interference and what this means for you.

- We are holding this briefing at the request of the Sergeant-at-Arms.

- It is designed to provide foundational knowledge on the threat. We'll discuss why you may be considered as targets of interference from foreign states, what methods the threat actors are using, and how you can better protect yourselves.

- I'm sure some you will be familiar with a lot of the material in this briefing, but it still beneficial to make sure that caucus members share the same foundational understanding of foreign interference.

- Foreign interference is a serious threat that undermines Canada's national interests, economic prosperity and values. It also affects the safety of Canadians, and their ability to exercise their fundamental democratic rights and freedoms.

- The better informed we are about the threat, the more resilient we'll be against it.

[APG]

- The format of this presentation will be a 22-25 min presentation with me, as the national counter foreign interference coordinator at Public Safety, and with colleagues from the Canadian Security Intelligence Service, the Canadian Centre for Cyber Security, and the Royal Canadian Mounted Police. We will then take the rest of the session to take questions and comments.

SLIDE 1: What is Foreign Interference (PS LEAD)

- (read definition)

- Foreign interference can take many forms, including threats against Canadian communities by repressive governments, meddling in democratic institutions and processes, covert influence activity, and economic interference.

- (highlight the distinction between overt influence/advocacy, and malign influence/interference)

SLIDE 2: Who are the Prominent Threat Actors (CSIS LEAD)

- Merci. As Sebastien noted I am Bo Basler, Director General and the Foreign Interference Coordinator at CSIS. Je suis accompagné aujourd'hui par mon collègue , président du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (le MSRE), qui est actuellement hébergée au SCRS et fait partie intégrante de notre infrastructure de sécurité électorale.

[APG]

- Divers acteurs étatiques hostiles se livrent à de l'ingérence électorale contre le Canada. On va se concentrer sur les principaux acteurs : la Chine, l'Inde, la Russie et l'Iran.

- **The People's Republic of China (PRC)** conducts foreign interference operations around the world including here in Canada. The government does this to further their strategic objectives. In Canada, the PRC uses overt and clandestine means to ensure Canada either supports or is neutral with respect to the PRC's political and economic interests. the PRC government also wants to make sure that the public narrative on China is positive, and is trying to undermine critics of the PRC, regardless of who or where they are.

- Another prominent objective of PRC political FI is to ensure that **you** and elected officials at all levels of government do not endorse or support what the PRC terms 'the Five Poisons' - Taiwanese independence, Tibetan independence, Xinjiang separatists, the Falun Gong, and the Chinese democracy movement or those generally perceived to be working against the interest of the Chinese government.

- The PRC leverages some of its *officials in Canada* and uses proxies in Canada to conduct interference activities, stifle criticism and influence Canadian communities to act as a block to further their interests.

- **India** interferes in our democratic processes in order to ensure a pro-India narrative is promoted and to counter activities by some

[APG]

communities that are viewed as counter to their national interests, such as advocacy for an independent Sikh homeland called Khalistan.

- As part of its FI operations, **Russia** carries out disinformation and propaganda efforts in the West to advance its strategic objectives. Russian intelligence services (RIS) and other state-linked actors conduct disinformation campaigns to:
    - Question the integrity of— and undermine public faith in— Western democratic institutions
    - Sow discord, stoke fear and anxiety, and weaken cohesion in Western democracies. For instance, over support for Ukraine.

- Lastly, **Iranian FI** efforts are guided by the central goal of regime preservation. Iran does not tolerate any domestic dissent or criticism or advocacy against the regime that calls into question the basic tenets of Iran's political system. The Iranian regime regards Canada-based criticism, lawful advocacy and dissidents as threats to suppress.

SLIDE 3: Elected and Public Officials (PS LEAD)

- Certain states, including the People's Republic of China, seek to manipulate and abuse Canada's democratic system to further their own national interests, or to discredit Canada's democratic institutions and erode public confidence.

[APG]

- Threat actors have sought to clandestinely target politicians, political parties, electoral nomination processes, and media outlets in order to influence the Canadian public and democratic processes.

- Elected and public officials are central figures in our democracy's political system. Ultimately, you, as elected officials shape our policies and laws, are key targets for foreign states, which may try to influence or coerce you to take policy positions that align with their interests.

SLIDE 4: What threat actors want from you (PS LEAD)

(follow slide bullet points)

SLIDE 5: Methods used by threat actors (CSIS LEAD)

[APG]

- While each of you because you are an elected official is of interest to foreign states, only some of you would be the focus of foreign interference operations, and this will depend on your role, your network, your constituencies, or your stance on issues of importance to a foreign government. If you are subject to interference operations, it can take multiple forms, or it can target different communities around you. Sometimes threat actors do this themselves or sometimes they use others as proxies, both witting and unwitting, to conduct FI on their behalf and they target not only federal officials, but provincial, municipal, indigenous officials as well in order to achieve their objectives. We have seen the following activities here in Canada and our partners have seen similar activities in allied nations. Different countries may not use all of the following techniques as each country operates a little differently.

- **A few examples of techniques that are directed towards elected or senior officials that I will address are:**
  - Elicitation;
  - Cultivation;
  - Coercion;
  - Illicit and corrupt financing;

    While my colleagues from CSE will address
  - Cyber attacks; and
  - Disinformation

- **Elicitation** is when a targeted individual is manipulated into sharing valuable information through casual conversation.

[APG]

- For example, someone could knowingly share incorrect information with you, in the hope that you will correct them, or they might share some form of seemingly sensitive information with you in the hopes that you will do the same – a technique referred to as the "give to get" principle.

- **Cultivation:** Effective adversaries seek to build long-lasting, deep, and even romantic relationships with targets.
    - Sometimes foreign-interference actors develop relationships over years, while often concealing the depth of their connection to a foreign state. Elected officials, including yourselves and your staff, are targets for this kind of activity.

    - How to avoid it: Be aware and keep track of unnatural social interactions, frequent requests to meet privately, out-of-place introductions or engagements, gifts such as expense-paid travel, or odd requests for employment with your office.

- **Coercion** such as blackmail and threats are the two most aggressive forms of FI.
    - If an adversary can acquire compromising or otherwise embarrassing details about your life, they may seek to blackmail you with it. This can occur after a long period of cultivation and relationship-building.

    - Sometimes they may attempt to put you in a compromising situation, so they can blackmail you with it later.

[APG]

- How to avoid it: Avoid sharing overly-personal information with untrusted individuals, both in-person and online. Avoid placing yourself in a compromising situations, and seek help if someone is threatening or blackmailing you.

- **Illicit and corrupt financing** are inducements that aim to secure your cooperation and influence your position.

  - We have seen political parties and candidates receive donations, seemingly from a Canadian, though actually originating from a foreign threat actor like the PRC and India.

  - How to avoid it: Be aware of inappropriate requests which involve money, and question the source of suspicious donations or "gifts".

- I will now pass to my CSE colleague.

NOTES for Q&A: A recent example of political FI - Christine Lee:

- *I would like to present you a recent concrete case of political inference reported via the British press. Early 2022, Christine Lee was the subject of a public British Security Service (MI5) Interference Alert. Lee, a London based lawyer, was the chief legal adviser to the Chinese embassy in London and served several groups promoting contacts between China and overseas Chinese communities. She is a prominent example of a political interference targeting a Western democracy.*

[APG]

- *Over years, UK Labour MP Barry Gardiner had befriended Lee who unknowingly to him was, acted as a Chinese agent aspiring to interfere in UK politics. Lee's firm has given more than £427,000 in financial support to MP Gardiner since 2015. Lee's friendship with Gardiner gave her access across the highest levels of political spectrum. She facilitated financial donations to political parties, Parliamentarians, aspiring Parliamentarians and individuals seeking political office in the UK, including facilitating donations to a political entities on behalf of foreign nationals.*

- *Her activities had been undertaken in covert coordination with the United Front Working Department (UFWD), with funding provided by foreign nationals located in China and Hong Kong. The UFWD is alleged to be seeking to cultivate relations with influential figured to ensure the UK political landscape is favourable to the Chinese Communist Party (CCP).*

- *It is difficult at this point to determine how the British security services have engaged MP Gardiner on the activities of Lee and how much of the threat he was made aware of. However, the case illustrates the way the Chinese state operates - a willingness to wait years for efforts to pay off, in potentially cultivating people at local level and at the outset of their political career. We invite you to be extremely vigilant on who is seeking to make contact with you and to be proactive in reporting those contacts back to us.*

SLIDE 6: Cyber Threats to Parliamentarians (CSE Lead)

[APG]

- Foreign adversaries are trying to influence Canada's democracy in various ways, including espionage, malicious cyber activity and online disinformation. As Parliamentarians, you and your staff are at risk of foreign states targeting your devices, tracking your activities, and stealing your information.

- Online disinformation has become ubiquitous. In the past two years, in every national election, around the world, we have observed mis and disinformation targeting the democratic process.

- Threat actors are increasingly using AI to create, spread and amplify disinformation. **We've assessed that it is very likely that foreign adversaries or hacktivists will use generative AI to influence voters ahead of Canada's next federal election.**

- Equally, we assess that deepfakes will almost certainly increase in the next two years, as this technology becomes more widely available. Synthetic content is already very difficult to detect and is getting harder still. This makes it harder for Canadians to trust online information about politicians or elections.

- While Canada is not a primary target for Chinese, Russian or other nation-state's information operations, these countries will opportunistically amplify and distort events implicating Canada, especially if there are bilateral tensions between Canada and these states.

[APG]

Notes for Q & A - APT31 example

- *The threat of nation-state targeting of government officials has recently been the subject of international news.*
- *In April, the US and UK filed charges and imposed sanctions on a company and individuals tied to a PRC hacking group named APT31.*
- *Since at least 2015, this PRC hacking group has sent thousands of malicious emails to the personal and professional email accounts of government and political officials in allied countries.*
- *This email targeting is highly sophisticated; email messages appear benign but contain an embedded tracking link which the user cannot see, and does not need to click to activate.*
- *Unbeknownst to the recipients, by simply opening these malicious emails, the PRC received information on their location, IP address, and the devices they used to access the email.*
- *Using this information, the PRC can launch more targeted, sophisticated cyber attacks to exploit the user's specific devices and network configurations.*
- *In 2021, the PRC targeted the email accounts of various officials who were part of the Inter-Parliamentary Alliance on China, or IPAC. This group – which consists of parliamentarians from around the world -- works to counter the threat posed by the Chinese Communist Party to the international order.*
- *Through its malicious email activity, the PRC has gained and maintained access to networks, and has stolen information including economic plans, intellectual property, and trade secrets.*

[APG]

SLIDE 7: How to protect your digital self (CSE LEAD)

- Because of your position, you are targeted by China and other sophisticated foreign cyber actors. Act accordingly. As a rule of thumb assume your online activities are being monitored.

- Whenever possible, use your Government of Canada provided phone, tablet, laptop. This gives you the highest degree of protection. Your government devices are hardened against attack by the Cyber Centre.

- Don't click on suspicious links or attachments. Call or text to verify the message is authentic.

- When using a personal Apple device, use lockdown mode.

- Also for your personal devices, use anti-virus or anti-malware software.

SLIDE 8: How to protect your social self (CSIS LEAD)

- Be discreet, avoid "over-sharing", and assume public conversations are monitored.
    - Do not discuss anything sensitive over a phone or near a phone or any wireless device, over open email or unencrypted messaging apps. Do not store sensitive or classified information on a device that connects to the internet.

[APG]

I appreciate this is very difficult for someone whose job it is to discuss public policy with their constituents. So what is important here is understanding what is sensitive and what is publicly available, and to apply the right level of protection to guard for this information. In essence, know what the crown jewels are what is for private knowledge.

- Be aware and keep track of unnatural social interactions, frequent requests to meet privately, out-of-place introductions or engagements, gifts such as offers of all expenses paid travel.

- Know what you are sharing online. For hostile states, the collection of open information is the easiest and often first strategy to obtain information. Some countries have sophisticated big data collection platforms and collect personal information from hacked datasets they have hacked or bought off the dark web, they then pool this information, analyze it with artificial intelligence which informs tailored, spearphishing messages which can facilitate access to all your electronic devices.

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

SLIDE 9: New Ministerial Direction

(PS LEAD)

[APG]

SLIDE 10: RCMP

- The RCMP is mandated (Security Offences Act) to prevent, investigate and disrupt illegal activities related to foreign interference in Canada
- The RCMP' established Foreign Actor Interference Team (FAIT) within the Federal Policing National Security (FPNS) program in 2019 to detect, investigate, and disrupt foreign interference.

- The RCMP works closely with our domestic and international law enforcement and intelligence partners, including Five Eyes, to take a comprehensive approach to counter foreign interference threats.

- RCMP investigators consider all Acts of Parliament with enforcement capability, including the Criminal Code and the Security of Information Act (SOIA). Multiple foreign interference investigations have led the RCMP to lay charges under these Acts.

- Currently, the RCMP has over 100 investigations into foreign actor interference activities in a range of key target areas, such as economic integrity, critical infrastructure, proliferation, transnational repression, theft of intellectual property, theft of protected information, or targeting democratic institutions.

- The RCMP also engages with at-risk communities through outreach and awareness initiatives as part of our efforts to counter FI.

SLIDE 11: SITE Task Force (CSIS Lead)

[APG]

- Le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (MSRE) a été mis sur pied avec le mandat de se concentrer sur l'examen de l'ingérence étrangère dans les élections. Il veille à la coordination de l'échange d'information, de l'harmonisation et de la sensibilisation concernant les questions liées à l'ingérence étrangère et aux élections. Le Groupe de travail MSRE a été actif durant les élections fédérales de 2019 et de 2021.

    - Il est composé de membres de 4 agences fédérales : le Service canadien du renseignement de sécurité (SCRS), le Centre de la sécurité des télécommunications (CST), Affaires mondiales Canada (AMC) et la Gendarmerie royale du Canada (GRC). Des membres du Bureau du Conseil privé participent à titre d'observateurs.

- Le Groupe de travail MSRE surveille, parallèlement à l'ingérence étrangère, les menaces terroristes intérieures dans le contexte de leurs répercussions possibles sur la sécurité des élections.

- Plus récemment, le Groupe de travail MSRE a également reçu le mandat d'être actif pendant les élections partielles fédérales incluent pendant l'un de Toronto St. Paul.

- Comme mentionné déjà, le SCRS préside actuellement ce groupe de travail.

[APG]

SLIDE 12: Where to Turn to (PS LEAD)

- Both the RCMP and CSIS have phone numbers and online reporting mechanisms that are monitored 24/7 for anyone who would like to report a threat to national security, including foreign interference.
- Should individuals ever be concerned for their personal safety and security, it is essential that they contact their local police for immediate action.
- CSIS' tip line is 613-993-9620, toll-free at 1-800-267-7685. The TTY/TDD number is 613-991-9228. The online reporting mechanism is on CSIS' web page under "Reporting National Security Information."

SLIDE 13: Questions

SLIDE 14: Additional Resources

[APG]