THREATS TO PARLIAMENTARIANS – Be Alert

UNCLASSIFIED//FOR OFFICIAL USE ONLY

April 2023

FOREIGN INTERFERENCE AND ESPIONAGE

Foreign interference (FI) and espionage relate to clandestine, deceptive or threatening activities by foreign states against Canadians and Canadian institutions to advance foreign interests to the detriment of Canada. States conduct and direct threat activities against all levels of government in Canada to for strategic, military, intelligence and economic gain; regime preservation; or to discredit liberal-democratic institutions.

Elected officials are of high interest to foreign actors.

- You possess or have access to information they want;
- You are in a position to influence government policy and public opinion/discourse.

COMMON FI AND ESPIONAGE TECHNIQUES

Elicitation takes place when you are being manipulated into sharing valuable information. For example, a threat actor could knowingly seek to provide you with incorrect information, in the hope that you will correct them, thereby inadvertently disclosing sensitive information.

Effective threat actors seek to build and exploit relationships of trust through **cultivation.** These relationships enable the manipulation of targets directly or using proxies to gather information or exert influence.

The use of **blackmail and threats** represent aggressive forms of recruitment and coercion. Threat actors could threaten to reveal compromising information, your chances for election, or even the personal safety of your or your family, especially if your family is not in Canada.

Threat actors may seek to use you as a proxy to conduct **illicit financing** on their behalf. Inducements may occur innocuously via a simple request for a favor.

Adept state actors can use **cyber attacks and online disinformation campaigns** to access information, influence you or your constituents, or punish you for perceived threats to their interests in Canada.

INCIDENTS HIGHLIGHTING THE THREAT

April 2023: Pro-Russian hackers disabled multiple Government of Canada and parliamentary websites. The attack coincided with the visit of the Ukrainian Prime Minister to Canada.

April 2023: A Florida court indicted four American citizens and three Russian nationals with working with the Russian government and Russian intelligence services on a multi-year malign influence campaign that included elections interference.

January 2022: British intelligence issued an alert warning MPs that a high-profile lawyer, Christine Lee, was engaged in political interference activities on behalf of the United Front Work Department of the Chinese Communist Party.

November 2020: Former Australian MP Di Sanh Duong was charged with preparing for an act of foreign interference. Duong is accused to have used donations to cultivate a relationship with a federal minister with the ultimate goal of influencing Australian government policy to the advantage of China.

VIOLENT EXTREMISM

A body of reporting indicates a broad trend of rapidly increasing threats to Canadian politicians and their close associates. This includes online threats, confrontations, vandalism and other physically intimidating behaviours. While more physical intimidation tactics are likely, serious extremist violence is also possible and could occur without warning.

The Integrated Terrorism Assessment Centre (ITAC) assesses that **an act of terrorism targeting a parliamentarian or public official in Canada COULD OCCUR**. An ideologically motivated violent extremism (IMVE) lone actor remains the primary terrorist threat.

Past attacks and attempted attacks on elected officials in Western countries indicate that party leaders, outspoken proponents of controversial initiatives, and officials with whom a pre-existing grievance or fixation exists are the most likely targets of an extremist attack. However, when capability is limited or primary targets are out of reach, more accessible but public figures could be targeted symbolically.

POSSIBLE MANIFESTATIONS OF THE THREAT

Online hate and incitements: Violent extremist influencers and propaganda attempt to exploit widespread conspiracy theories and lingering distrust in government by vilifying elected officials and encouraging political violence in a purposeful attempt to provoke susceptible followers into conducting attacks.

Threats and acts of intimidation: Individuals inspired by violent extremism harass and make threats online, by email, by phone and in confrontational encounters with elected officials and their staff. Other acts of intimidation could include vandalism, arson or aggressive behaviours.

Doxing: Extremists with intent and capability could exploit an opportunity to conduct an attack in a low-security setting. The release of personal information, including residential addresses, is a considerable opportunity factor.

Attacks: An attack on a Canadian MP would likely involve a lone actor inspired by IMVE using unsophisticated methods. Attackers who radicalize and plot in isolation leave few traces for intelligence collectors and law enforcement. An attack could occur without warning.

INCIDENTS HIGHLIGHTING THE THREAT

2016: UK MP Jo Cox was shot and stabbed in the street by a neo-Nazi.

2019: German politician Walter Lubcke was shot at his residence by an anti-immigration extremist.

2020: Driven by conspiracy theories, Corey Hurren breached Rideau Hall, seeking to 'arrest' PM Trudeau.

2021: UK Conservative MP David Amess was stabbed to death by an Islamist extremist at a community event.

2022: An arson attack occurred at the office of Mississauga MP Peter Fonseca in the wake of the Freedom Convoy and Emergencies Act.

2022: Former Japanese PM Shinzo Abe was shot and killed by man with grievances linked to the PM's political connection to a religious group.

2022: The husband of then-US House Speaker Nancy Pelosi was attacked at home by a conspiracy theorist.

2023: A man threw a pipe bomb at Japanese PM Fumio Kishida, possibly inspired by grievances with election rules.

THREATS TO PARLIAMENTARIANS – Be Alert

UNCLASSIFIED/FOR OFFICIAL USE ONLY

April 2023

PROTECT YOURSELF FROM FOREIGN INTERFERENCE AND ESPIONAGE

- Be aware of the threat; increasing our collective resilience against foreign interference is a shared responsibility.
- Do your due diligence before sharing information or entering into arrangements, know your partners and assess the risks of any partnership in advance.
- Be cyber safe.
- Remember to always verify the credibility of your information sources to ensure that you are receiving accurate information.
- Report suspicious activities and any incidents of intimidation, harassment, coercion, or threats to CSIS or to your local law enforcement authorities.

PROTECT YOURSELF FROM ATTACKS AND OTHER PHYSICAL THREATS

- Avoid routines as organized protesters and groups study routines and can mobilize quickly to disrupt movements and/or events.
- Avoid posting itineraries on social media ahead of time. As much as transparency is valued, the more plans are shared publicly, the more likely protesters are to plan disruptions.
- Be aware of your surroundings. In public venues such as hotel bar, restaurants, etc. position yourself o minimize the likelihood of being recognized. Ask the restaurant staff to keep and empty table beside you, if possible.
- Identify threat cues. Threat cues usually come from the hands, not the face. Watch the hands for clenched fists, agitation, etc. Always position yourself in a position where you have time and space to react and reposition. Use obstacles to your advantage.
- Discuss scenarios ahead of time with property representatives and partners.
- Create an emergency response plan at your office and at home.

IMMINENT THREAT / EMERGENCY	Call 911
NON-IMMINENT THREAT: SAA-CS – Risk Management and Investigations Unit (7:30 – 7:30, business days)	+1-613-995-4777 saa.ops@parl.gc.ca
DOMESTIC AND INTERATIONAL PROTECTIVE SERVICES: RCMP	+1-833-226-7622 Protective_Policing@rcmp-grc.gc.ca
SUSPECTED FOREIGN INTERFERENCE OR ESPIONAGE: CSIS	+1-613-993-9620
EMERGENCY ABROAD: Global Affairs	+1-613-994-1294 SMS:+1-613-209-1233 SOS@international.gc.ca
CYBER EVENT: Canadian Centre for Cyber Security	Contact@cyber.gc.ca
GENERAL ENQUIRIES: PCO Security Operations	+1-613-960-4000

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

Canada