

SECRET
2019 06 17**Classified Briefing to Political Parties: CSIS Mandate & Threat Landscape****CSIS Mandate on FI**

- At CSIS, we collect intelligence on threats to the security of Canada and foreign intelligence using a variety of investigative methods.
- CSIS investigates threats which may, on reasonable grounds, be suspected of posing a threat to the security of Canada.
- We also have the authority, in certain circumstances, to take reasonable and proportionate measures to reduce the threats we detect.
- We collect and analyze information and we produce intelligence reports, including threat assessments and security assessments, to various departments of the federal government and law enforcement authorities.
- CSIS is not a law enforcement agency like a police force or the RCMP. We have no authority to arrest or detain people.
- At CSIS, accountability is at the centre of everything we do. The Security Intelligence Review Committee reviews all our activities. We are also subject to judicial oversight. A warrant from the Federal Court is required for any intrusive investigative measure we use.
- Since the Service's inception, it has been mandated to investigate espionage, sabotage and foreign interference threat activities. In the CSIS Act, foreign influenced activities or foreign interference are defined as any activities within or relating to Canada that:
 - are detrimental to the interests in Canada, and
 - are clandestine or deceptive or involve a threat to any person.
- As a member of the SITE taskforce, CSIS collects information about foreign interference and provides advice, intelligence reporting and intelligence assessments to the Government about these activities, as well as other hostile state activities.

SECRET
2019 06 17**Threat Overview****Election 2019: Trends**

- Current threat landscape in Canada is consistent with past practice from threat actors: Little discernable increase in overall interference activities at this time.
 - Cyber threat activity has been directed against other Western elections. We are not aware of any significant cyber threat to Canadian elections at this time.
 - HUMINT threat activity remains the most prominent form of foreign interference in Canada. We assess this is unlikely to change ahead of Election 2019.
 - Use of social media platforms by foreign state actors to conduct disinformation and amplification activity has increased globally. This trend likely to be a factor in the Canadian electoral context. At present, discernable FI activity in the social media space is limited.
-

What is FI and who are the Threat Actors

- The CSIS Act uses the term Foreign Influenced Activity and defines it in specific terms as having a clandestine, deceptive or threatening element behind it. Internally, we use this language and definition in our investigations.
- More broadly, however, governments (GC and international) have adopted the term Foreign Interference in order to distinguish it more clearly from foreign influence activities that are overt and a routine part of global diplomatic engagements.
- Overt influence refers to the use of public diplomacy and other means whereby a foreign state openly attempts to influence Canadian policy, the political landscape and/or electoral processes. One goal of overt influence activity can be to affect electoral outcomes within Canada but because it is overt and transparent, it initiates alternative diplomacy response mechanisms.
- We are careful to consider whether activity by a foreign state is simply aggressive lobbying in line with diplomatic norms, as opposed to FI threat activity. Distinguishing between the two can be something of a grey zone – as it is not always clear cut where legitimate, overt activities end and where illegitimate, clandestine activity begins.
- FI activities are long-standing, ongoing, systematic, and deeply rooted threats. While foreign interference differs from traditional espionage, FI and espionage

2

SECRET
2019 06 17

- activities are often conducted simultaneously via similar tradecraft and threat networks.
- Foreign states continue to engage in extensive foreign interference against Canadians and Canadian institutions. Foreign interference in the Canadian political system is motivated by foreign governments' political, economic and security agendas.
 - The main goals of foreign state actor FI activity in Canada are:
 - strategic and economic gain (notably, influencing elections and their outcomes or pressuring Canadian officials into taking specific stances on key issues);
 - regime preservation of the foreign state; and,
 - discrediting liberal-democratic institutions with the aim of advancing their own regime interests.
 - Foreign threat actors use a range of levers in their influence and interference activities: cyber operations can be used together with traditional human intelligence operations to undermine democratic processes
 - FI activities are conducted by foreign diplomats, intelligence officers, state proxies and co-optees including key members of diaspora communities.
 - All levels of political power in Canada have been targeted: federal, provincial, territorial and municipal. Political office-holders, candidates, office personnel and other persons with perceived access or influence have been the main targets.
 - As a multicultural society, diaspora communities in Canada are vulnerable to FI activities, and in some cases, are the targets of state-directed threats of violence or other punitive measures.
 - Tactics may include threatening, harassing and even detaining family members outside of Canada or refusing to issue travel documents or visas without cooperation.
 - Coerced, or even sympathetic, community members are then used as proxies by foreign threat actors to engage with Canadian decision-makers or undertake activities that would not be appropriate for official representatives in Canada.

For Public Release

SECRET
2019 06 17

- State-sponsored cyber information operations against democratic institutions are on the rise globally and will continue to impact democratic institutions worldwide.
- A small number of nation-states (notably, Russia) have undertaken the majority of the cyber activity against electoral processes worldwide. Other Western democracies have been targeted by cyber actors.
- While Canada is not immune to this threat, we are not aware of any significant cyber threat to Canadian elections posed by state actors at this time. Furthermore, we have no information to indicate that non-state actors are actively conducting, or plan to conduct, cyber-based influence operations.
- The rise of social media and web platforms creates new risks and enables influence activity at unprecedented scale and sophistication. These new systems have generated unintended threats to the democratic process, depriving the public of true and relevant information, informed political commentary, and the means to identify and ignore fraudulent information.
- We are almost certainly not aware of the full extent of the FI activities of hostile states in Canada.

Main actors in Canada that carry out FI activities – China and Russia

The People's Republic of China and the Russian Federation are the top-tier FI threats. Based on the observed FI activities, we assess these states believe they can operate in Canada with relative impunity. FI activities tend to increase leading up to and following elections.

China

Strategic Points:

- Most significant foreign interference actor – the threat emanates [redacted] through [redacted] *Chinese officials* [redacted] in Canada, uses Chinese Canadian Community groups, social media tools, trusted contacts, co-optees and cut-outs (business people, Canadian permanent residents and citizens), staff members of elected officials, and China media language outlets, to advance Communist Party of China objectives.
- Covert influence on key individuals is long-standing, occurs Canada-wide, directed toward all major political parties. China seeks to clandestinely and/or

4

For Public Release

SECRET
2019 06 17

deceptively support Canadian candidates, parties, and policies perceived to further the Communist Party of China's (CPC) strategic interests.

- Targets of China's threat activities are often unaware of the Chinese government's interest in them – though some targets willingly cooperate with China's threat actors.
- China is currently consolidating its strategic approach, which involves selecting preferred political candidates across federal party lines, aligning community-influence groups to promote Chinese political objectives, and arranging financial support to be funneled to preferred candidates. Local priorities may take precedence over national-level preferences
- Elected officials and candidates across all levels of government targeted – China covertly directs financial and voting support for favorable candidates, parties, and policies perceived to further the China's strategic interests.
- There is a general trend towards China interfering with Canadian officials at all levels of Canadian Government. [redacted] preferred supporters at municipal levels of government and then direct them upwards to provincial and federal levels for long term cultivation.
- China's intelligence capabilities are advanced, and its intent to utilize its range of levers is high. [redacted] China remains an active cyber player with interests in many Canadian entities and sectors, [redacted]
- Based on historical patterns of Chinese interference activity in the lead-up periods to Canadian elections, [redacted] we assess that Chinese activities will increase closer to the October election.

Russia

Strategic Points:

- Globally, Russia is a significant foreign interference threat actor and this is particularly true for threats to democratic institutions. Notwithstanding the latter, to date, [redacted] Russian activity against Canada's 2019 Election and Canadian democratic institutions has been minimal.

SECRET
2019 06 17

- Canada's electoral processes will be targeted if Russia sees disruption and interference as strategically beneficial. [redacted]

[redacted]

- [redacted]

- [redacted] Canada's election is not a priority target for Russia. Given Russian FI efforts in other countries, we will remain watchful for similar levels of Russian preparatory actions undertaken prior to the Canadian election that may lead to Russian interference activity.

- [redacted]
- [redacted]

While Canada does face other state-based threat actors that could potentially interfere in electoral areas, these states' intent and capability remain low compared to the threat Canada faces from China and Russia.

SECRET
2019 06 17

[Redacted]

India

- [Redacted] the Sikh extremist threat, and monitoring the Sikh community in Canada, is a priority for Indian officials in Canada, [Redacted]

- Indian officials have utilized a network of contacts, which includes politicians, academics, businesspersons, media personalities and community leaders, to monitor Canadian-based individuals that are of interest to the Government of India.

- [Redacted]

[Redacted] Some of this activity has been conducted in either a clandestine or deceptive manner making it foreign interference.

- Furthermore, Indian interference activities targeted at Canadian Members of Parliament, Provincial Legislative Members, [Redacted] outside the scope of regular diplomatic norms, has been observed.

- [Redacted]

Pakistan

- [Redacted] Pakistani officials in Canada have likely tried to clandestinely influence and support Canadian politicians of Pakistani descent, with the aim of furthering Pakistani interests in Canada.

[Redacted]

[Redacted]

For Public Release

SECRET
2019 06 17

Iran

