Summary Report

Author: Alan R. Jones, former Assistant Director, Canadian Security Intelligence Service, Executive Advisor, National Security Program, University of Ottawa, Professional Development Institute.

Panel Theme: Canada's National Security Apparatus

KEY ISSUES:

Foreign Interference (FI) may take many forms: from traditional person to person interference using deception, manipulation and even violence but now it is increasingly enabled and advanced by social media using Misinformation and Disinformation and Artificial Intelligence.

FI is part of broad state versus state campaigns: Election interference will never be a singular goal unto itself – it is simply one angle in multi-faceted FI campaigns to damage Canada and Canadian interests. It overlaps with espionage, corruption and even terrorism and may have common tactics, actors and objectives with those other threats.

The response to FI will need to be as nuanced and as layered as the threat is itself. Only the most extreme forms of FI will ever meet a threshold for law enforcement and those cases will likely be exceedingly rare. The vast majority of FI campaigns will be cloaked in legitimate diplomatic and business or cultural activities.

Adversary states are becoming increasing aggressive and using tactics, including criminals and proxies, that cross clear "red lines" such as acts of violence, with impunity.

International and domestic co-operation is vital to identifying and mitigating foreign interference. Allies and partners that share common liberal democratic values are developing strategies that Canada can benefit from. A whole of Government and whole of society approach will be needed to protect Canadian values and democratic institutions.

As with most emerging national security threats new threats do not replace traditional threats they simply become another layer of threats to deal with; existing tools and resources may not be inadequate. CSIS, the RCMP, CSE and other agencies have powerful investigative powers but expertise development and coherent frameworks around the investigation of FI are more difficult to develop. Developing expertise on complex issues within ethnic and business communities requires a specific focus and dedicated resources and training.

Public exposure of foreign interference can be very effective at diminishing the threat by denying the adversary the protection of being clandestine or deceptive.

ASSESSMENT:

The Government of Canada responses to threats of Foreign Interference will need to be as nuanced and layered as the threat itself: from subtle to blunt. NS responses may include anything from raising awareness of a threat to denying a threat the environment to materialize: diplomatic initiatives, disruption, or law enforcement and arrest, if possible, of the actors involved.

Foreign Interference is unfortunately concomitant with state to state relations. The intent of Foreign Interference may be to influence an election but its almost always within the broader intent of an overall objective to weaken or manipulate an adversary politically, economically or militarily. It is often underpinned by an ideological framework.

Foreign Interference emanates not just from obvious adversaries but sometimes even from "friends".

https://www.abc.net.au/news/2024-08-11/asio-boss-warns-friendly-nations-interfering-in-australia/104211120

A disturbing trend was directly addressed recently by Ken McCallum, Director General of MI5, the British Security Service when he was referring primarily to actions by the Russia government including murder of dissidents in the UK but also including states such as Iran. Mr. McCallum went so far as to say that Moscow was seeking to cause "mayhem" on the streets of Europe. The alleged Government of India involvement in the murder of a Canadian would fit this trend.
https://www.reuters.com/world/uk/russias-gru-seeking-cause-mayhem-britain-europe-uks-mi5-spy-chief-says-2024-10-08/

In a September 2019 working paper published by the Finnish Institute of International Affairs (FIIA), Mikael Wigell uses the notion of 'hybrid interference' to mean 'non-military practices for the mostly covert manipulation of other states' strategic interests'. Wigell makes a clear distinction with hybrid warfare, 'which is essentially a military approach to conducting "indirect war" under special circumstances'. Focusing not only on Beijing and the Kremlin, but also by Erdogan's Turkey and Iran, Wigell explains that 'the idea is not to confront the target head-on, but to weaken its resolve by more subtle means of interference calibrated to undermine its internal cohesion'. This 'wedge strategy' fosters divisions or aggravates existing tensions…

https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652082/EPRS_BRI(2020)652082_EN.pdf

An example of the above is the current crises surrounding the alleged involvement of the Government of India in the murder of a pro-Khalistan Canadian Sikh. The GoI exploited the growing tensions between the Canadian Sikh diaspora and the increasing diaspora from Gurjarat, PM Modi's political stronghold.

All the elements of Bill C-70 have yet to be implemented or even fully understood. It may have been rushed into being. The Foreign Influence Transparency Registry (FITR) will, over time hold a considerable body of information potentially related to Foreign Influence. Some records will be considered innocuous at the time of creation but may later change in context. FI often involves slow and methodical recruitment and manipulation which may take months or years to become a threat. But the background information could provide invaluable intelligence leads to reveal a developing threat and create a window to counter it, but only if the record can be accessed and analyzed by CSIS or the RCMP.

Countering options could include public policy decisions, disruption, diplomatic responses including expelling diplomats, deporting foreign actors who are not diplomats, denying entry into Canada of threat related individuals, freezing assets, blocking acquistions and supporting civil society and academic initiatives, or criminal prosecution.

Section 15 of the FITR is not clear that CSIS or the RCMP would be able to request access to those records in the course of an existing NS investigation that may not relate to the strict violation of the registry requirements but could certainly be related to a foreign interference investigation under 2(b) CSIS Act or an RCMP corruption investigation. The request would not be a fishing trip - it could only be made in the context of a duly authorized intelligence or police investigation. No new powers are required but disclosure clarification is.

Disclosure to Elected Officials:

Interference in the democratic process often involves compromising elected or aspirational public officials. Other countries have the same challenge and other approaches may be of use to Canada. In the UK, the MI5 website addresses an aspect of this issue under: "FAQS: Does MI5 vet Ministers and Members of Parliament?"

Ministers and MPs are not subject to vetting by MI5 and further states an incoming Prime Minister will be told about any information it (MI5) may have about a potential Cabinet Minister that "raises serious national security concerns and only if it appears likely that the individual concerned will need access to sensitive information…
A similar arrangement has been in operation for the Official Opposition since 1992. The Leader of the Opposition is briefed on any serious security issue concerning a possible member of the Shadow Cabinet. This is necessary because members of the Shadow Cabinet are often briefed on security issues."

https://www.mi5.gov.uk/faq

Public Disclosure:

Public disclosure of the nature of an FI threat could be very useful in building societal or sectoral resiliency – shedding light on a threat may be one of the most effective means of negating the value of a covert or deceptive threat by a foreign state. This could range from limited disclosure to specific public parties up to what the US refers to as "Strategic Disclosure" which involves downgrading or declassifying intelligence for broader dissemination to achieve a specific outcome: a balanced achieved in protecting National Security while disclosing sensitive information to expose threat actors, tactics and targets.

In June 2022 the heads of MI5 and the FBI publicly addressed the threat of Foreign Interference from China. The address is too lengthy to fully address in this document but it emphasizes the objectives of the Chinese leadership to gain political, military and economic advantage by interfering in the home affairs of its global competitors. It highlights the techniques which are blended with legitimate diplomatic and business relationships – which can involve "friendships" where the unwitting "friend" has no idea they are pawns in a foreign interference operation. These insidious activities are difficult to detect, prove and counter.

https://www.mi5.gov.uk/joint-address-by-mi5-and-fbi-heads

The US via the FBI has pioneered an approach in prosecuting foreign intelligence operators and thereby disclosing their names, the elements of the state arm that they work for, their methodology etc… The individuals may never be arrested but the disclosure via indictment documents is effective in exposing the nature of the threats. Public disclosure can help the public build confidence in the work of our NS agencies.

Central National Security Structure:

Oversight and review has been modernized but the role of NSIA and its supporting processes remain only partially institutionalized as part of the Canadian governance structure. The setting of Intelligence priorities must be more than a perfunctory annual workplan for agencies. Intelligence must be rolled up to inform Government of Canada Public policy development.

We have an effective, coherent review apparatus to determine if things are not being done properly under the law but we have a minimal central structure to ensure that Canada's overall National Security is well protected on an ongoing basis or if not, what must be done to address gaps. There is an ongoing debate about whether or not Canada needs a stand-alone Foreign Intelligence Service but this is a different discussion from a statute defining what foreign intelligence is in Canada and who exactly is currently responsible for it at the moment.

Recommendations:

Study should be undertaken to:

1. Identify an outreach strategy to vulnerable communities and individuals and civil society for a whole of Government approach, with due regard for agency mandates:

- to provide a safe and discrete way for complaints and information to be shared with the Government of Canada to identify threats, incidents, trends, actors and mitigation opportunities and to warn the vulnerable and provide mitigating and protecting options.
- outreach must be conducted with sensitivity to vulnerable individuals who may have a fear of Government officials; particularly police, intelligence and immigration.

2. Develop functional relationship with Federal, Provincial and Municipal political party leadership to create mechanisms for CSIS and the RCMP to disclose / forewarn of potential threats to the integrity of political parties and to provide a safe and discrete way for complaints and information to be shared with the Government of Canada.

- Specific training programs need to be developed for agencies, officials, civil society and for public awareness. Academia can support this effort.

3. Ensure effective and efficient information sharing mechanisms between Federal and Provincial agencies and departments with regard to elections and the protection of democratic institutions.

- Create, where necessary, classified information sharing and retention mechanisms including clearances and secure data sharing and holdings systems.
- Attention to be given to ineffective or blocked information sharing of Federal information holdings that are intended to support intelligence or criminal investigations into Foreign Interference including, but not exclusively, Sec 15 of the Foreign Influence Transparency Registry (FITR).

4. Review existing legislation that is directly and indirectly involved in providing the legal "tools" for Canada to mitigate and counter FI. Over the years, including C-70, the legislative framework has become something of a patchwork aimed at specific events rather than a strategic effort to create a coherent counter FI framework. Once reconciled and streamlined, the tools at hand can be better assessed as to adequacy and gaps.

5. Engage academia on research into FI including Misinformation and Disinformation including the role of Artificial Intelligence in creating deep fake imagery, audio, documentation and other deceptive techniques.

6. Increase international co-operation with allies and partners with shared democratic powers to access examples and leverage mutual capabilities to identify and counter malicious Foreign Interference actors and to learn from other jurisdictions on building resilience in Canadian society. The Australian approach could be very informative in terms of institutions, objectives and effectiveness.

https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

Additional Remarks

Agencies such as CSIS and the RCMP need to speak directly to Canadians to understand how a suspected threat is developing or transpiring in Canadian communities. Without that intimate access to personal relationships it is difficult to understand the threat environment and provide forewarning of the harm to come. Google is not a substitute for personal dialogue.

There is a compression of the intelligence collection timeline caused by increasing the threshold of intelligence investigations and investigative powers to near criminal evidence levels. The vast number of criminal charges are filed after a crime has occurred. Intelligence is supposed to about forewarning and about more than just crimes.

An ancillary issue to this remains the definition of "relevance" relating to Canada Evidence Act S. 38 disclosures. What is generally referred to a the Stinchcombe "relevance" issue results in the disclosure of large amounts of sensitive information which is ultimately found not to be material to a prosecution or other process under Judicial review. Prosecutions remain potentially imperiled by the redaction of classified information that is not material to the case but gets caught up in the excessively broad "relevance" definition.

Alan R. Jones