THE NECESSARY EVOLUTION OF COUNTER-INTELLIGENCE IN RESPONSE TO FOREIGN INTERFERENCE

Date: November 21, 2024

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 21, 2024, a Canadian Security Intelligence Service (CSIS) Executive presented *The Necessary Evolution of Counter Intelligence in response to Foreign Interference* for this year's West Coast Security Conference. The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key theme discussed was how intelligence work has transformed since the end of the Cold War and in response to the threat of Foreign Interference in particular. The presenter outlined why Canada is an attractive target for Foreign Interference threat actors and highlighted how Canada's intelligence professionals and legislative framework has had to evolve as a result.

NATURE OF DISCUSSION

Counterintelligence has evolved since the end of the Cold War, and the rigidity of countering major nation-states and armies has evolved into an increasingly complex information landscape. The old days of guarding tangible materials and installations have become more complicated; every space must now be defended, and that requires reaching out to and collaborating with public and private sphere stakeholders. Intelligence agencies, especially those with a domestic mandate, will need to navigate the grey area of hybrid warfare, upholding individual civil liberties, and managing what explicitly counts as foreign interference.

BACKGROUND

Presentation

The CSIS Executive explained that counterintelligence is far more complex today than in the past. Protecting Canada's national security and economic interests is not just about catching Russian and Chinese spies. Instead, modern counterintelligence is about understanding the complex range of threats that hostile states pose. It is also increasingly about stakeholder engagement, education and outreach, including through participation in events like the CASIS West Coast Security Conference. Additionally, the CSIS Executive explained that the skills and work performed by intelligence professionals has had to evolve in response to those threats and the ever-changing national security environment.

The CSIS Executive began his career as an Intelligence Officer at the Service in 2001. During this period, counterterrorism defined CSIS's main area of operations, and for the first 20 years of service the primary focus of the Executive's portfolio was counterterrorism – tactical-level operations responding to specific terrorist threats. This intelligence work involved regular collaboration with a typical set of partners that are familiar with intelligence work and the national security threat landscape. Examples of traditional partners provided by the Executive included Five Eyes (FVEY) partners, the Department of National Defense (DND), the Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency (CBSA).

As global threats evolved, the CSIS Executive shifted to working full-time in counterintelligence, fulfilling roles which differed slightly from what they had expected. Counterintelligence, despite common perceptions, was not only about working in the shadows to identify and thwart hostile state actors. Counterintelligence requires meaningful understanding of what hostile states' objectives are as well as what activities hostile states undertake to achieve those objectives. To identify and counter those threat activities today, intelligence professionals need to appreciate the vulnerabilities inherent to Canadian supply chains, Canadian democratic processes, sensitive Canadian research, critical mineral and resource development, and cyber security. Today's national security landscape is complex and can at times be difficult to navigate.

The CSIS Executive outlined that foreign interference is deliberate and covert activity undertaken by a foreign state to advance its interests, often to the detriment of Canada's. The CSIS Act describes Foreign-Influence Activities as "activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person". It poses a significant threat to the integrity of our political systems, democratic processes, social cohesion, academic freedom, economic prosperity and challenges Canadians' rights and freedoms. As described by the National

Security and Intelligence Committee of Parliamentarians, foreign interference threatens the fundamental values of our country and our national security.

The presenter outlined the reasons why foreign actors target Canada and highlighted that its greatest strengths are also its greatest vulnerabilities. The speaker noted that Canada has some of the world's most coveted natural resources, technology, education, occupied a geopolitically strategic location, and had strong allies. Furthermore, as one of the most open and transparent democracies on the planet, Canada arises as a prime target. Given these characteristics, it is unsurprising that our adversaries would want to exploit our vulnerabilities to advance their agenda.

The "old days" of simply defending tangible Canadian assets and top-secret installations are over. They no longer just want our secrets. A host of hostile states want our data, our resources, our know-how and our influence. Our adversaries' targets have evolved and now include universities, city halls, technology parks, private enterprise and a variety of other unclassified spaces. How we defend ourselves must also evolve. In very real terms, this evolution has demanded changes to how intelligence professional do their business as well as the national security legislation that governs that business.

For example, specific areas of vulnerability may include Canada's First Nations communities, technology and infrastructure, and our inclusive democratic process. For instance, Canada's First Nations communities can be targeted for influence by a foreign state as a means of driving wedges between various levels of government in Canada. Similarly, if a foreign state-owned enterprise was to win a bid to supply technology to a local hospital or infrastructure project, they could also gain access to sensitive personal or economic data that could then be exploited or even weaponized against Canada and its allies. Lastly, as recent findings from the Public Inquiry into Foreign Interference have made clear, our democratic processes are vulnerable. Rules around party nomination races are prone to be exploited, as are social media narratives as foreign actors may seek to amplify or suppress certain stories.

The CSIS Executive reasserted that it is an individual's democratic right to choose any political ideology they prefer. It can be challenging to establish a link whether individuals are acting of their own accord or at the behest of foreign actors. Foreign interference requires this link.

Countering these threats has required that intelligence professionals are comfortable meeting with and briefing public officials, CEOs of companies, researchers, academic and a variety of other stakeholders. This type of public facing activity has also required legislative changes such as C-70, legislation that allows CSIS to partner with non-federal entities and build greater resiliency against the threat for foreign interference.

Question and Answer

Is there a first four years of training?

This is something that remains in flux. The CSIS Representative spoke about their experience when they got their first assignment at headquarters, followed by training prior to receiving a field assignment. They encouraged those interested to apply, to build professional connections, and to remain patient amidst a time-consuming hiring process.

How does the organization balance legal considerations with operational needs?

The organization is very cautious regarding how to implement new legislation. Just because something has become law doesn't mean the department has the policy to immediately and responsibly execute. The new C-70 legislation is being put into practice with prudence. The organization must remain very cautious in intelligence work while respecting the democratic rights of Canadians.

KEY POINTS OF DISCUSSION

- Intelligence and government agencies must adapt to an evolving threat environment by developing specialized tools to clearly define and act upon foreign interference.
- Canada's desirable resources, technology, education, strategic location, and transparency make it a prime target for adversaries, necessitating an evolved security approach to protect its institutions.

FURTHER READING

Kelshall, Candyce. (January 31, 2023) "DISRUPTION: HIDING IN PLAIN SIGHT." *The Journal of Intelligence Conflict and Warfare 5*(3), 101–104. https://doi.org/10.21810/jicw.v5i3.5175.

Meyers, S. (2018). How Canadian Intelligence is Exposed to the Impact of Globalization: A Critical Analysis of the Security Threat of Right-Wing

Extremism. *The Journal of Intelligence, Conflict, and Warfare*, *1*(2), 22–30. https://doi.org/10.21810/jicw.v1i2.637

Pyrik, J. (2015) Communicating risk. In R. Arcos & R. Pherson (Eds.), *Intelligence Communication in the Digital Era: Transforming Security, Defence and Business* (pp. 42-56). Palgrave Pilot, London. https://doi.org/10.1057/9781137523792_4

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/