FROM SECURITY TO INTELLIGENCE: CANADIAN SECURITY AND INTELLIGENCE ARCHITECTURE IN AN ERA OF STRATEGIC THREAT

Date: November 19, 2025

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 19, 2025, Mr. Dan Faughnan presented *From Security to Intelligence: Canadian Security and Intelligence Architecture in an Era of Strategic Threat* at the 2025 West Coast Security Conference. The presentation was followed by a question-and-answer period with audience members and CASIS Vancouver executives. The presentation examined the historical evolution of Canada's security and intelligence architecture, identified structural limitations in responding to contemporary strategic threats, and outlined the need for institutional reform in light of foreign interference, emerging technologies, and intensifying geopolitical competition

NATURE OF DISCUSSION

Mr. Faughnan argued that Canada's intelligence and security institutions were designed for a markedly different threat environment and have not yet adapted at the pace required by contemporary geopolitical instability. Until recently, geographic insulation, alliance dependence, and post-Cold War assumptions were described as insufficient buffers against modern hybrid and state-driven threats. He emphasized the need for greater self-sufficiency in intelligence collection, more assertive and risk-tolerant leadership, and more agile resource allocation across the national security community.

BACKGROUND

Mr. Faughnan traced the origins of the Canadian Security Intelligence Service (CSIS) to the dissolution of the RCMP Security Service following the McDonald Commission. He noted that CSIS inherited elements of a policing-oriented culture that prioritized support to law enforcement over the production of independent strategic intelligence. Early operational focus centered on domestic

counterterrorism, including investigations linked to the Air India Flight 182 bombing and groups such as the Heritage Front.

During the 1990s, CSIS expanded its mandate to address a re-emergence of foreign espionage, the proliferation of weapons of mass destruction, and international terrorism, reflecting a gradual broadening beyond more narrowly defined domestic security threats. However, this expansion was described as resource-intensive and, at times, unevenly applied across competing mandates. In the early 2000s, the organization shifted further toward the production of strategically oriented intelligence intended to inform long-term national security planning.

Despite these evolutions, Mr. Faughnan contended that Canada's broader intelligence architecture remains structurally fragmented and constrained by, amongst other challenges, interdepartmental competition for mandates and resources. He characterized Canada as lacking a deeply embedded intelligence culture at both the public and policy levels, limiting reform momentum and investment in independent collection capabilities. In an era marked by foreign interference, cyber and hybrid threats, and AI-enabled operations by both state and non-state actors, these structural limitations were described as increasingly consequential.

To address these shortcomings, Mr. Faughnan proposed three reform priorities. First, improved resource allocation to address globalized threats, particularly foreign interference and emerging technological risks. Second, the development of a mandated foreign human intelligence (HUMINT) capability to reduce reliance on allied reporting. Third, and perhaps most importantly, the cultivation of more risk-oriented leadership within Canada's security and intelligence institutions. He argued that longstanding reliance on allied intelligence – particularly within the Five Eyes framework – has fostered institutional risk aversion and delayed the development of independent capabilities. Without reform, Canada risks remaining dependent and reactive, rather than strategically proactive in an intensifying threat environment.

Question and Answer

From a whole of government perspective, how can Canada evolve to the changing threat environment?

To stay ahead of these threats, Canada should look to prioritize operational agility over structural perfection - the 90% solution executed vigorously is more effective than the 100% solution executed never. Effective defence requires a whole-of-government approach that favors flexible policy and rapid execution over rigid legislative mandates that struggle to keep pace with rapidly evolving

pressures from state adversaries, foreign interference, cyber and hybrid warfare, and emerging technologies, without the certainty of sustained allied intelligence support.

What specific strengths does CSIS bring to the Five Eyes and how might intelligence sharing amongst Canada's allies change over the coming years?

Canada's reputation as a trusted and unobtrusive middle power remains a strategic asset. However, sustaining credibility will require modernization of legislative authorities, organizational structures, and collection capabilities to ensure Canada remains a net contributor rather than a dependent partner.

As some Canadian Special Operations and CSIS's responsibilities broadly evolved out of the RCMPs mandate, what shared lessons learned have come out of the growth of both organizations?

The biggest lesson learned was moving away from a policing mentality and toward an intelligence culture, where the organization became more professional in its approach to the planning cycle and the training and recruitment of personnel.

In Canada, we have multiple agencies and departments working on similar threats; how do we ensure there are collaborative systems in place for information sharing between departments?

Operational-level cooperation tends to function effectively during crises but is often hindered by bureaucratic friction in routine contexts. A shift away from siloed intelligence practices toward clearer accountability structures and greater autonomy for organizations to act within defined mandates would reduce duplication and institutional competition.

KEY POINTS OF DISCUSSION

- Canada's security and intelligence architecture was originally designed for a different strategic era and is now sometimes misaligned with contemporary threats, such as foreign interference, hybrid warfare, and AI-enabled operations.
- A limited intelligence culture and structural fragmentation have constrained reform, investment, and independent collection capabilities.
- Longstanding reliance on allied intelligence is increasingly untenable in an environment of intensifying geopolitical competition.

- Institutional modernization requires improved resource allocation, development of foreign HUMINT capacity, and more risk-tolerant leadership across the national security community.

FURTHER READINGS

Faughnan, D. (Guest Speaker). Gurski, P. (Host). (2022). The Challenge of Running a Large Domestic Security Intelligence Operation (Episode 131). [Audio podcast episode]. In *Canadian Intelligence Eh*. Borealis Threat & Risk Consulting. https://borealisthreatandrisk.com/episode-131-dan-faughnam/

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/