Hristijan Ivanovski
Research Fellow and TA
Centre for Defence and Security Studies (CDSS)
University of Manitoba
Dec 8, 2018, updated Mar 24-5, 2019
E-mail: hristijan.ivanovski@umanitoba.ca

CSIS, CSE & CFINTCOM

The Pearls of Canada's Security and Intelligence Establishment

Speaking in the broadest terms, the Canadian Security and Intelligence Community (CSIC) may sometimes be perceived as a nation-wide network of diverse and more-or-less interconnected security organizations and entities, each operating on a different level, whether municipal, provincial, federal, and/or international. That's quite logical, since, no doubt, all these security providers, from the RCMP officers patrolling the tiniest and most remote rural communities in Canada's hinterland and the intel units created within the police forces of the largest Canadian cities, the special bodies and programs run by provincial police services or departments of justice, to the relevant federal offices, departments (Public Safety and Emergency Preparedness Canada, Dpt. of National Defence, Public Services and Procurement Canada) and spy agencies, have a stake in "Helping Keep Canada and Canadians Safe and Secure."

Defined more conservatively, however, the CSIC is exclusively a federal-level structure. According to a dedicated brochure released by the Privy Council Office (PCO), at the century's turn the Community consisted of nine core security and intelligence actors established across four federal portfolios and offices. In pursuing their mission of protecting the *raison d'état*, these nine actors were functionally complemented by the Citizenship and Immigration Canada (CIC), Justice Canada, Transport Canada, and what was then known as Canada Customs and Revenue Agency (CCRA).

Hristijan Ivanovski
Research Fellow and TA
Centre for Defence and Security Studies (CDSS)
University of Manitoba
Dec 8, 2018, updated Mar 24-5, 2019
E-mail: hristijan.ivanovski@umanitoba.ca

While, in structural terms, the CSIC has undergone significant reform since 9/11, its overall strategic mission remains the same. Guided by the national security ideal, the Community's stakeholders are collectively responsible "not just [for] the [physical] safety and security of the country and its citizens," but also for "guarding [Canada's] national values and interests against...internal and external dangers."

Today, three CISC stakeholders stand out as "a significant national asset," especially when it comes to protecting Canada's interests and values abroad. These are as follows:

- the CSIS,
- the Communications Security Establishment (CSE), and
- the Canadian Forces Intelligence Command (CFINTCOM).

Established in 1984, CSIS is Canada's primary secret security service tasked with both intelligence and counter-intelligence operations. Over the past 35 years, this civilian and fairly autonomous spy agency, falling under the Public Safety portfolio, has abandoned the law enforcement model initially inherited from the RCMP as its historical cradle—notwithstanding recent, seemingly retrograde developments (e.g. the reportedly novel practice of CSIS agents being armed when on duty in dangerous foreign lands, Bills C-51 and C-59 vesting CSIS with disruptive powers such as the power to detain)—and has grown into a modern, reliable, and well-connected intelligence organization capable of conducting covert and overt operations globally. In a functional sense, this means maintaining a strong focus on intelligence gathering and

analysis, such as in the context of combating terrorism, with intelligence information sharing being a key segment. Today, like other CISC stakeholders, CSIS puts a premium on information exchange by offering, on the one hand, a distinct Canadian security perspective to allied counterparts and, on the other hand, harnessing its partnerships "with more than 200 hundred agencies worldwide."

To fulfil its demanding dual mandate, which includes virtually everything, from basic open-source intelligence collection and analysis to undertaking covert and clandestine activities "with no [explicit] territorial limit," CSIS has been divided into four branches:

- Counter-Intelligence,
- Counter-Proliferation,
- Counterterrorism, and
- Research, Analysis and Production (RAP).

Given its structure and competences, as well as its background, it is obvious that CSIS continues to nurture a robust homeland security component. This approach, according to some, may not be anachronistic (quite the contrary) but definitely comes at the expense of doing better-resourced and more focused foreign intelligence work. Regardless, CSIS remains the primary actor in "gather[-ing] security intelligence on direct threats to Canada." Not only has it survived reform proposals aimed at setting up a separate foreign intelligence agency for Canada, but, as prudently observed by Elinor Sloan, it "increasingly collects information on threats...that originate in a foreign country."

Hristijan Ivanovski
Research Fellow and TA
Centre for Defence and Security Studies (CDSS)
University of Manitoba
Dec 8, 2018, updated Mar 24-5, 2019
E-mail: hristijan.ivanovski@umanitoba.ca

Thus far, the Service has hardly had any substantial failure in identifying and reducing 'purely' external threats (the 1985 Air India bombing featured a significant domestic dimension, apart from being blamed on what was then a nascent security service). To the contrary, CSIS operatives, along with their DND counterparts, have recently been a significant Canadian intelligence asset on the frontlines in Afghanistan. Moreover, the country benefits from their subtle human intelligence (HUMINT) work in a few other important strategic regions. Hence, in spite of the continuing debate over whether Canada, like many other countries, needs a dedicated foreign intelligence service, CSIS keeps playing a gigantic role in keeping Canadians safe and secure wherever they are.

Unlike CSIS, the two other intelligence structures with a lion's share in safeguarding Canada's vital interests on a global scale fall within the broader National Defence portfolio. Drawing its roots from WWII and the legendary Examination Unit (XU, 1941-46), the CSE is Canada's dedicated signals intelligence (SIGINT) agency, equivalent to the NSA, GCHQ, ASD, and GCSB within the Five-Eyes Community.[1] As a national cryptologic authority, the CSE performs two main functions: providing the Government of Canada with foreign SIGINT, specifically "by collecting, analyzing, and reporting on foreign radio, radar, and other electronic signals," and safeguarding government telecommunications against "interception, disruption, manipulation or sabotage." In pursuing this "primary mission," the agency works "with provincial and territorial

[1] NSA, GSHQ, ASD, and GCSB stand, respectively, for National Security Agency (US), Government Communications Headquarters (UK), Australian Signals Directorate (Australia), and Government Communications Security Bureau (New Zealand).

governments and the private sector" on protecting "Canada's critical information infrastructure" while also assisting its CSIC partners in carrying out their respective mandates.

Looking ahead, the CSE is already paving the future of Canadian cryptology and cyber security. With its cyber defence role growing in pace with the complexity and challenges of the cyber space and the Liberal government's effort to regulate this effectively within a single national security framework (Bill C-59) well under way, the agency is bound to increasingly rely on new, in-house built tools, in addition to the highly controversial metadata, for identifying, analyzing, and tackling cyber threats. Given the level of commitment and "leading-edge technology," the CSE's visionary striving for "information superiority" might not be as elusive as some might think.

In fact, the newly-erected futuristic Ottawa headquarters, fitted with a high-capacity data centre (over 100 kms of cables) and equaling the size of 11 NHL hockey rinks, speaks for itself being nothing less than a meta-strategic enabler for the decades to come.

Finally, turning to the more traditional, military side of Canada's defence intelligence, the Canadian Forces Intelligence Command (CFINTCOM) is currently in focus. After a prolonged process of (re-)transformation of the Canadian Armed Forces' (CAF) command and control (C^2) structure that started in 2005/06 under General Rick Hillier, this newly-formed "Level 1 command" (out of seven existing in total) is not simply the present Canadian version of the Pentagon's Defense Intelligence Agency (DIA). Working at "the strategic level," yet, with a

significant role in operational support ("mission-focused [and] outcome-oriented") and a head placed on par with other CAF operational commanders, CFINTCOM makes one comprehensive (and even somewhat *sui generis*) military intelligence fusion and analysis centre with good prospects of becoming Canada's cognitive 'fist' in an ever changing world plagued by hybrid warfare.

Just as a curiosity, up to 35% of the Command's personnel, which consists of "about a thousand people" in total, are civilians, mostly analysts. Through such subordinate units as the Directorate of Transnational and Regional Intelligence and the Directorate of Scientific and Technical Intelligence, they help assess foreign political, military, scientific and technical information, thus keeping "an around-the-clock intelligence watch on developments abroad…" What this basically means is that, in a time when many security and intelligence recruiters begin to look outwards for providers of diverse non-military perspectives on global affairs, CFINTCOM is on the right track making sure its future work does not get hindered by what General Stephen Bowes describes as a culturally-limited view of how our adversaries operate.

"Intelligence is Canada's first line of defence," asserts Chapter 6 of Canada's 2017 Defence Policy, and the 'enemies,' which are currently mounting enormous pressure on the Canadian and allied security and intelligence services, are as follows: the global shift in power and influence, rapid high-tech advances, and the changing nature of conflict. Spearheaded by CSIS, CSE and CFINTCOM, the evolving 21st-century CSIC is poised to tackle these generic challenges in both conventional and unprecedented ways.

Hristijan Ivanovski
Research Fellow and TA
Centre for Defence and Security Studies (CDSS)
University of Manitoba
Dec 8, 2018, updated Mar 24-5, 2019
E-mail: hristijan.ivanovski@umanitoba.ca

Hristijan Ivanovski is a Research Fellow at the University of Manitoba (UofM) Centre for Defence and Security Studies (CDSS), Associate Editor (Europe) of iAffairs Canada, and a former coordination officer with Macedonia's Secretariat for European Affairs. Since 2016, he has been a Member of East-West Bridge (EWB) contributing to the Foundation's Foreign Policy Task Force. Hristijan can be reached @ hristijan.ivanovski@umanitoba.ca.