NOTE FOR NATIONAL DEFENCE:
Foreign Intelligence, National Security and Defence

Author: Dave McMahon, Clairvoyance Cyber Corp

Canada has worked under fragmented model of foreign intelligence collection since the second World war, heavily relied on allies for intelligence, while the global environment has become more complex and gaps in intelligence have widened to the point where Canada is strategically disadvantaged.

A new foreign intelligence framework is required for national security and defence. One that combines the collective mandates of the security service, national policing, cryptologic establishment, military, and diplomatic core with a new Service.

THE COMPETITIVE ENVIRONMENT

Changing demographics, resource competition, environment change, globalization, economics, governance, urbanization, competitive geopolitics, the unprecedented advancement in science and technology, are significant trends shaping the future security environment. These trends are developing rapidly along converging timeline to create emergent effects, threats and competing opportunities. Never has the need for enhanced foreign intelligence been more critical and a sovereign Canadian capability more important. The defence intelligence enterprise (DIE) plays a critical role in the collection and production of foreign intelligence.

Foreign states have successfully targeted Canadian nuclear programs through spying and subterfuge for the purpose of building their nuclear weapons capabilities. Canada has been implicated in nuclear weapons proliferation owing to export policy, academic collaboration and susceptibility to espionage. The nuclear threat from nation states and extremist groups could be better informed and countered by a Canadian foreign intelligence service. Nuclear weapons proliferation would be a critical defence intelligence priority.

The contest to control and influence the fabric of cyberspace will be as significant as the Manhattan project.

Canada's adversaries will continue to weaponize in cyberspace and seize vital high ground as

part of grand strategies for AI supremacy and dominance of the Information Cognitive Domain[1]. In this future, soft power, intelligence and influence will become critical.

We foresee the build-up of offensive cyber capabilities of nation states and a consolidation of darkweb territory by transnational crime that is supported by adversary states. Ultimately leading to increased competition and conflict that will spill out in real life. Superior, Criminal organization will compete directly against Canada's armed forces in cyberspace.

"*Canada's post-Cold War enemies are hidden, and Canada's diplomatic and military allies have remained economic competitors. On those grounds alone, Canada needs a Foreign Intelligence Service."*[2]

Pacing threats such as China, Russia, Iran and North Korea, compete with Canada in cyberspace and economically just below the level-of-armed-conflict. China's road and belt initiative will shift the balance of economic, technological and military global power. The Thousands Talent Plan recruits leading international experts in scientific research, innovation, and entrepreneurship. United Front Work gathers intelligence on, and attempts to influence elite individuals and organizations inside Canada. Meanwhile, a Three Warfares strategy of the People's Liberation Army (PLA) coordinates public opinion, psychological and legal warfare.[3]

Pragmatically, China is shaping global infrastructure at an alarming speed: launching low orbit 5G satellites over Canada's Arctic, conducting industrial espionage against our business and seeking to impose their a social credit system of surveillance onto Canadians through manipulation of telecommunication standards and applications.

Russia for their part, is a multi-domain threat that holds North America at risk, whether it be projecting power globally through informationized or hybrid warfare, compromising supply chains or propagating a firehose of falsehoods, misinformation and disinformation[4], which intend to erode, disrupt and degrade trust in the democratic system and undermine fundamental Canadian values and quality-of-life.

Meanwhile, rogue states, such as Iran and North Korea, pound Canada in cyberspace, outside of any international norms of behaviour.

Amongst all the pacing threats, we see tight collaboration industry, government, military, intelligence services and organized crime as part of a grand strategy. To this, Canada lacks an equivalent counter-strategy or public-private partnership.

INTELLIGENCE CHALLENGES

The three key Intelligence challenges are:

[1] That part of cyberspace that is not hardware or software. Human interpretation of and contribution to information. Human thought processes influence by cyber.
[2] A foreign intelligence service for Canada - Canadian Defence & Foreign Affairs Institute 2007
[3] This is China's grand strategy for world domination economically and tied directly to military power and espionage.
[4] Misinformation is mistakes about the truth, disinformation is lies about the truth

1. Perhaps, the greatest challenge of our lifetime will be the war on truth - from foreign influence, interference and mis-information;
2. Rebalancing the playing field from Global economic competition;
3. Getting in front of[5], the proxy wars between nation states who are directly targeting the private sector (often over cyberspace) thus bypassing the military, intelligence, security and police.

Canada has a blind spot when it comes to strategic foresighting, information collection and intelligence production relating to the political, military or economic activities of foreign states for the purpose of protecting Canadian interests globally.

The information domain is blocked, balkanized, censored and denied in over 127 countries, thus greatly impairing our view from Canada, and limiting the fidelity and acuity of our foreign and military intelligence. Furthermore, the intelligence community will need to better demonstrate direct value to the socio-econonic well-being of Canadians and businesses.

Economic security and intelligence will require strong industry partnerships.

For many of these reasons, it is more important than ever that we consider establishing a Canadian Foreign Intelligence Service, to provide accurate and timely foreknowledge to the capabilities, plans, designs and deceptions, of which our adversaries prefer to keep hidden.

HISTORY

Historically, the foreign intelligence mission has been segmented across multiple agencies and departments; leaving strategic gaps, operational exposures and creating inefficiencies, while driving up costs and risk. Divergent mandates and priorities have further segmented the business. Regressive legislative interpretation and policy decisions since 1990, and most recently in 2021, have exacerbated the situation substantively, thus requiring a reframing of Canada's approach.

"The Canadian security and intelligence community is focused on domestic threats. These are important, no doubt, but in an increasingly globalized world, where neither travel, commerce, communication, and especially conflict, are domestic, it has become necessary to develop a capacity for acquiring timely intelligence regarding the intentions and capabilities of foreign states, corporations, and non-state political and religious actors."[6]

THE INTELLIGENCE BUSINESS

Espionage is the World's second oldest profession.

Foreign Intelligence is serious business. One needs a system (people, processes, technology) designed for a singular purpose. The culture and game is entirely different than security or

[5] CFIS could get close to or infiltrate adversaries. Deploy forward in contented environments or adversarial space.
[6] IBID

signals intelligence, diplomacy, military operations or law enforcement.

You can't take volleyball, basketball and soccer players and ask them to play competitive hockey.

Foreign intelligence agencies require fundamentally different: talent, technology, infrastructure, organizational models, legislation, training, tactics, techniques and procedures (TTP). One of the noteworthy differences is that a foreign intelligence service operates clandestine assets abroad in contested or hostile environments not necessarily pursuing threats but opportunities. Hence, foreign intelligence services distinguish themselves with an extended global infrastructure, enhanced stealth, operational security and a greater assumption of risk.

It could be envisioned that a foreign intelligence service could fulfill a number of missions in the cyber domain: from recruiting agents within adversarial cyber programs, analyzing nation state capabilities, attribution of actors, recruiting and running sources online, conducting close access operations, foresighting or determining strategic intent.

The military is also deeply concerned with the collection, processing, analysis and dissemination of information from all-sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, and their impact or potential effects on national security and defence issues.

ATTRIBUTION

Attribution will likely remain a challenging problem for the intelligence community, particularly in Cyberspace, but is also the most necessary for effective deterrence, defence and as a legal imperative for effective countermeasures. Cyber intelligence, attribution and targeting, will require close partnerships with industry and government departments.

DEFINITIONS

Defining foreign intelligence is perhaps the most fundamental yet complex practical challenge. It is not just intelligence collected on foreigners abroad but can include intelligence collected within Canada, or cyberspace and may even touch on Canadians.

Starting with the distinction between Security Intelligence (SI) and Foreign Intelligence (FI). Intelligence helps to manage complexity not just counter threats.

Security Intelligence (SI) pertains threats against Canada whereas Foreign Intelligence (FI) involves information collection relating to the political or economic activities of foreign states.

In reality, the Canadian Security Intelligence Service, Global Affairs, Department of National Defence, Royal Canadian Mounted Police and the Communications Security Establishment collect both security intelligence and foreign intelligence to various degrees. The differences are very nuanced.

The Canadian Security Intelligence Service has both a SI and FI mandate and may investigate threats to the security of Canada anywhere. CSIS collects and analyzes threat-related information, which is typically disseminated to government partners through intelligence reports and other intelligence products. Key threats include terrorism, the proliferation of weapons of mass destruction, espionage, foreign interference and cyber-tampering affecting critical infrastructure. CSIS authorized to collect SI abroad from foreign agencies through liaison, run human sources and forward deploy collection assets. CSIS may also take measures to reduce threats to the security of Canada in accordance with well-defined legal requirements and Ministerial direction. CSIS can also assist the Minister of National Defence or the Minister of Foreign Affairs to collect information or intelligence relating to the capabilities, intentions or activities of any foreign states or group of foreign states in defence of Canada or the conduct of the international affairs of Canada, was limited to acting within Canada,

The Communications Security Establishment (CSE), has the government mandate to collect signals intelligence outside of Canada, covertly or otherwise, information from or through the global information infrastructure, in accordance with the Government of Canada's intelligence priorities. CSE is not permitted to collect Human Intelligence (HUMINT). The CSE mission includes alerting the government to the activities of foreign entities that seek to undermine Canada's national prosperity and security. Signals intelligence activities relate to foreign-based cyber threats, espionage, terrorism, kidnappings of Canadians abroad, Note that these are SI functions. More substantively, CSE foreign intelligence also supports government decision-making and policy-making in defence, security and international affairs by providing important insights into global events. Note the CSE appears to define Foreign Intelligence and any intelligence not targeting Canadians whether it is for SI or FI.

Military Intelligence (MI) within the Canadian Armed Forces is concerned with providing relevant and correct information to enable commanders to make decisions. This definition is exceptionally broad, but in practice is taken to mean pertaining to authorized military targets in theatres of operation abroad or restricted to military bases within Canada.

Criminal intelligence is the mandate of Law Enforcement Agencies (LEA) such as the RCMP. The investigation must related to individuals suspected of breaching the Criminal Code of Canada. The RCMP's mandate, as outlined in Section 18 of the Royal Canadian Mounted Police Act, is multi-faceted and includes preventing and investigating crime; maintaining peace and order; enforcing laws; contributing to national security; ensuring the safety of state officials, visiting dignitaries and foreign missions; and providing vital operational support services to other police and law enforcement agencies within Canada and abroad. The RCMP is unique in the world since it is a national, federal, provincial, and municipal policing body. The National Security Criminal Investigations Program conducts investigations into terrorism, transnational crime, espionage, sabotage, cyber attacks, foreign influenced activities or threats from chemical, biological, radiological, or nuclear weapons et.al. The RCMP has liaison officers stationed abroad. You can see how the RCMP mandate may overlap with CSIS in both SI and FI. However, typically the RCMP get involved when an investigation is reaching the stage of prosecution.

Global Affairs Canada collects diplomatic information and intelligence related to International

Security through their threat assessment and intelligence services division and Global Security Reporting Program (GSRP).

The private sector also works in this space: Multinational Corporations, Commercial intelligence companies, private military contractors (PMC), non-government organizations (NGO), security researchers and academics.

With so many players on the field, a Canadian Foreign Intelligence Service is still necessary because there are still FI gaps between mandates and gaps not filled by existing mandates owing to competing priorities or competencies. The use of HUMINT means of collection outside of Canada remains a critical gap in coverage cannot be adequately addressed through other means. Furthermore, much of Canada's FI requirements are met through what allies chose to share.

"Canada is a net consumer of intelligence produced by others for their own purposes."[7]

ATTRIBUTES OF DISTINCTION

It is envisioned that a Canadian Foreign Intelligence Service would principally be a HUMINT agency exclusively operating external to Canada. Nevertheless, if we look at similar agencies like Canadian Intelligence Agency (CIA) and the British Secret Service (MI6), only 20 percent of the volume of intelligence is achieved from human sources. It is reasonable therefore to expect that a Canadian Foreign Intelligence Service would need to have a sophisticated organic open source and technical intelligence collection capability dedicated to their unique operational missions and mandates. Commensurately, an all-source analytical capacity would be needed to corroborate sources, provide context and develop narrative for that reporting makes sense to clients and is actionable. Contextualized analysis and the normalizing the reporting by each agency helps prepare the material for central analysis and consolidated intelligence estimates.

COOPERATION AND COVERAGE

As previously mentioned, many government agencies and private sector entities collect both SI and FI. This overlapping coverage requires cooperation, collaboration and coordination, the management of intelligence equities and operational de-confliction. A Canadian Foreign Intelligence Service would fit into this rubric while providing unique value to the community.

A great example of grey area is that of nuclear weapon proliferation. Certainly, one can make the case that this is both a FI or SI issue. Multiple agencies have a vested interest in this subject. Duplication of efforts or operational fratricide are a concern as is absence of engagement by any agency.

VALUE PROPOSITION

The value proposition and performance measurements between law enforcement, signals, security and foreign intelligence are objectively different. Trying to support national security,

[7] IBID

global economic competitiveness, environmental, or world health with intelligence from within Canada is limited. A global worldview means that one needs to be well-positioned abroad. Even domestic mandates require global perspectives. Security intelligence and threat intelligence often need foreign intelligence to determine adversarial capability and intent.

A foreign intelligence service can provide a significant return-on-investment for a country while protecting citizens and institutions. A sovereign foreign intelligence service allows for:

- Direct and targeted answers to important questions for analysts and decision makers;
- Enhanced Situational awareness and understanding of the global competitive space particularly that which is deliberately hidden from view;
- Context and external perspective;
- Advanced warnings and indicators from outside of Canada;
- Deterrence and covert signaling to avoid strategic miscalculation such as trade disputes, or conflict. Espionage has been credited with averting nuclear war on several occasions;
- Pre-emptively countering industrial espionage while promoting competitiveness through actionable business intelligence;
- Positive attribution of foreign actors. Without a foreign intelligence capability, there can be no end-attribution necessary for prosecution or targeting;
- Greater efficacy and coverage than current methods of gatherings foreign intelligence;
- Corroboration from multiple sources for enriched accuracy; and
- Mitigating strategic surprise for health, global affairs, politics, trade and the military.

Economic security matters to Canadians. Foreign state-sponsored industrial espionage is serious. CSIS in their 2021 annual report recognizes that espionage and inference is a primary threat to Canadians. Similarly, the FBI reports two–thousand open cases involving just Chinese espionage and interference with a new case every ten hours. Nearly every Canadian will be affected by foreign source cyber attacks, costing the country over $1 billion annually. We will need FI to play forward and close the attribution chain.

Only with enhanced foreign intelligence and security intelligence collection abroad will Canada be able to foresee and counter such threats, while competing globally. Otherwise, the first time we are seeing an attack is after it has hit our shores. Perhaps, compromising cyber systems, infiltrating supply chains, disrupting national response to the pandemic, or interfering with the democratic process. Reacting to threats is costly and leaves few options. It puts extra burden on security and law enforcement agencies.

CULTURE JAMMING

Canadian politicians and judiciary need to stop pretending that we live in a walled garden or that the current system is good enough. All G20 nations have foreign intelligence services - except Canada. Few of our adversaries actually believe that Canada does not conduct foreign intelligence operations, and as consequence, innocent Canadian citizens are arrested on fabricated spying charges.

An enduring challenge has been that Canada has little intelligence culture and literacy amongst politicians, the establishment and citizenry. What many Canadians believe about intelligence work comes from watching the news, television shows or Hollywood movies. This makes it exceeding difficult to have deep discussions on national security and foreign intelligence. Foreign Intelligence needs sophisticated clients to help shape primary intelligence requirements, get the most out of the system, and to interpret the end-products.

Hence, the need for an open dialog on Intelligence.

Intelligence is about getting to the truth of the matter and producing action intelligence. There is no substitute for the intellectual hard work of ingesting complex information streams, doing the analysis. All-source foreign intelligence provides context and enhanced narrative with global perspective with a wide-aperture, enhanced acuity and fidelity. Whereas, single-source domestic intelligence only one piece of the puzzle. Relying on allies for our foreign intelligence to access an external worldview, invites cultural and political bias into our decision-making.

We have Canadian content rules in broadcasting and entertainment, but not in intelligence.

Creating a foreign intelligence organization is complex. The Royal Commission of Inquiry into Certain Activities of the RCMP, better known as the McDonald Commission published findings in 1981, found that a law enforcement agency is unsuitable for security intelligence work. Hence, CSIS was established in 1984 as result. The RCMP Security Service, became CSIS overnight, but the resources infrastructure and culture were all based on policing. It took nearly two decades to gradually transform the organization into a security intelligence agency.

The central reason is that policing and intelligence are entirely different in culture, mission and mandate. Police-work starts with a local crime and builds a case for court. The infrastructure and governance is decentralized. Organizational model and data flows are mostly centralized for Security intelligence with regional points of presence. Analysis can either be issue-based or targeted to an actor. Technical intelligence and big data play a more substantive role in production than for a Law Enforcement Agency (LEA). The product is not developed for criminal prosecution but threat intelligence or threat reduction activities. In contrast, a signals intelligence agency is highly-centralized and uses technical sources exclusively to collect foreign data of potential value exclusively for government clients.

The difference between SI and FI is not the geography but the value proposition. FI helps to level-the-playing-field for a country globally by providing unique information to decision makers. FI is mostly not about threats, though it can be, it is about advantage and foreign policy outcomes. A FI service can also provide a covert capability including capacity building to allies. In contrast, SI is a defensive mandate to protect Canadians and Canada (at home and abroad from harm).

It is worth noting that CSIS has collected Security Intelligence (SI) on foreign soil since 1984 and Foreign Intelligence (FI) domestically under Section 16 of the Act. Recent interpretation by the court has curtailed decades of domestic FI collection, and sparked this debate for a Canadian Foreign Intelligence Service (CFIS).

A foreign intelligence service most resembles a security-intelligence service in organizational model but with a number of key differences: it operates abroad and is tasked with information collection and intelligence production relating to the political, military or economic activities of foreign states for the purpose of protecting Canadian interests globally.

For these reasons, a foreign intelligence agency cannot simply be created by transplanting resources and mechanisms from security, police, military or diplomatic worlds. The infrastructure is not reusable, nor is the analytical process. Some skills are transferrable but many are not. Foreign intelligence requires scouting and recruiting unique talent and special training for analysts and operatives. The enterprise will require sophisticated support infrastructure. Collection networks, non-traditional partnerships and a client ecosystem will need to be established from the ground up.

Big data is the currency of all intelligence agencies

A high-performance culture will need to be cultivated to align with new missions and mandates. The fusion of human and technical intelligence will require sophisticated big data analytics - much like SI but with some nuance. Such a foreign intelligence service will rely on open source intelligence (OSINT) to a far greater degree than other agencies and establishments. Architects of the new agency will need to recognize the close link between (OSINT) and Foreign Intelligence (FI) and have deep experience in both. Such a service would require integral Cyber support, distinct from Signals Intelligence SIGINT. The work will be substantively riskier than sitting comfortably back in an office in Canada or behind diplomatic protection. Thus requiring the next-level of operational security (OPSEC) and overwatch.

A national intelligence apparatus requires the integration of SI and FI. Terrorism, counter-proliferation and espionage (such as theft of IP) are now intrinsically linked with trade, aid, monetary and foreign policy. Decision makers need "a rich picture" - which is derived from all-source, integrated analysis rather than a revolving door of SI, FI, LEA, SIGINT and Military Intelligence (MI) message-bearers all providing valuable but unique perspectives on key issues.

The good news is that a sovereign solution was designed in the 1990's when these questions were first asked. Allies, adversaries and industry have already paved the way. It is worth noting that, the power-shift between nation states and non-state players will be particularly acute. Already a commercial intelligence market has emerged with the rise of OSINT and data brokers to fill the gap.

"By refusing to use secret foreign intelligence gathering, Canada fails to do all it can to provide industry with the information needed to compete successfully in foreign markets, to say nothing of wider political matters."[8]

REALISTIC COSTS AND TIMELINES

Common criticisms for the establishment of a Canadian Foreign Intelligence Service are the

[8] IBID

potential costs and timelines. Some would say that such an agency would be enormously costly and take a generation to reach maturity, Such can be ill-afforded during a time of final restraint and deficient.

Firstly, we cannot to compare a potential Canadian Service to US agencies. The CIA is a colossal enterprise including the launching of satellites and conducting paramilitary operations. A CFIS would have a much tighter focus.

"Even a small espionage service with a limited number of strategic targets, given well-trained espionage officers, tough offensive tactics, and a bit of luck, could well produce intelligence of very high value to Canada and its closest allies on matters."[9]

It is true that establishing deep clandestine HUMINT networks takes time. However, standing up an interim capability can be achieved quickly at a reasonable cost. It is a question of leadership, expertise, efficacy and concentration.

Intelligence production can start early while the organization is still building capacity. This can be achieved by leveraging deep field research, advanced OSINT, technical means, outsourcing, or leveraging government and industrial partnerships. There are a number of great models within the commercial intelligence space including: country profiles, counter-influence, de-radicalization, human rights, technological foresighting, cyber attribution and threat reduction.

A Foreign Intelligence Service has greater opportunity to pay for itself than conventional security intelligence because FI can deliver geo-political and economical intelligence, which converts into generating monetary profit while limiting financial losses.

THE WAY AHEAD

How we go about envisioning and creating a Canadian foreign intelligence service is important. Such a service is substantively different that what already exists. The talent and expertise will not be exclusively found within the current establishment. Nor should decision-makers in the federal government limit from whom they seek council.

CONCLUSION

In conclusion, Canada requires an independent Foreign Intelligence Service to protect national interests in a globalized competitive environment. A foreign intelligence service would need to be an independent agency with separate legislation and mandate but subject to national intelligence review and oversight. In this discussion paper we have provided recent historical context, shown why a distributed foreign intelligence mandate has not functioned as it should and highlighted systemic gaps in coverage. Foreign intelligence, conducted abroad principally by recruiting human sources, is fundamentally different from current missions. Emerging threats, competition and opportunities in global security environment make for a compelling case

[9] Should Canada Have a Foreign Espionage Service? - Richard Geoffrey St. John, Canadian Military Journal

for a Canadian foreign intelligence service – one that has a unique value proposition. The common arguments against a new agency - essentially cost, timelines, risk and redundancy – are speculative. The opposite is likely true. The cost of building a sovereign capability is far less than the price that Canadians are paying for not having one. For example: advanced warning of the pandemic, which a foreign intelligence service may have been able to provide, could have saved billions of dollars and thousands of lives, paying for itself overnight. A foreign intelligence service would not compete with, but complement other agencies. Hence, its mandate and resourcing would be tightly focused. A new service could be stood up rapidly, and cost-effectively, using near-gen technology, modern business processes and industrial partnerships, without the expense of inheriting legacy infrastructure or culture. There are a number of poignant examples of foreign intelligence capacity building which lend support to this conclusion.

The challenge is more complex than many perceive, but not as unsolvable as some would have led us to believe.