Centre for International
Governance Innovation

Reimagining a Canadian National Security Strategy | No. 6

Prepared: Canadian Intelligence for the Dangerous Decades

Greg Fyffe

Reimagining a Canadian National Security Strategy | No. 6

Prepared: Canadian Intelligence for the Dangerous Decades

Greg Fyffe

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
CIGI Senior Fellow and Project Co-Director Wesley Wark
Manager, Government Affairs and Partnerships Liliana Araujo
Senior Publications Editor Jennifer Goyder
Graphic Designer Sami Chouhdary

Centre for International Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Project

Canada's approach to domestic and international security is at a profound moment of change. The shock wave of COVID-19 and its looming future effects highlight the urgent need for a new, coordinated and forward-looking Canadian national security strategy that identifies emerging and non-traditional threats and considers their interrelationships. Complex interactions between foreign policy, domestic innovation and intellectual property, data governance, cybersecurity and trade all have a significant impact on Canada's national security and intelligence activities.

Reimagining a Canadian National Security Strategy is an ambitious and unprecedented project undertaken by the Centre for International Governance Innovation (CIGI). It aims to generate new thinking on Canada's national security, inspire updated and innovative national security and intelligence practices, and identify ways that Canada can influence global policy and rulemaking to better protect future prosperity and enhance domestic security.

CIGI convened interdisciplinary working groups, which totalled more than 250 experts from government, industry, academia and civil society, to examine 10 thematic areas reflecting a new and broad definition of national security. Each thematic area was supported by senior officials from the Government of Canada, designated as "senior government liaisons." They provided input and ideas to the discussions of the working group and the drafting of thematic reports. Project advisers provided support and advice through specific lenses such as gender and human rights. This was critical to strengthening the project's commitment to human rights, equity, diversity and inclusion.

The project will publish 10 reports, authored independently by theme leaders chosen by the project's co-directors. The reports represent the views of their authors, are not designed as consensual documents and do not represent any official Government of Canada policy or position. The project was designed to provide latitude to the theme leaders to freely express new thinking about Canada's national security needs.

A special report by the project's co-directors, Aaron Shull and Wesley Wark, will analyze Canada's new national security outlook and propose a security strategy for Canada.

About the Author

Greg Fyffe was president of the Canadian Association of Security and Intelligence Studies from 2012 to 2021. He served as executive director of the Intelligence Assessment Secretariat in the Privy Council Office from 2000 to 2008. He is currently a consultant and facilitator/instructor with the Telfer Centre for Executive Leadership and the Centre on Public Management and Policy, both part of the University of Ottawa, and teaches courses focusing on intelligence and security, leadership, and strategic thinking.

Acronyms and Abbreviations

CAF	Canadian Armed Forces
COMINT	communications intelligence
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CSIS Act	Canadian Security Intelligence Service Act
DNI	director of national intelligence
GSRP	Global Security Reporting Program
HUMINT	human intelligence
IMINT	imagery intelligence
IP	intellectual property
MIGs	Mission Intelligence Groups
MPs	members of Parliament
NATO	North Atlantic Treaty Organization
NSC	National Security Council
NSIA	national security and intelligence advisor
NSICOP	National Security and Intelligence Committee of Parliamentarians
ODNI	Office of the Director of National Intelligence
ONA	Office of National Assessments
ONI	Office of National Intelligence
OSINT	open-source intelligence
PCO	Privy Council Office
SIGINT	signals intelligence

Executive Summary

This report focuses on two key elements of Canadian intelligence — collection and assessment — and the related institutional structures. All need to be upgraded.

Canada's allies frequently evaluate the effectiveness of their intelligence communities. This report proposes some significant changes in the Canadian intelligence community. A core recommendation is that Canada follow the example of our allies and initiate a comprehensive review of our security and intelligence capabilities — and follow up with changes prompted by the review results.

The current threat environment features renewed great power competition, compounding cycles of technological change, climate disasters and the increasing fear that we are entering an age of serial pandemics. Leaders confronting these dangers will require strong intelligence support to complement other sources of expert knowledge.

They will also need the support of an informed public. A regular, comprehensive published review of the government's assessment of the national and international security environment would generate productive public debate.

Coordination of intelligence and security in Canada has steadily improved, but our system needs a higher degree of integration. Without the necessary changes in governance, it will be more difficult to have an integrated perception of threats and achieve maximum effectiveness in dealing with them.

The last major upgrading of Canada's intelligence capacity was a necessary response to September 11, 2001. Canada must now match its intelligence resources to the certainty that we face decades of international volatility that will directly affect the lives of Canadians and the prosperity of our country. The intelligence community must be able to provide the support that Canada's leaders will need to face a prolonged period of interconnected dangers.

The report makes the following recommendations.

→ The Government of Canada should conduct a comprehensive review of the Canadian security and intelligence community, and its capabilities. This practice should be repeated regularly in future years.

→ The Government of Canada should publish a regular national security review with a comprehensive definition of threats.

→ Canada should establish a Canadian National Security Council (NSC) to promote greater integration of the Canadian community. While drawing on the many integration and coordination bodies of our allies for ideas, a Canadian NSC should reflect Canadian needs, experience and governance structures.

→ The position of national security and intelligence advisor (NSIA) should be reviewed and confirmed by statute. NSIAs should be appointed for a five-year term.

→ The Canadian Security Intelligence Service Act (CSIS Act) is dated and should be revised to meet the current threat environment.

→ The Canadian Security Intelligence Service (CSIS) should have the capacity to collect foreign intelligence abroad if necessary for foreign and defence policy or operational reasons. Approvals should mirror the current requirements for foreign intelligence collection within Canada.

→ There should be a common community platform for open-source intelligence (OSINT) and a designated senior official responsible for maximizing the effective use of open sources.

→ The resources allocated for intelligence assessment should be reviewed to ensure that analytical capacity matches intelligence collection capacity and client need.

→ Canada should make greater use of experts from outside the intelligence community by establishing a Joint Strategic Warning Committee composed of community professionals and outside experts.

→ The Canadian community should develop a contingency plan to deal with the possibility that the fractious politics in the United States will have a negative impact on the US intelligence community and the intelligence relationship with Canada.

→ Canadian security and intelligence agencies should have the capacity to provide regular unclassified briefings to members of Parliament (MPs) as requested and appropriate.

Introduction

Governments require comprehensive information and insightful analysis to design policies and operationalize them. In many domains, information needs can be met from government resources or generated from public sources.

When the focus is on the intentions of malicious domestic organizations or hostile foreign actors, information is frequently not available from easily accessible sources.

Uncovering and analyzing threats to national security and public safety is the core mandate of Canada's intelligence collection agencies. Intelligence agencies are expected to be effective, secret where necessary, transparent where possible and always accountable.

Intelligence organizations are necessarily protective of secrets, but the definition of what that necessity is has changed. Intelligence agencies now report regularly on how they are acting against priority threats. There are limits to what intelligence organizations can reveal and still operate effectively. The linked principles of transparency and accountability assure Canadians that intelligence organizations work within a framework that protects rights and privacy.

Canada's Five Eyes allies (Australia, New Zealand, the United Kingdom and the United States) have evolved ways of improving their intelligence collection and assessment systems. All have comparable institutions for accountability. We could benefit, as our allies have, from regular public reviews of effectiveness measured against threats. Reviews reach their highest potential for productive reform if they are driven by an informed public and responsive governments.

How much has the security environment changed?

Twenty years ago, the Twin Towers in New York were destroyed by a terrorist attack. Canada's own interests, and reciprocal obligations to allies, required new resources and a reorganized Canadian intelligence and security community. Since 2001, pressures on Canadian diplomacy, the Canadian military and Canada's intelligence and security community have escalated.

Despite one attempt at a comprehensive review of Canada's national security policies after 2001, Canadian governments have chosen an incremental approach to informing the public about the threats to Canada's security. Unlike most of its allies, Canada has not adopted the practice of regularly publishing a strategic overview of all dangers and the resulting integrated set of priorities. No review can see every danger, but periodic comprehensive reviews ensure that important changes in the threat environment are described in a coherent and integrated way. An incremental approach cannot mobilize Canadians inside and outside government to anticipate dangers and drive necessary change.

The CIGI project Reimagining a Canadian National Security Strategy is a review of the dangers Canada faces and potential responses. In common with the other themes, the Rethinking the Role of Intelligence working group was composed of an eclectic group of experts. The task has been to anticipate the capacities and organizational structures Canada's intelligence community will need. Discussions have drawn on the deep knowledge of academics and practitioners from Canada and our Five Eyes allies. Their informed views on the geopolitical environment, different organizational options and the implications of new technologies, have been invaluable. This report draws on the working group discussions, but also explores ideas for expanding system effectiveness beyond those raised by the working group.

The report assumes a dual audience — those in the Government of Canada responsible for the security and intelligence community, and the interested public.

Developing capabilities requires investment, but also a consensus that the capabilities are needed and can be developed at an acceptable cost. Since Canadians are impacted by current security risks both as individuals and as citizens, public debate is an important complement to internal government analysis. An effective intelligence system ultimately rests on a strong intelligence culture in both government and the public — an informed expectation of what intelligence can and should contribute to peace, order and good government.

This overview of Canada's intelligence system, and the recommendations, are intended to provide the stimulus for a comprehensive government review, which should draw on both outside perspectives and inside experience. As noted,

Canada's allies regularly conduct reviews of all aspects of their intelligence systems, and the resulting reforms upgrade the ability of their intelligence communities to match capabilities to rapidly evolving dangers. Canadian capabilities need the same regular examination.

Since this report is focused on intelligence collection and assessment, the reference is usually to the "intelligence community" rather than the "intelligence and security community." In fact, the two mandates are intertwined, but the report does not examine many issues that are exclusively on the security side, some of which are probed by other reports in the Reimagining a Canadian National Security Strategy project.

The hope is that the report will give readers a good overview of the intelligence community. Where there is a strong reason for advocating a significant change, there is an explicit recommendation. In other instances, the report describes a function for which it would be difficult to make a credible recommendation from the sidelines.

For similar reasons, the intelligence capacities of the Canadian Armed Forces (CAF) are referred to in passing, not because they are unimportant, but because they constitute a separate and diverse universe.

The Threat Environment and the Canadian Context

Intelligence capabilities and priorities reflect identified threats and government capacity. All of these evolve constantly, but new dangers appear more often than old ones recede.

This is a perilous time for national and international security. More than in the past, Canadians are alert to the consequences of the dangerous decades ahead for themselves and for Canada.

The signals of danger are pressing:

- We have reverted to a period of great power rivalry. The United States, China and Russia assert incompatible versions of international security.
- State and non-state actors are exploiting new cyber capabilities to conduct espionage, subversion and sabotage, and enable fraud and ransomware.
- False information campaigns deliberately poison the information reservoirs of democratic societies. Information operations by foreign entities are aided by domestic conspiracy theorists spreading absurd and harmful beliefs.
- The nature of potential conflicts has been expanded by information technology. A future conflict could include armed conflict, remote attacks on infrastructure, the paralysis of rival economies or combinations of all of these.
- Terrorism evolves, but persists, enabled by failing states, civil conflicts and modern weaponry. Violent extremist ideologies have multiplied and spill across national frontiers.
- Modern information technology tools have increased the dangers from insiders serving a personal agenda or providing sensitive information and technology to foreign state and non-state actors.
- The danger of pandemics is ongoing, without, so far, the international coordination needed to defeat them. Biosecurity has become a central component of every country's national security, and global security more generally.
- Universal threats, including not only climate change and pandemics but also violent extremism, foreign interference, weapons proliferation, mass migration and the unpredictable interactions of these with new technologies, threaten the natural environment and the stability of nations.

These new globalized challenges require all governments, including Canada's, to urgently update the capacities of their intelligence communities.

Canada's Intelligence Capacity and Requirements

Canada's geographic position has historically protected Canada from immediate threats. We are surrounded by oceans and share a border only with the United States.

The geography has not changed, but the array of threats has. Weapons technology has steadily increased the speed with which an existential threat could reach Canada's frontiers. The reaction time has been reduced from hours to minutes. Cyber weapons are now capable of inflicting extensive damage in milliseconds.

Canada has not escaped the storm of great power rivalries in the past and is liable to be drawn into them again in future.

The rapid development of information technology has generated new attack pathways. Internet-based threats, and other attack vectors, compromise both security and economic prosperity. Canadian government and strategic infrastructure can be rendered useless through cyber penetrations by foreign actors, government or criminal, and sometimes by internal actors. Companies may lose intellectual property (IP), which destroys their competitive position and their contribution to the Canadian economy. Individual Canadians must constantly guard against malware, which can destroy their personal data, steal their identity for criminal exploitation, or be the first step in an expensive fraud. Our relative geographic isolation is no longer a protection. Life online is life in a danger zone, and the danger zone is global.

The amount of information that can be stolen by a cyberattack is vast and unlimited in comparison to what could previously be extracted by a well-placed human spy. Protecting Canada's economic assets is increasingly linked to our ability to deter cyber compromises of databases, and accurate threat intelligence.

The pandemic has shown that accurate detection and risk assessment are vital. The climate emergency has complex interactions with the security environment, the economy and immigration. In all cases, warning must be connected to an accurate assessment of consequences, including security consequences.

The international security environment is unsettled, with multiple risk drivers.

What does this mean for Canada's security and the Canadian intelligence community?

- → Defending Canadian communications and data assets is a top priority. This has implications for all government departments, whether for their own assets and communications, or for services they provide to other government entities.
- → Threats to critical infrastructure, most of which is in the private sector, are constant and potentially hidden. Most data assets are also in the private sector.
- → Insider compromise of data systems can be costly and undermines the confidence of allies in Canada's security and counter-intelligence alertness.
- → The pandemic has expanded the definition of what critical infrastructure includes by showing the complexity of goods and services networks.
- → Government security and intelligence capacities need to be linked with those of the private sector to protect critical infrastructure and IP vital to the economy.
- → Traditional secret intelligence collection on malicious state and non-state actors can now be supplemented by greater use of open and partially open sources.
- → The criminality threat to individual Canadians has dimensions beyond the capacity of local law enforcement to deal with. Criminal regimes, or regimes that permit criminal activity, are a preoccupation of Canada and its allies.
- → Detection and risk assessment on pandemic threats, and on the security consequences of climate change, will be preoccupations for the intelligence and security community.
- → Climate change and pandemics must be added to the increasingly long list of transnational challenges that interact with core intelligence community priorities.

To respond, Canadian decision makers need to be served by an integrated and effective intelligence community, able to provide them with comprehensive information and insightful analysis.

Intelligence and Governance

Intelligence and security is one of the defensive portfolios of government. It must be handled well, mostly without public acclaim. However, it is a close partner of international and domestic portfolios that actively advance Canada's international interests and protect security and stability at home.

While there are obstacles to openly claiming credit for success, there is an open-ended credibility risk if crises are not anticipated and managed. Journalistic coverage reinforces this unequal pairing of credit and risk. Successes are veiled; failures are a conspicuous drama of incompetence.

A natural reaction for governments is to push security and its necessary companion, intelligence, into the untouchable zone — a bothersome intrusion on scarce leadership time.

There is a prudent alternative. Unsettling surprises and distracting emergencies can be avoided by creating a system that informs the prime minister and Cabinet of pending crises, warns of credible dangers and ensures that when the worst does occur, the leadership response is measured and informed. Anticipation is the product of a wise use of resources by dedicated government structures.

An investment of time and attention when dangers are distant can produce effective reactions when they arrive. As the COVID-19 pandemic has demonstrated, discounting disagreeable warnings and pressing dangers multiplies the eventual pain.

Intelligence Collection and Intelligence Analysis

The principal intelligence activities are collection and analysis.

"Intelligence" describes an array of information categorized by collection method, source and apparent value. Classification ranges from unclassified to top secret and above. Usually, some aspect of intelligence activity is classified, whether it is the source, the method, or the analytical and operational conclusions that are reached. Human intelligence (HUMINT) is collected by agents. Signals intelligence (SIGINT) intercepts all types of electronic emissions. An important sub-category is communications intelligence (COMINT), which gives access to the communications of a target (whether a terrorist or a nation), and is often encrypted, which means that COMINT agencies are also experts in cryptology. Many categories of SIGINT are highly technical and exploited principally by militaries. Satellites and drones capture still and video imagery (imagery intelligence [IMINT]), and electronic emissions.

OSINT has grown from the exploitation of completely open sources, such as newspaper reporting, to a highly sophisticated domain. Social media posts are a prime source. Imaginative techniques uncover information that is difficult to access, and often of high value, but not secret.

Different intelligence activities are captured in the concept of the "intelligence cycle." Clients and intelligence leaders set priorities, which are translated into collection activities. Intelligence must be processed — decrypted, translated, evaluated, summarized and classified. It must be securely distributed to clients, analysts and security operations. Intelligence assessment judges the reliability, value and implications of the information for the benefit of decision makers, investigators or operational planners. It can convert a collection of diverse intelligence into an insightful analytical conclusion or a warning of pending danger. This last step, distilling intelligence into useful conclusions for decision makers, requires both useful assessments and receptive clients.

Intelligence is essential because threat actors hide their motives, capabilities and intentions. Today, "threat actors" includes states, terrorists, violent extremists and criminal organizations.

Canada has a strong intelligence capacity of its own through agencies such as CSIS, the Communications Security Establishment (CSE) and the CAF. However, our overall intelligence access is lifted to that of a middle power by our membership in the Five Eyes alliance.

Intelligence may reach decision makers in the form of an intelligence report limited in subject matter and sourcing. At senior levels, the need is for an analytical product that integrates many types of information to insightfully answer specific policy-relevant questions. If the investment in intelligence collection is not complemented by adequate assessment resources, then its value is limited. The Canadian community is served by many skilled intelligence analysts. A recurring question is whether analytical resources are adequate, well-integrated and used to maximum effect.

Canada's Current Intelligence Capacity

Significant resources were added to the Canadian intelligence community after September 11, increasing both counterterrorism and core capabilities. The Department of National Defence is engaged in a major expansion and internal review of its intelligence capacity, which builds on previous enhancements. Canada has traditionally seen the capacity of CSE as a major contribution to the Five Eyes alliance and has continued to make it a priority for new resources. Unlike its alliance partners, Canada does not have a dedicated foreign intelligence HUMINT agency.

Organizationally, Canada upgraded the capacity of the Privy Council Office (PCO) to coordinate the intelligence and security community by establishing a national security advisor in 2004 (now NSIA with "intelligence" added). Two PCO secretariats report to the NSIA — Security and Intelligence, and Intelligence Assessment. Under the NSIA are several coordinating committees of deputy ministers and assistant deputy ministers from community departments and agencies.

The intelligence capacity of the community has increased, and community integration structures have been improved. Every intelligence power continuously reviews its intelligence collection capacity and organizational structures to meet evolving threats. Canada has the same need for the same reasons.

Specific Intelligence Capabilities

COMINT

CSE is Canada's communications intelligence agency. As such, it is part of the Five Eyes communications intelligence network. Canadian decision makers and analysts benefit from the strong capacity of CSE and receive a large flow of Five Eyes material. CSE is recognized within the Five Eyes as having an expert capacity in multiple areas of communications intelligence and cryptology.

Canadian governments have considered CSE's recognized capacities in communications intelligence and cryptology to be an important contribution to the Five Eyes alliance, and it has been funded accordingly. CSE has an important role in the alliance, in protecting Government of Canada data assets and, increasingly, in liaising with private companies whose security is important to the Canadian economy.

The Cyber Challenge

The principal output of CSE is communications intelligence, but communications agencies are the natural home for the development of cyber capacity. CSE has been active in this field with its Five Eyes partners and under the Communications Security Establishment Act 2019[1] was given authority to conduct offensive and defensive cyber operations.

This capacity is important to the security of Government of Canada operations, the protection of IP vital to Canada's economic prosperity, the integrity of its democratic institutions and the safety of Canadians online.

- New cyber technologies provide hostile state and non-state actors with unparalleled opportunities for espionage, subversion and sabotage.
- The threat surface for the Canadian government has dramatically increased, with boundaries blurred between national security, critical infrastructure, the private sector and the everyday, online lives of Canadians.
- Social media makes it quicker, cheaper and easier to propagate disinformation than ever before. Disinformation undermines democracy, leads citizens to make distorted judgments about their own society and undermines public health policies.
- The protection of infrastructure has been a continuing priority for Canada's government, including the security and intelligence sector. The risks have steadily grown as malicious actors, including foreign states, have increased their capacity to compromise computer systems and databases, possibly for a prolonged period without detection. The risk is that infrastructure will be damaged or immobilized at a critical period. Russia has frequently launched infrastructure attacks against other countries. China, North Korea and Iran are also active. However, the capacity for target countries to retaliate has also increased.

1 See https://laws-lois.justice.gc.ca/eng/acts/C-35.3/.

- Internal threats have required additional attention to internal security and counter-espionage capabilities.
- The ability of non-state actors, usually criminal, to endanger infrastructure or enable fraud has also mounted. Some state actors, notably Russia, permit malicious actors to operate without interference because their actions may serve state objectives. Ransomware is a major threat because it can shut down any company, facility, utility or individual that downloads malicious software. This is a constant risk. Because ransomware attack vulnerability is widespread and random, there is an ongoing threat to public safety if hospitals, fuel systems, transportation, vital supplies or public safety forces are incapacitated.

Countering the impact of disinformation is more than the Canadian intelligence community (or any other intelligence community) can or should undertake on its own. Instead, it is necessary for the Canadian intelligence community to collaborate with the private sector, particularly the tech giants, to promote digital literacy and resilience against disinformation among Canadian citizens.

The Canadian Centre for Cyber Security provides unclassified information to Canadian entities to assist them in protecting proprietary information and infrastructure security. CSE also shares classified intelligence as appropriate for the same purposes.

While COMINT itself is a flexible collection platform, which can be redirected to other targets and priorities more easily than HUMINT, redirection may require new personnel capacities that can be difficult to start up. Some buffer capacity is necessary in a volatile environment.

COMINT and cyber capacity are both vital to Canada's security and have been a priority for government support. (Note: A separate report from the Reimagining a Canadian National Security Strategy project addresses cyber issues in detail.)

HUMINT

The debate over the absence of an explicit foreign intelligence HUMINT agency is long-standing in Canada, dating back to the period immediately after World War II.

CSIS was set up as a domestic security agency and the CSIS Act of 1984[2] emphasizes this focus. Under the CSIS Act, foreign HUMINT can be gathered within Canada, and security intelligence can be collected outside Canada. CSIS is excluded by section 16 of the CSIS Act from collecting foreign intelligence abroad that is not related to Canadian security.

The debate on this restriction in the collection mandate of CSIS has focused on whether Canada should have a HUMINT foreign intelligence capacity. If Canada did collect foreign intelligence abroad, should that capacity be assigned to CSIS or to a separate agency, because of the different methods and legal basis for domestic versus foreign intelligence collection?

There are many sources of foreign intelligence. As noted above, CSIS can obtain some foreign intelligence within Canada. We have other agencies that collect foreign intelligence by technical means, and we have access to Five Eyes HUMINT, and some incidental HUMINT from other allies. Global Affairs Canada's diplomatic reporting and assessments provide insight into foreign actors.

The gap in HUMINT collection is narrow but potentially important. CSIS cannot collect foreign HUMINT on an issue that does not directly touch Canada's national security. What is included and excluded by this provision can be ambiguous. Canada does have foreign policy priorities not directly related to our own security. Canadians have business assets in other countries. There will not always be allied intelligence that helps to advance Canada's perspective. Canada tracks human rights abuses and has an interest in countries that are sources of immigration. We support collective action by international bodies, sometimes in agreement with our allies and sometimes not.

Collecting HUMINT has become more challenging because modern technology makes it easier to track the movements of suspected intelligence agents and their contacts. Technology also frustrates the elaboration of credible cover identities for intelligence agents. Even if it is accepted that Canada does, at times, need foreign intelligence not directly related to security, the traditional resistance to a separate Canadian

2 See https://laws-lois.justice.gc.ca/eng/acts/c-23/.

intelligence agency is reinforced by doubts about the future of traditional HUMINT.

A recent decision of the Federal Court validated the extraterritoriality of CSIS warrants, and allows the agency to conduct operations abroad, even if they break the laws of the country involved. However, this supports the existing ability of CSIS to collect security intelligence abroad. It does not modify the section 16 provision limiting the collection of foreign intelligence to within Canada.

The argument that Canada can get most of the intelligence it needs is valid, but there are collection gaps, which could be significant on critical files. The immediate question is whether it would be appropriate for CSIS to have the authority to collect on these gaps on a case-by-case basis when there is an explicit need for Canadian HUMINT. This could support Canadian foreign policy objectives.

The choice is not necessarily between no change to the limitations on foreign HUMINT and initiating a major new capacity. There will be times when CSIS or its agency partners need access to foreign-collected HUMINT to serve an important intelligence or foreign policy requirement.

Permitting the collection of foreign HUMINT on a limited, as-needed basis, would give Canada the potential to initiate collection within its current capacities and networks. This would be a careful step toward meeting future intelligence requirements in a fraught international environment. It could enable a CSIS representative to canvass other countries for what they could share, or to undertake limited collection operations. It would recognize that international and domestic threats are increasingly entangled.

The actual results of a limited ability to collect non-security foreign intelligence abroad would determine whether the capacity would ultimately be eliminated, expanded or left as an occasional option.

The Canadian intelligence community is divided on whether permitting CSIS to collect non-security intelligence would add a necessary capability. In the context of a general review of Canada's developing needs, the question of additional HUMINT capacity should be explicitly examined. A review could recommend necessary restrictions, such as those that currently exist in section 16 (personal request in writing of the minister of global affairs or national defence, and the personal assent in writing of the minister responsible for CSIS). This report recommends that CSIS have a limited ability to collect foreign intelligence abroad.

OSINT

Open-source information is transforming the nature of intelligence. Until relatively recently, intelligence collection concentrated on secrets. That is no longer the case. In today's information age, accessible data can be used to provide policy makers with a decision advantage — the purpose of intelligence.

OSINT collection has evolved rapidly. Increasingly useful volumes of OSINT are available, but capturing it is now a highly skilled specialty. Bellingcat, a publicly funded open-source research organization, has demonstrated the value of open sources by identifying those responsible for assassination operations in allied countries. The organization uncovered exact details on how Malaysian Airlines flight MH17 was shot down by a Russian missile over Ukraine on July 17, 2014. It has exposed the use of banned munitions and identified the sources of poison gas shelling in Syria. Researchers for intelligence communities are using OSINT to obtain similarly critical information.

The use of OSINT will grow with the continued availability of social media feeds, ubiquitous data-collection sensors, advanced data-analysis capacities and the commercial availability of sophisticated technology, such as satellite radar and high-resolution photo imagery. OSINT will be utilized by independent research and investigation units outside the secrecy walls of government.

Open-source intelligence, like other collection disciplines, must also work around countermeasures. Social media companies are restricting and deleting data in response to privacy concerns. Militaries are banning social media posts useful to hostile forces and public media. Authoritarian regimes are hostile to posts that could be used by open-source analysts to gauge popular discontent. Some of the data being deleted because of violent, hateful or disturbing content is needed by open-source analysts to build files on violent extremist organizations. Losses in data accessibility are offset by new tools and sources, some of which are not shared publicly. OSINT organizations can sometimes purchase "grey" data — information possessed by third parties.

Private sector OSINT capacity is extensive, and potentially accessible to the intelligence community.

National intelligence communities are developing their OSINT capacities in different parts of their communities. The United States has an assistant deputy director of national intelligence for open source. Canada should take steps to ensure that OSINT capacity serves the whole community. Our allies have facilitated access to OSINT by making it available on a common community platform and ensuring that a senior official promotes the accessibility across the community of OSINT. It is recommended that there be a common OSINT platform for the Canadian community, coordinated by a senior official.

Scientific and Technical Intelligence

Scientific and technical intelligence has long been a focus of defence intelligence. However, technical and scientific innovations increasingly have implications for other aspects of national security. This is particularly evident with information technology, which has completely changed the potential for the capture of critical databases by foreign entities. It has extended the threats to national economies and critical infrastructure, and exposed companies and individuals to ransomware. Technical innovations allow criminal organizations to protect their communications, buy and sell on the dark web, and create new addictive drugs. Drones have revolutionized warfare but have also given new opportunities to terrorists and criminals. Domestic extremists, criminals and terrorists have access to disruptive technology.

Scientific and technological advances have changed intelligence itself, dramatically altering the potential for HUMINT operations, and the potential of open-source collection.

Technical and scientific capacities are central to understanding climate change, and health science is at the centre of pandemic-warning intelligence.

The challenge is to make sure that the intelligence community can assess the impact of the scientific and technical intelligence held by other parts of the communities and the private sector on core issues — terrorism, domestic security, criminal activity and the fundamentals of intelligence collection and counter-espionage. This is another area in which a more robust degree of community integration would help protect Canadian security.

Diplomatic Reporting

Although not part of covert intelligence collection, Canadian diplomatic reporting provides a detailed perspective on foreign countries through Canadian missions abroad. Reports are sometimes shared with allies. Because diplomats were responsible for many non-reporting functions, diplomatic reporting became, by default, a lower priority for Global Affairs Canada. The establishment of the Global Security Reporting Program (GSRP) re-established diplomatic reporting as a priority activity for designated countries. The presence of GSRP officials in countries of security and intelligence interest may have a potential for providing information on pandemic indicators or provide evidence of security-related impacts of climate change. Normal diplomatic reporting also has a high potential to produce information on these priorities as diplomats have a daily opportunity to observe the countries in which they live. Global Affairs Canada recently set up its own assessment unit to provide intelligence analysis prepared to meet the specific needs of the department.

Intelligence Assessment

Intelligence assessments combine information from all available sources to succinctly summarize what can be known about a subject of interest. Analysis synthesizes diverse sources, provides context and insight, and examines possible outcomes. It directly serves senior decision makers, sometimes with conclusions bearing on a pending decision, sometimes as background. Assessment is an important output of the intelligence cycle and its most visible component for many intelligence users.

Analysts and their clients alike can access numerous sources of information. The large flow from technical intelligence, allies and the increasing flow from ubiquitous data points and open sources have led to two plausible speculations on the future of analysis. One is that decision makers have a complete array of information sources available to them and do not need intelligence analysis. The other is that it will take expert information analysis to dissect the voluminous available information, real and fake, and produce succinct, usable conclusions.

As the information base for any discipline expands, those who can use information need the right combination of expert analysis and integrating generalists to make the best use of it. While it is true that decision makers and their advisers have access to a very wide array of information resources, there will be more rather than less need for expert analysis to focus on what is crucial.

It is a common observation about intelligence systems, the Canadian one, in particular, that the large amounts of money spent on collection are not always matched by the necessary intelligence analysis to make sense of it.

No matter how the assessment capacity is structured, there is still the danger that intelligence assessment will not be used by decision makers. Assessment must add value and be seen as adding value.

Intelligence analysts also have the crucial role of warning of the emergence of a dangerous mutation in the security environment. This requires timely intelligence and experience in analyzing an important target.

Intelligence assessment is always policy neutral. Departmental policy analysts may cite it in their analysis of options, giving decision makers a synthesis of options and reasoning, without undermining the neutrality of intelligence analysis.

As part of a general review of Canada's intelligence capacity, it is recommended that there be a review of whether we have the necessary analytical capacity. This should include a review of the overall size of the analytical cadre, the match with the needs of decision makers, and whether the perspective of analysis is factored into community priority setting.

The Diversity Advantage

The Canadian government promotes diversity in its workforce for reasons of fairness, equity, representativeness and range of viewpoints. All of these considerations apply with emphasis to the intelligence sector. Agency employees must track the potential for global and domestic group conflict, understand different cultures and religions, handle input from dozens of languages, see problems from different perspectives and avoid the dangers of an unrepresentative consensus on the nature of threats.

Canada's intelligence community leaders recognize the compelling reasons for diversity. Interpreting a complex international security environment requires a workforce with multiple skills and perspectives. The active programs to enhance diversity in the community are vital to mission success.

Linkages

Outside Experts

It is common in other Five Eyes intelligence systems for security and intelligence experts from outside government to contribute to the work of the community. Canada does this to a much more limited degree. Both the United Kingdom and the United States have access to large pools of intelligence-relevant expertise in universities and other centres of expertise. The US system of partisan appointments to the public service means that experts often alternate between government and universities or the private sector.

Outside experts are useful because many have intensively studied an area of interest to the intelligence community. They maintain broad networks of professional contacts, and bring different perspectives to assessment, policy and possible future developments.

Intelligence communities have several alternatives for using outside expertise in addition to hiring the experts full time. Academics or others can be brought into intelligence organizations on temporary secondment. They can be consulted when their expertise is need for an analytical paper. Academics and other outside experts are regularly invited by CSIS's Academic Outreach staff to make presentations to the intelligence and policy community. As the Canadian community increases its mining of open sources, outside expertise becomes more relevant and more accessible. Open-source organizations within government can provide a useful linkage for mobilizing external expertise to illuminate security issues.

If outside experts are invited for consultations or to make presentations, security clearances will usually not be necessary. For more intensive discussions pooling inside and outside perspectives, they sometimes will be.

Outside expertise is also useful on advisory councils, but such councils must add

real value for everyone or enthusiasm for their existence diminishes quickly.

One of the functions that could benefit from the right mixture of community and outside expertise is strategic foresight. Strategic foresight is always identified as an important community need, but discussions on long-term probabilities are frequently displaced by urgent priorities. As the pandemic has shown, disruptive events are foreseen by some people some of the time. If disruptive events are at least on the radar, it is possible to assess if the danger is increasing.

A Joint Strategic Warning Committee would be a useful experiment in combining community and outside expertise. Its analysis of potential short- and longer-term threats and opportunities would give senior political and agency discussions on strategic assessment realistic and detailed possibilities to consider. The first step in dealing with disruptive events is to predict their potential occurrence.

These discussions would be useful in building the overall threat picture, which could later be integrated into the drafting of public annual or biannual statements on strategic priorities.

The establishment of a Joint Strategic Warning Committee is included in the list of recommendations.

Briefing MPs and the Public

The National Security Act,[3] given royal assent in 2019, and the National Security and Intelligence Committee of Parliamentarians (NSICOP) Act of 2017[4] established strong accountability structures for Canada's security and intelligence community. With parliamentarians able to review in detail the activities of the relevant agencies, and report publicly, there is a greater chance that interested parliamentarians, and Canadians in general, can be better informed on the preoccupations of the security and intelligence community.

There is still a need for more briefings for MPs not involved in NSICOP but who need to make informed comments on issues of security, foreign policy and defence. Many interact regularly with constituents representing different interests, speak with representatives of foreign embassies in Ottawa and visit foreign countries on official business. Few have a functional knowledge of what the intelligence community does and why. Many interact with people and organizations they should know more about.

The public also needs more information, through regular annual reports by agencies in the intelligence community, and by a regular and comprehensive government overview of the security environment. Similar reports are regularly published by our Five Eyes allies, and other nations, and increasingly include references to the security implications of global warming and the continued threat from pandemics. Such reports inform the public, set out security priorities in general terms and generate useful debate around important areas of public policy.

The community should continue to find ways to set out the connections between intelligence and peace, order, good government and prosperity, as a means of informing the public and fostering an "intelligence culture" — a balanced appreciation of intelligence as a tool of government.

Intelligence agencies do brief MPs through committee hearings, NSICOP and as support for MP visits abroad. Making on-request unclassified briefings available to MPs would be an important step, ensuring that debates on national security issues are well informed.

The production of a regular security update, and the ability of agencies to brief MPs as appropriate, are recommended.

Canada and Alliances

The Five Eyes Alliance

Today's new globalized environment is causing governments to rethink fundamental aspects of national security. A cornerstone of Western national security since the middle of the twentieth century has been the Five Eyes alliance. The alliance was initially formed to share SIGINT among Australia, Canada, New Zealand, the United Kingdom and the United States. Sharing now extends across all intelligence disciplines. As the threat environment changes, should the membership remain as it is, or should the alliance be expanded?

There are plausible partners if the Five Eyes were to be expanded, but the alliance draws its

3 See https://laws-lois.justice.gc.ca/eng/acts/N-16.56/index.html.

4 See https://laws.justice.gc.ca/eng/acts/N-16.6/index.html.

strength from the historic association between the five member countries. Common values and a successful partnership over a span of more than 70 years have built many strong bonds among the existing allies. The ability to share intelligence and consultations in a common language facilitates exchanges and minimizes delays and misunderstandings. (Canadian agencies work internally in both official languages but share material in English with Five Eyes partners.) The alliance is vital to Canada's national security and Canada is committed to making a significant contribution.

Each of the countries in the Five Eyes has numerous bilateral and multilateral relationships with other countries, and some of those relationships are close. Most of the advantages that would be gained by an expanded Five Eyes can already be achieved by other relationships and alliances, without disruptions to the Five Eyes itself.

The Range of Bilateral Relationships

Canada has bilateral sharing arrangements with many countries with which it shares common objectives. These arrangements are a necessary addition to the Five Eyes alliance, as they provide additional coverage and different perspectives to that of our primary allies. Sharing partners range from countries that are comfortable historic partners for Canada, to more difficult ones where contacts are closely regulated by legal boundaries and by practitioners themselves.

North Atlantic Treaty Organization

Canada also benefits from intelligence sharing via the North Atlantic Treaty Organization (NATO), but much of the highly classified intelligence is supplied by the two Five Eyes partners — the United Kingdom and the United States. Canada benefits from the wide variety of perspectives within NATO.

Canada and the United States

The United States is the largest provider of intelligence in the Five Eyes alliance. This capacity has been of great value to the Five Eyes partners, including Canada.

Although the Five Eyes partners share common values, this does not mean that their policies are identical. Despite divergences of opinion on foreign policy, the underlying intelligence-sharing alliance has persisted, with only occasional disruptions because of policy differences.

As US politics become more fractious, it is possible that the separation of alliance processes from sometimes diverse policy agendas will be more difficult to maintain. This would be particularly challenging for the Five Eyes alliance if the leadership of the US community were less frequently in the hands of professionals determined to keep national political agendas separate from the sharing of intelligence. Relationships would be complicated further if politics influenced intelligence collection and assessment. Allies would have less confidence that the material shared with them by the United States was free of politicization.

It would not be the first time US intelligence was seen in Canada as reflecting a US worldview. Nor would it be the first time intelligence had been politicized. It would mark the first time the politicization of intelligence was an endemic rather than an exceptional factor.

Canadian liaison officials in Washington are well placed to track important changes within the US intelligence community. Any decrease in the value of intelligence shared by the United States would be a very serious issue for Canada, as there would be no affordable way of replacing the volume and value of what we now receive. In addition to monitoring the evolution of the US community, Canadian officials should develop a contingency plan in case the sharing arrangements with the United States are less reliable in the future.

Community Integration

Characteristics of an Integrated Community

Intelligence communities are composed of different agencies specializing in different kinds of intelligence and different tasks. In addition to core members of the community, there are many other government entities that are clients for the community's intelligence and analysis. Some have mandates that require a capacity to receive intelligence. Others generate a specialized type of intelligence or have important security functions related to their own mandates. Achieving the necessary degree of integration and coordination across diverse communities is a constant challenge for every country, complicated by the size of the overall security and intelligence component in government, and the national political structure.

Well-integrated communities have an effective central decision-making capacity, the ability to mobilize community capacity to serve cross-government needs, specialized committees for core community coordinating tasks, and an active warning capacity that anticipates and detects developing threats.

Integration Options for Canada: A Canadian National Security Council?

National intelligence systems evolve over time, usually in the direction of greater effectiveness in coordinating collection capacities and serving the needs of senior policy officials. The development of Canadian intelligence machinery has been in the same direction, but we are at an earlier stage of development than the United States, the United Kingdom and Australia.

Many countries have established a national security council at the apex of their security and intelligence system. NSC structures vary, but their common purposes are to achieve unity of direction and tasking within the security and intelligence community, and to promote a greater coherence of foreign, defence and security policy.

NSC mandates may include all or some of the following:

- Integrate security and intelligence collection and operations with foreign, defence and national security policy to implement system priorities, share information and resources, and build a consensus on threats and opportunities.
- Ensure that community priorities reflect both strategic and tactical needs, immediate and longer term.
- Implement measures to improve the effectiveness of intelligence and security activities, anticipate the operational implications of technological change, and use financial and human resources to the best advantage.
- Ensure the alignment of security and intelligence activities with government priorities.
- Enforce community standards for internal security and counter-espionage.
- Contribute to the government and public consensus on the threats and opportunities facing the nation.

Some allied structures are focused on the coherence of the intelligence community. Others exist primarily to support senior-level discussions of foreign, defence and security policy. Some do both.

There is no model that can be adapted directly to the Canadian context as we have our own priorities, history and government structures. If (as is recommended below) the Government of Canada decides that we should move to a more integrated system, we will need to weigh which general models best suit our needs, and which specific features should be adapted or developed. As we have found with the position of NSIA, and as our allies have found with their own structures, the important initial step is to choose an institutional direction, and then adjust the model over time.

Potential Models

NSC Models

US NSC

The US NSC is part of the White House structure and as such is staffed by partisan appointees. Its leader is frequently a well-known expert on international issues (for example, Brent Scowcroft and Henry Kissinger). There is a large secretariat. Formal NSC meetings are chaired by the president and other meetings are of principals — cabinet ministers and senior officials from foreign policy, defence and security-related agencies. In the US system, all of these are appointees of the president. Many, but not all, of the agency heads will be partisan appointees.

This structure is congruent with the US system of separation of powers, the US international role and the long-standing practice of staffing the senior levels of the public service with partisan nominees. While some ideas on central direction could be borrowed for Canadian purposes, the specific structure is not compatible with the Canadian system of parliamentary government, and the tradition of career public servants with a low public profile.

Nevertheless, the US NSC has provided a strong support structure for the presidential role in national security, defence and foreign policy, with

the Principals Committee providing a senior forum for thorough and blunt discussions chaired by the national security advisor rather than the president.

UK NSC

The United Kingdom established its NSC in 2010 as a further refinement of the security structure developed over many decades. It is a committee of cabinet, normally chaired by the prime minister, and with senior officials from the relevant departments and agencies frequently in attendance. It is separate from the Joint Intelligence Committee to preserve the distinction between policy and intelligence assessment. It is supported by a secretariat. The NSC is also supported by the Civil Contingencies Committee, more commonly known as COBR (COBR stands for Cabinet Office Briefing Room), which manages national emergencies.

A 2014 evaluation of the NSC by the UK Institute for Government found that the NSC had generally been successful in promoting integration, with some important qualifications (Devanny and Harris 2014). Its influence is directly tied to the attention given to it by the prime minister. It is seen as overstressing foreign affairs, and the secretariat was judged to be underpowered given the expansive range of the NSC. Shorter-term discussions routinely supplanted longer-term strategic ones.

The UK government continues to review and adjust the structure of the NSC.

There are elements of the design that make it similar to Canadian cabinet committees, which have had a similar mandate. In the UK case, a strong effort has been made to establish it as a permanent committee so that it can build a consensus around UK strategies and priorities. It periodically issues a public national security statement.

US Office of the Director of National Intelligence

Originally, the director of the Central Intelligence Agency was the statutory leader of the US intelligence community, but it was difficult for an agency head to play this role within the diverse US community. September 11 and a series of misjudgments on Iraq led to the creation of a central authority over the entire community — the director of national intelligence (DNI), which is a cabinet position in the US government.

The Office of the Director of National Intelligence (ODNI) is an independent agency supporting the DNI, with a mandate to integrate intelligence across the community. The DNI has usually been a respected community professional. The secretariat is responsible for the production of the President's Daily Brief, formerly a product of the CIA.

As with the US NSC, there may be elements that Canada can borrow from the ODNI model, but it too is aligned with the US Constitution and political conventions. It is resourced at a level that is well beyond Canadian capacities or needs.

Australian Office of National Intelligence

The Australian Office of National Assessments (ONA) was established in 1977 to provide independent assessments and oversight of the intelligence community, reporting to the prime minister. A review in 2017 led to substantial changes in the Australian community. The Office of National Intelligence Act (2018)[5] expanded the ONA to become the Office of National Intelligence (ONI) — a statutory body. The act increased the number of agencies constituting the intelligence community from six to 10. A deputy director-general for intelligence enterprise management was established, and this role is carried out with the support of Mission Intelligence Groups (MIGs), each headed by an experienced intelligence officer.

Unlike the NSC models, but more like the ODNI, the ONI is focused directly on the effectiveness of the intelligence community and not on the integration of the foreign defence and security policy.

According to Australian academic and former practitioner Patrick F. Walsh (2020), the ONI model is a very significant reform step and has "made progress on formal intelligence coordination and priority setting process through the MIGs" but has not yet fully met all the expectations of it for coordination and leadership of the community. There is also a National Security Committee of Cabinet, chaired by the prime minister.

5 See http://classic.austlii.edu.au/au/legis/cth/num_act/oonia2018259/.

Advantages and Disadvantages of the Models for Canada

The UK NSC is the model closest to Canadian cabinet government precedents. A demonstrated weakness of the model, both in the United Kingdom and Canada, is that it explicitly depends on a high degree of participation by the prime minister. A diminished interest by the prime minister for any reason could lead directly to a decline in its prominence within the government structure and, therefore, its effectiveness as a strategic integrator. Other models are more resilient as focal points for integration, despite inevitable variations in the degree to which the prime minister can participate as chair.

The Australian ONI model is also aligned with a parliamentary system. However, because it is focused on improving assessments and specific community accountabilities, it is less dependent for mandate effectiveness on overt prime ministerial attention. The separation between intelligence input and policy development is greater than in the NSC model. A drawback is that the intense focus on community effectiveness comes with a corresponding need for sufficient expert secretariat resources to meet its extensive responsibilities. Both the ONI and the National Security Committee of Cabinet perform an integration role, but they are separate entities.

The US NSC has the mandate and resources to support presidential leadership on security, defence and foreign policy. While it operates in a much different constitutional context, it is able, within the bounds of a presidential term, to promote strategic coherence and thoroughly debate options for the president and with the president. During the Trump presidency, there was a frequent turnover of national security advisors. Historically, term lengths have varied from one or two years to the length of a presidential term.

A Canadian Structure

It would be overly ambitious for an external review to be precise about all the details of the model that the Canadian government should pursue. The model must reflect an internal government view on several key questions:

- Is there a need for a greater degree of integration of intelligence capacity with foreign policy, defence and security policy?
- Is there an advantage in having a central coordinating body, which will have an established structure, mandate and membership over a longer period than has been typical for cabinet committees with an intelligence mandate?
- Should the key elements of the model be set out in legislation?
- Should a priority be the ability of a central community authority to pursue in depth the effectiveness of community “enterprise” lines as a means of implementing intelligence priorities?
- To what extent should the effectiveness of the community authority be dependent on the continuous, visible involvement of the prime minister?
- What is the most effective way of combining the perspectives of cabinet ministers and the public service leaders of key departments and agencies?
- Can the government resource a secretariat of the size and expertise needed to support the favoured model?
- Should the body established be responsible for regularly issuing a public document on security threats and priorities?

Without hazarding excessively detailed recommendations, if Canada is to take a step toward greater integration, which this report suggests is required, the central elements would be:

- A National Security Committee of Cabinet, with the prime minister as chair, membership of senior cabinet ministers and the frequent presence of senior intelligence community officials. The NSC would benefit from being recognized as a permanent component of the cabinet structure, with a permanent core mandate. It should be developed and enhanced over time, but not regularly disassembled and reconstructed as has frequently happened. The UK NSC would be one model to study, but not the only one.

- Enhanced authority for the NSIA by making the position statutory. It would also be useful to review the mandate of the NSIA to see whether the various coordination, intelligence briefing and policy recommendation roles are compatible with each other.
- An NSIA who would be appointed with the assumption or provision of a term of approximately five years, to match the length of term seen as necessary for agency heads in the community. There is an advantage to appointing a senior official who is near the end of their career, but this advantage is lost if turnover in the position is too frequent for the NSIA to effectively pursue a complex set of priorities.
- Although the chairmanship of an NSC by the prime minister would give intelligence and security issues the focus they need in the cabinet system, the other preoccupations of the prime minister suggest that a strong deputy chair (deputy prime minister, minister of public safety) would be a plus and increase the possibility that the committee could adhere to a regular meeting schedule. While the frequent presence of the prime minister is an important signal on the importance of national security files, the NSC or an officials' subgroup would, at times, benefit from the ability to debate issues extensively without the presence of the prime minister.
- A primary role for the NSC should be the anticipation of crises that could potentially preoccupy the prime minister and Cabinet. If this difficult role were performed well, it would justify the investment of prime ministerial time, as well as being invaluable to the intelligence community itself. Input from the proposed Joint Strategic Warning Committee would be a valuable source for this function.
- The overall central structure would benefit from the senior-level expertise that characterizes the US NSC, and the ability to manage intelligence "missions" as carried out by the Australian ONI.

Legal Issues

The statutes respecting national security were extensively revised with the passage of the National Security Act, 2017. The objective was principally to balance the proposals of the previous government to expand some intelligence agency powers with a corresponding expansion of the review and accountability system.

Since the original passage of the CSIS Act in 1984 and its subsequent five-year review, the security environment has been transformed by information technology, private encryption keys, data analytics, cyber intrusions, terrorism, cyber-enabled criminal organizations, and numerous other innovations and developments. Crime is more international, terrorism has taken many new shapes and foreign powers can interfere directly in the integrity of Canadian democracy and public health institutions.

As recommended above, the CSIS authorization to collect foreign intelligence should be reviewed. This is a potentially important amendment, but it is not the only aspect of the CSIS Act that needs to be reviewed. It is time for a comprehensive review of the act.

A Comprehensive Review of the Canadian Intelligence Community

An outside review, such as this one, can argue for changes that would improve the intelligence system, but for government itself an outside review is not definitive. The recommendations may be bold, and they may set out exactly what is needed, but they lack the inside knowledge of capabilities and needs that an internally mandated and supported review can provide.

Other communities have used regular comprehensive reviews, whether by recognized experts with a background in the community, or by a legislative oversight body, to implement needed reforms. NSICOP has the potential to make suggestions to improve the Canadian intelligence system, but the committee and its members are not yet at the level of knowledge and expertise that would enable them to conduct an urgent and in-depth review of an entire system. A stronger NSIA might, in future, propose major reforms. At this time, the best option for a deep and broad review of the intelligence and security community is one established and facilitated by the government itself.

There are many cost pressures on the Government of Canada. In any review, the community will need to make submissions that are affordable in a constrained environment. The recommendations in this report are directed primarily at a greater degree of integration, efficiency and effectiveness. Resource decisions are never easy, and they are particularly difficult if the ultimate good to be achieved can only be judged retrospectively, as it sometimes is for intelligence and security reforms. However, more than in the past, Canada's economic health is directly linked to our ability to understand threats to governments, private companies and citizens.

A review could encompass consideration of all of the recommendations in this report, or proceed with some of them through separate processes.

Recommendations

CSIS and Foreign Intelligence

→ As part of a comprehensive review of Canada's intelligence community, the government should review Canada's need for non-security-related foreign intelligence and consider whether to permit CSIS to collect foreign intelligence outside Canada. Such a capacity could be limited, and subject to restrictions that currently apply to domestic collection of foreign intelligence.

OSINT

→ The Government of Canada should continue to develop its OSINT capacity and ensure that there is a common OSINT platform across the intelligence community. A designated senior official responsible for maximizing the contribution of OSINT to the overall intelligence collection enterprise should be appointed to achieve this objective.

Intelligence Assessment

→ The government should review Canada's assessment capacity to determine whether it meets the needs of decision makers.

Outside Experts

→ The government of Canada should make greater use of experts outside government by promoting exchanges between government agencies and universities or private sector organizations, inviting experts to brief senior officials, or regularly using outside experts to work with open-source organizations. A limited number of outside experts should receive appropriate security clearances to promote consultations with government officials.

→ A Joint Strategic Warning Committee composed of both government analysts and outside experts should be considered as a means of increasing the capacity for strategic warning within government.

Briefings for Parliamentarians

→ Canadian security and intelligence agencies should have the capacity to provide regular unclassified briefings to MPs, as necessary and appropriate.

Security Review for the Public

→ There should be a public annual or biennial report on national security, setting out the government's assessment of the national and international security environment, including general priorities. The security environment review should include conclusions on the security implications of developing non-traditional, serious security threats, such as global warming and the assessed state of the continuing danger from pandemics.

Relations with the US Intelligence Community

→ Senior leaders in the Canadian intelligence community should consider the possible implications for Canada of a more politicized US intelligence community and develop a contingency plan.

Central Coordination

→ The Government of Canada should establish a permanent National Security Committee of Cabinet, compatible with the Westminster system of parliamentary and cabinet government, drawing on the features of the different related integration

mechanisms that would enhance its potential as a community integrator.

- → The prime minister should be the chair of the NSC, with a senior intelligence community portfolio minister as deputy chair.
- → The position of NSIA should be established in legislation, and the process of preparing the legislation should include a review of the NSIA mandate.
- → Appointments to the position of NSIA should be made on the understanding, or with the provision, that the term of the appointment is five years.

Government Reviews

- → The Government of Canada should conduct a comprehensive review of the CSIS Act to ensure that the mandate and accountabilities of CSIS meet contemporary needs.

The Government of Canada should initiate a comprehensive review of the Canadian intelligence community, including consideration of the proposals in this report.

Conclusion

In his June 8, 2021, presentation, hosted by CIGI, then NSIA Vincent Rigby stated: "My bottom line is this: the world is at an inflection point. It is experiencing seismic political and economic shifts and facing a complex combination of new and enduring national security challenges. And as COVID-19 has made painfully clear, these challenges are relevant to all Canadians in their daily lives. This environment requires a new, broader definition of 'national security.' And it requires Canada to be prepared and to step up its game" (Rigby 2021).

The purpose in preparing this report is to provide ideas for a necessary national debate on how intelligence capacities, old and new, can be mobilized to protect the security of all Canadians.

Author's Note

The author would like to thank Assistant Director of the Applied History Project at Harvard Kennedy School Calder Walton for his contribution to the Rethinking the Role of Intelligence working group as co-theme lead and co-chair of the working group sessions.

The author also thanks all those who participated in the three workshops that led to this report. Significant changes and additions resulted from the detailed comments on early drafts. The author is responsible for all errors, omissions and opinions.

Works Cited

Devanny, Joe and Josh Harris. 2014. *The National Security Council: National security at the centre of government.* Institute for Government. November 4. www.instituteforgovernment.org.uk/publications/national-security-council.

Rigby, Vincent. 2021. "National Security Challenges in the 21st Century." Speech by the National Security and Intelligence Advisor to the Prime Minister to the Centre for International Governance Innovation. June 8. www.canada.ca/en/privy-council/services/national-security-intelligence-advisor-challenges.html.

Walsh, Patrick F. 2020. "Transforming the Australian intelligence community: mapping change, impact and challenges." *Intelligence and National Security* 36 (2): 243–59. www.tandfonline.com/doi/abs/10.1080/02684527.2020.1836829?journalCode=fint20.

Acknowledgements

The Reimagining a Canadian National Security Strategy project wishes to acknowledge the valuable engagement we have enjoyed with senior officials during working group discussions and the drafting of the report. The senior government liaisons who took part in discussions about the Rethinking the Role of Intelligence theme and who consent to be acknowledged are:

- Tricia Geddes, Deputy Director, Policy and Strategic Partnerships, Canadian Security Intelligence Service
- Daniel Rogers, Deputy Chief, SIGINT, Communications Security Establishment Canada

Their involvement with the project does not in any way indicate their agreement in whole or in part with the theme report and their participation does not reflect any official Government of Canada policy or position.

The project wishes to acknowledge the valuable contributions made by working group members during discussions and the drafting of the report. The working group members who took part in discussions about the Rethinking the Role of Intelligence theme and who consent to be acknowledged are:

- Martin Benjamin, Director General, Intelligence Bureau, Global Affairs Canada
- Ray Boisvert, Associate Partner, Security Strategy, IBM Security
- Mel Cappe, Distinguished Fellow, Munk School of Global Affairs and Public Policy, University of Toronto
- Marie Careau, Trainer/Facilitator, HPCI Consultants
- Erik J. Dahl, Associate Professor, Department of National Security Affairs, Naval Postgraduate School
- Carol Dumaine, Nonresident Senior Fellow, Atlantic Council
- Michael Goodman, Professor, Intelligence and International Affairs; Head of Department; Dean of Research Impact, King's College London
- Jennifer Irish, Director of Operations, Privy Council Office
- Candyce Kelshall, President, Canadian Association for Security and Intelligence Studies — Vancouver
- Genevieve Lester, De Serio Chair of Strategic Intelligence, US Army War College
- Mark M. Lowenthal, President and CEO of the Intelligence & Security Academy, LLC
- Stephen Marrin, Program Director and Associate Professor, Intelligence Analysis, James Madison University
- Dave McMahon, Chief Executive Officer, Clairvoyance Cyber Corp; Chair, Cyber Council, Canadian Association of Defence and Security Industries
- Rob Mendoza, Senior Advisor, Canadian Defence Academy, Dallaire Centre of Excellence for Peace and Security, Department of National Defence, Government of Canada
- Bill Robinson, Research Fellow, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto
- Jason Shepherd, Director, Analysis and Innovation, Thomson Reuters Special Services International
- Jean-Louis Tiernan, Minister-Counsellor, Embassy of Canada, Global Affairs Canada
- Patrick F. Walsh, Associate Professor, Australian Graduate School of Policing and Security, Charles Sturt University
- Alex Wilner, Associate Professor of International Affairs, Norman Paterson School of International Affairs, Carleton University

Their involvement with the project does not in any way indicate their agreement in whole or in part with the theme report.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org