Centre for International
Governance Innovation

CIGI Special Report

Reimagining a Canadian National Security Strategy

Aaron Shull and Wesley Wark

CIGI Special Report

Reimagining a Canadian National Security Strategy

Aaron Shull and Wesley Wark

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
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Sami Chouhdary

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publication enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

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 Authors

As CIGI's managing director and general counsel, Aaron Shull acts as a strategic liaison between CIGI's research initiatives and other departments while managing CIGI's legal affairs and advising senior management on a range of legal, operational and policy matters. A member of CIGI's executive team, Aaron provides guidance and advice on matters of strategic and operational importance, while working closely with partners and other institutions to further CIGI's mission. He also serves as corporate secretary. Aaron is an expert on cybersecurity issues. He coordinated the CIGI essay series Governing Cyberspace during a Crisis in Trust. In his introduction, he argues that more robust international norms for cybersecurity are a national imperative for Canada. Prior to joining CIGI, Aaron practised law for a number of organizations, focusing on international, regulatory and environmental law.

Wesley Wark is a CIGI senior fellow and an adjunct professor at the University of Ottawa's Centre on Public Management and Policy, where he teaches professional courses on security and intelligence topics. He recently retired from the University of Toronto's Munk School of Global Affairs and Public Policy, where he had taught since 1988. He served two terms on the prime minister of Canada's Advisory Council on National Security (2005–2009) and on the Advisory Committee to the President of the Canada Border Services Agency from 2006 to 2010. More recently, he provided advice to the minister of public safety on national security legislation and policy. He has appeared on numerous occasions before parliamentary committees and comments regularly for the media on national security issues.

Executive Summary

Political leaders routinely acknowledge that national security is a core responsibility of government. In Canada, that responsibility is too frequently exercised behind the scenes, far from public attention and understanding. National security policy operates today without any strategic framework or forward-thinking capacity. It can be easily captured by legacy thinking, prone to fighting yesterday's battles or resting on outdated views. It operates from an inadequate institutional and decision-making foundation. To borrow from the evolutionary sciences, it functions according to its own "punctuated equilibrium,"[1] where change is usually slow and incremental and is only stimulated to a greater pace by a crisis.

A moment of faster change is upon us. It is a product of our current health-security emergency but is embedded in a wider phenomenon of major alterations to the threat environment that Canada faces. As this report is being written, coronavirus disease 2019 (COVID-19) has taken more than five million lives across the planet (and that is, no doubt, an underestimate). But behind the breaking wave of COVID-19 looms an expansive set of unprecedented challenges. Canada's traditional approaches to national security — even our inclination to complacency and innocence, and an assumption that we can be rescued from security dangers by others — will not suffice. Worse still, these new challenges are only being recognized as national security threats very late in the day.

This CIGI special report is a *cri de cœur* arguing for a new approach to national security strategy and honest, transparent engagement with the reality of the threats we face as a country. It outlines the key threats that we now confront: a vastly altered geopolitical environment with the rising power of China at its core, ongoing and future pandemic threats, climate change security impacts, uncontrolled technological change and the undermining of economic security. Meeting these threats requires a sovereign, made-in-Canada response that protects Canada's democracy and national interest and that operates within an environment of informed public understanding.

To call attention to rising national security threats and the current deficiencies of the Canadian strategic outlook is not a counsel of despair or based in fearmongering. But it is a call for action — action to change thinking, to engage with Canadians, to improve the nature of policy making and to better understand not only the threats that might be generated within our borders, but also the larger dangers that confront us. Canada must pivot to face looming global threats and can and must do so from a position of knowledge and strength.

This special report is the culmination of a project unprecedented in scale and scope in Canada. Beginning in the fall of 2020, CIGI set out to mobilize a large and diverse set of Canadian and international experts to examine Canada's national security landscape. The CIGI project, Reimagining a Canadian National Security Strategy, will feature the publication of this capstone report, authored by the project's co-directors, alongside 10 thematic reports allowing for deeper dives into critical, present-day national security issues. The project has been greatly enhanced by the willingness of senior government officials in the national security world to assist us with their knowledge and expertise, while recognizing the integrity and independence of the project's work.

We hope that this capstone report and the 10 thematic reports produced by the project will stimulate new thinking and action on national security. This work is urgently needed and a window of opportunity for change is at hand.

This report makes a series of key policy recommendations to assist the Government of Canada in addressing the challenges of a new security environment. They are set out in four categories: strategic review, decision making and governance; legislative amendments; transparency and public reporting; and engagement and capacity building.

[1] The concept of punctuated equilibrium was championed by Stephen Jay Gould in *The Structure of Evolutionary Theory* and *Punctuated Equilibrium*.

Scale and Scope of the Project

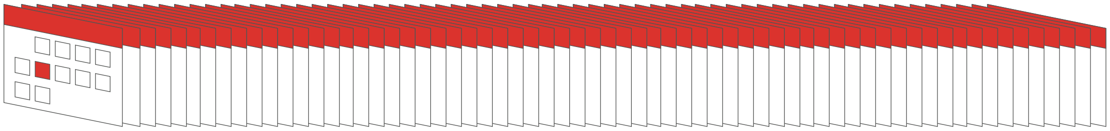
Project Advisers 4

Senior Government Liaisons 21

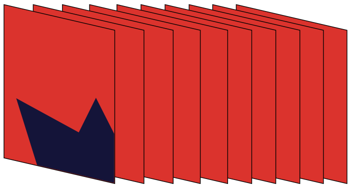
Working Group Theme Leads 17

Experts 250

Working Group Meetings 65



Reports 10



Special Report 1

Key Recommendations

Strategic Review, Decision Making and Governance

→ The Government of Canada must develop and publish a national security strategy describing the current and anticipated threat environment, the objectives of national security policy, the role of national security in advancing Canada's national interest and the key capabilities needed to meet the threat environment. The national security strategy should be an inclusive and integrated statement, linking national security to Canada's defence, foreign affairs, economic, data governance and international development strategies. A published national security strategy will be a key piece of guidance demonstrating Canada's resolve to respond to the challenges of a new age of national security.

→ To ensure leadership and informed political decision making, a cabinet committee on national security should be established. The committee would be chaired by the prime minister with a deputy chair on a rotating basis selected from the ministers of Public Safety, the Department of National Defence (DND) and Global Affairs Canada. Such a committee, devoted specifically to priority national security issues, would complement the current Incident Response Group (IRG), modelled on the UK Civil Contingencies Committee, more commonly known as COBR (COBR stands for Cabinet Office Briefing Room), which was established to deal with emergencies of all kinds. The IRG includes cabinet ministers and senior officials, and "will convene in the event of a national crisis or during incidents elsewhere that have major implications for Canada" (Office of the Prime Minister 2018). The IRG responds in an ad hoc fashion to a "crisis" or "incidents" as they arise. A cabinet committee on national security would have a more focused mandate and a forward-looking capacity to consider strategic and longer-term responses to threats. This was the rationale behind the Cabinet Committee on Intelligence and Security that operated during the Cold War but was subsequently set aside.

→ The government should undertake a comprehensive internal review of its national security capabilities in relation to the new threat landscape. This review would be separate from the broad integrated strategy but complementary to it. The review would set out options for changes to the governance of national security, emphasizing enhanced leadership, stronger centralization and coordination of effort, and better use of intelligence reports in decision making. One option to be explored is the creation of a Canadian-style National Security Council (NSC) to better integrate and inform senior decision making. The adoption of an NSC system would require changes to the cabinet committee structure. An alternative to an NSC construct, at the senior bureaucratic level, would be the strengthening of the current system of deputy minister tables, to ensure the effectiveness, in particular, of the deputy minister committee on intelligence and the deputy minister committee on national security.

→ All governance options should be on the table for what would be the first review of its kind on national security capabilities since the Cold War.

Legislative Amendments

→ The role of the national security and intelligence advisor (NSIA) to the prime minister should be established in legislation, including requirements for the preparation of reports to Parliament and the internal advice, reporting and coordinating functions of the NSIA. The capacity of the NSIA's office, including the Intelligence Assessment Secretariat function for strategic reporting, should be reviewed and enhanced. Special attention should be paid to upgrading assessment capabilities geared to the new threat environment, including for geopolitical developments, climate change, pandemic threats, technological change and economic security.

→ In preparation for the mandated parliamentary review of the national security legislation in Bill C-59, scheduled to commence in 2024, the Department of Public Safety, with the support of the Department of Justice, should lead a comprehensive gap review of Canada's national security legislation and should consider the viability of generating a consolidated national security act to bring disparate pieces of legislation into one comprehensive framework. Special attention should be paid to updating the Canadian Security Intelligence Service (CSIS) Act, including removing the artificial distinction between security and foreign intelligence and empowering CSIS with a regime to provide security advice as necessary to entities outside the federal government, especially as they relate to foreign interference and economic security. The review should also consider the nature of open-source intelligence (OSINT) and its lawful uses, including the compilation of data banks by the security and intelligence community, with privacy protections in mind. Updating the 37-year-old CSIS Act should be conducted to ensure that its authorities are in line with technological changes in the world of intelligence collection.

→ The government should revisit the legislation that established the National Security and Intelligence Committee of Parliamentarians (NSICOP) to ensure independence for its investigations and reporting. Changes to legislation should include a requirement for the government to respond in writing to NSICOP recommendations. The groundwork for changes to the legislation should be laid in preparation for the mandatory parliamentary review of the NSICOP legislation, slated to begin after June 2022.

Transparency and Public Reporting

→ The prime minister should present to Parliament an annual statement on the worldwide threats that Canada and Canadians face. COVID-19 has proven that threats can materialize suddenly, with profound impacts on the lives and livelihoods of all Canadians. The annual worldwide threat assessment would be coordinated by the NSIA on behalf of the Canadian security and intelligence community.

→ The prime minister, supported by the NSIA, should provide an annual statement on Canada's intelligence priorities, as decided by Cabinet, to Parliament.

→ The minister for public safety should produce an annual report on delivery of the government's national security transparency commitment and should introduce legislation to enshrine the principles of the national security transparency commitment in law.

Engagement and Capacity Building

→ National security agencies should reflect our societal makeup, histories and identities; perform in accordance with societal norms; and be representative of the broader talent base of society. There is, at present, a gap between promise and delivery in that regard. The NSIA should prepare an annual public report on diversity and inclusion targets and results for the national security system.

→ The Government of Canada must undertake a review of the implications of technological change for Canada's national security, to identify key threats and opportunities and to consider how best to ensure that future leaders in government are equipped with sufficient knowledge and expertise regarding technology development and application.

→ In order to enhance the ability of the national security system to draw on outside expertise, the government should convene a series of expert advisory councils on the following issues:

- Canada-China relations and challenges to Canadian national security;
- climate change and security;
- pandemic and biosecurity threats;
- cybersecurity and technological advances;
- economic security; and
- border security.

Each of the expert councils would have a mandate to consider both current and future developments. They should report to the prime minister through the NSIA. Permanent advisory councils of this nature will mark a significant change in the ability of the government to understand threats to national security.

Reimagining a Canadian National Security Strategy

Our Brave New World

Canada faces a new and extremely challenging national security threat environment that is unlike anything we have ever experienced before. Strengthening our readiness to understand and respond to this environment, with its many complex dimensions, must be a national priority.

Senior leaders and key institutions in the Canadian national security system are clearly alert to this altered threat environment and, importantly, willing to speak publicly about it. In an address hosted by CIGI in June 2021, NSIA Vincent Rigby was blunt in his assessment. “National security threats against Canada,” he said, “whether from state or non-state actors or from global phenomena such as pandemics and climate change — are greater than ever and directly impact our economy, our democratic institutions and our way of life” (Rigby 2021). He emphasized that “Canada’s security and intelligence community needs to evolve and adapt to this new landscape” (ibid.).

The director of CSIS, David Vigneault, has also spoken out about the new threat environment. In a rare public address, Vigneault called attention to the “one-two” punch being generated by heightened levels of foreign espionage and interference operations conducted by states such as China and Russia. He reminded the audience that even if they did not feel they had a big interest in the dynamics of geopolitics, “geopolitics is interested in you” (Vigneault 2021). He warned that “hostile state actors seek to leverage all elements of state power to advance their national interests” (ibid.) and will do so in ways that affect Canada’s national security.

National security now encompasses dangers that have a direct impact on the daily lives of Canadians. High on the list of such dangers are those emerging from the digital environment (Wark and Shull 2021). Shelly Bruce, the chief of the Communications Security Establishment (CSE), recently provided a pointed message about the cyberthreats that Canada faces: “the threat and risk surface is growing, and the slate of players looking to exploit both human and technical vulnerabilities is also growing” (Bruce 2021). Cybercrime is a pervasive threat; critical infrastructure is at risk, especially from ransomware attacks; intellectual property (IP) is being exfiltrated; and cyber capabilities have been turned into weapons by state actors to undermine democratic systems (ibid.).[2]

Never before have three key leaders of Canada’s security and intelligence system chosen to call public attention to the threats the country faces. This, too, is a sign of our times. The task at hand is to prevent our “brave new world” from becoming a dystopian one. The world is, as suggested by the NSIA, at an “inflection point” (Rigby 2021). Canada must reinvent its national security outlook and system to meet these new realities.

Our thinking on national security is outdated. Canada has not produced a national security strategy since April 2004, more than 17 years ago. The 2004 strategy was the first ever produced; it has had no successor.

Political leaders are usually quick to state that national security is a prime responsibility of the state. The hard work of thinking about and putting in place a new strategic framework — reimagining Canadian national security strategy — must now follow.

[2] See Canadian Centre for Cyber Security (2020).

Looking Back to 2004 to Look Ahead

To reimagine a Canadian national security strategy, it is useful to reflect on the circumstances and substance of the one previous effort — the April 2004 policy *Securing an Open Society: Canada's National Security Policy*,[3] written under the stewardship of the Privy Council Office and endorsed by a covering letter from the then prime minister, Paul Martin. If there was a compelling context and a set of national security concerns that generated this 2004 effort, the case is many times greater in 2021.

The 2004 policy was generated against a political backdrop and was a response to the experience of a greatly altered security environment. The Canadian government needed to find a way to signal its support for and alignment with key allies such as the United States, then at the height of its pursuit of a "global war on terror." At the same time, demonstrating an independent approach to national security, in line with Canadian interests and values, was seen as an important response to domestic critics eager to argue that Canada was simply a follower of US-led policies, whose merits they disputed.

After three years of ad hoc responses following the September 11 terrorist attacks, including new counterterrorism legislation, new and ramped up national security spending, and new approaches to border security, there was a perceived need for a comprehensive framework. National security strategies can provide organizing principles, and, in this way, the 2004 policy was intended to be a stock-taking effort following an emergency and to set out future-leaning guidance.

What is the relevance of these conditions today? Since early 2020, we have lived through — and continue to confront — a national security emergency generated by COVID-19. The security establishment has been slow to identify COVID-19 and pandemics in general as a national security threat, despite their many national security implications. COVID-19 has taken many Canadian lives, caused illness and suffering, revealed critical deficiencies in early warning and threat assessment capacity, disrupted the normal processes of government, cast doubt on the effectiveness of our federated system, introduced political divisions, impacted our economy, revealed key short-comings in supply chains on which the Canadian economy depends, facilitated greater cyberthreats and altered the global geopolitical landscape.

COVID-19 is a very different threat from that posed in the past by globally oriented terrorist groups such as al-Qaeda. It is this decade's September 11 — only worse in terms of its impact. But we must not repeat past mistakes and reorient national security strategy around a single threat. The experience of COVID-19 is one important driver for change, but only one. Reimagining Canadian national security does not rest solely on the current emergency but must also take into account a series of overlapping threats, some persistent, some new or newly recognized. They emerge out of a complex mix of state actor, non-state actor and transnational, "actorless" threats.

Among transnational threats, the impact of the current pandemic is matched, arguably even overmatched, in urgency by the rapid acceleration of climate change and its related security impacts, especially noticeable in Canada's Arctic.[4]

The White House,[5] the Pentagon[6] and the US intelligence community[7] have recently issued reports emphasizing that climate change will intensify long-standing threats to global security. These documents mark a heightened awareness by the US national security establishment of the risks posed by climate change. Together, they emphasized that the shifts untethered by climate change have the power to restructure US strategic interests and the economy, and offer new opportunities to adversaries, while also intensifying uncertainty in nuclear states. The White House report stressed that "climate change may lead to nearly three percent of the population (totaling more than 143 million people) in three regions — Sub-Saharan Africa, South Asia and Latin America — to move within their country of origin by 2050" (The White House 2021a, 4). This will be a destabilizing force, which will also

[3] See Privy Council Office (2004).

[4] See Conger and Fetzek (2021). Also see Dalby and Lawrence (2021); Dalby (2021a).

[5] See The White House (2021a).

[6] See Department of Defense (2021).

[7] See National Intelligence Council (2021).

create a corresponding obligation on wealthy nations to support climate refugees (ibid.).

While climate change vies for top billing as the greatest actorless menace facing the global community, other types of threats abound. There are rising cyberthreats; the ongoing rapid march of technological change; an international system threatened by increasing confrontation and fracture and lower levels of cooperation; and ongoing arms races. There are challenges to the legitimacy of democracies, elevated levels of foreign interference, heightened foreign espionage hunting new targets, new threats to our economic security, and uncertainty around how Canada can position itself as a middle power and operate within a fast-changing landscape of alliance structures. This is a formidable list of challenges for Canadian policy makers that cannot be understood nor met in isolation.

Canada needs to define its path forward in a vastly altered world of national security threats. Defining its path means four things:

- putting succinct meaning to the idea of national security and its objectives, so that Canadians can understand the concept;
- identifying the priority national security threats the country faces;
- defining Canada's interests and values; and
- addressing how to respond to and mitigate threats.

Toward a Definition of National Security

Defining a precise meaning of national security is not an easy task. The 2004 strategy created some verbal scaffolding, emphasizing national security as a singularly important obligation of government. It also stressed that national security involves dealing with threats that have the potential to undermine the security of the state or society, requiring a national response. The 2004 strategy also underlined the importance of aligning national security with the protection of core Canadian values and rights, and the intermingling of national and international security.

What more is needed? Without denying any of the tenets of the 2004 definition, for national security to really mean something to Canadians, it needs to be more people-centred and less insular and defensive. At the same time, not every issue falls into the basket of national security problems. For many Canadians, security evokes ideas about protecting livelihoods and ways of life. This can be elevated to the national security realm by understanding that a national security strategy has a role to play in protecting Canadians' collective economic security and in shielding them from threats posed by cyberattacks and clandestine foreign interference in our democracy. This is where Canadians can see how national security matters directly to them, rather than being an abstract concept best left to governments to deal with in relative secrecy and silence.

The idea of the codependency of national and international security also needs to be taken seriously, not just in terms of worrying about threats that come at us from beyond our borders, but actively promoting Canadian ideas of best practices and governance models for achieving international security. A Canadian national security strategy must be robustly international and pursued on more than symbolic lines. This will strike a chord with Canadians, who like to see Canada as a principled actor on the world stage, and it aligns with an international perception of Canada in some, although not all, quarters as an international good citizen and responsible partner in a rules-based international order.

How can this be tied into a definition of national security that is succinct but also resonates? The Privy Council Office has an updated definition of national security, which it provided to the NSICOP: "protecting the safety and security of Canada's territory, government, economy and people, and the promotion and protection of Canadian interests" (Privy Council Office, quoted in NSICOP 2019, 17).

This definition is overly broad. It fails to link security to any concept of threats, their severity and the danger they might pose. It leaves us with a definition that is far too inclusive to be meaningful. The language must aim for more precision. Thus, this "reimagined" wording is proposed:

> National security aims to protect Canada and its people from major threats that would undermine our democratic institutions and processes,

> our economy, our social fabric and values, and our interests.

There is no escaping the fact that national security is a portmanteau phrase, but this definition at least gives key words — protection, major threats, democracy, economy, societal cohesion, interests — that better reflect the contemporary reality. The definition is not bounded by geography (national security depends on international security); it does not argue that protecting the state is the only objective (protecting people, including our social fabric, is key); it links a concept of national security to our national interest. It emphasizes that national security is about safeguarding democracy and its legitimacy, not just about a militarized watch on borders. It equates national security with economic security. The ground truth is that economic prosperity pays for national security, and national security provides the necessary conditions for economic security.

The Reality of Threats

Laying down a national security strategy means being honest and transparent with Canadians about the realities of the threats we face. It also means staying abreast of contemporary and future trends in a threat environment that is subject to fast-paced change. The greatest weakness in national security strategy is to be a prisoner of the past — fighting the last war — and reinforcing legacy missions and expenditures of declining relevance. This is a weakness that besets current Canadian policy.

Just how much has the threat environment changed over the past two decades?

In the early 2000s, Canada was understood to face a range of threats: global terrorism after September 11, proliferation of weapons of mass destruction, failed and failing states, foreign espionage, natural disasters, critical infrastructure vulnerability, organized crime and pandemics. These were the eight main threats identified in the 2004 national security strategy. How do we need to think about threats differently in 2021 and beyond?

All of the threats listed in 2004 remain but the deck has been shuffled mightily. Global terrorism, conducted by organized groups with a primary objective to attack the so-called "far enemy" (the West), which reached its modern high point with the September 11 attacks, is not currently a top-tier threat to Canada. Concern is now more focused on regional terrorist violence in areas of the world where affiliate organizations linked to al-Qaeda and Daesh operate. Watchfulness regarding future developments in Afghanistan following the Taliban's return to power is warranted. The possibility of Afghanistan becoming, once again, a terrorist haven, must be monitored. Beyond the new emphasis on terrorism as a regional threat, an important shift has taken place in counterterrorism policy. More attention must now be placed on forms of ideologically motivated violent extremism (IMVE) manifested domestically, with Canada keeping a watchful eye on potential spillover from developments in the United States. The threat posed by IMVE in its various forms documented by CSIS appears on the rise (CSIS 2021). Societal dislocations and political polarization in response to COVID-19 may add some stimulus to far-right and other extremist groups (Roach 2021).

Concern about weapons of mass destruction has grown beyond nuclear proliferation, brought to public light in horrific ways by the use of chemical weapons in the attempted assassination in Salisbury, England, of Sergei and Yulia Skripal (Permanent Representation of France to the Conference on Disarmament 2018), and as an anti-insurgency instrument utilized by the Syrian regime against its opponents (Arms Control Association 2021). COVID-19 has amplified concerns about possible leaks from high-containment laboratories or the weaponization of biological agents (Office of the Director of National Intelligence 2021).

The drivers contributing to failed and failing states have been amplified by concerns about the impacts of climate change and the rising tide of nationalist authoritarianism, even while the idea of trying to intervene to prevent terrorist havens or restore failing states has been cast into grave doubt by the failed mission in Afghanistan and its aftermath.

Foreign espionage has increased in intensity, altered its targets to zero in on private sector information, and aided and abetted efforts to interfere in democratic practices. The new spy threats are very different from the old.

Natural disasters are thought of differently and with more urgency now, as their links to climate change impacts are appreciated. Successive recent climate emergencies in British Columbia are a clear indication of the dangers our future holds.

A diffuse concern about critical infrastructure has been brought into laser focus by the experience of cyberattacks and ransomware demands. The recent attack on health infrastructure in Newfoundland is one horrifying example (CBC News 2021a).

Organized crime has been significantly enabled by digital capacities and encryption.

The lens brought to the pandemic threat has been vastly enlarged by our experience of COVID-19 and a sickening sense that there may be worse to come. No one in 2021 or beyond will list pandemics as the last and least in a set of potential threats — as it was set out in 2004. It has rocketed to the forefront of our concerns.

The New Threats

As we look on the catalogue of previously enumerated threats with different eyes, recognizing the ways in which they are both persistent and transformed in nature, we must also appreciate that there are new threats that demand our attention and must be factored into a reimagined approach to national security.

Five new and pre-eminent threats can be identified:

→ geopolitical disruption, with a focus on China;

→ pandemics;

→ climate change;

→ technological change; and

→ economic insecurity.

One thing that was missing entirely in the 2004 strategy was any expression of Canadian concern about geopolitics, amid assumptions about the long-term stability of the international system. That assumption has since been exploded. Recent changes to the geopolitical order, generated above all by the rise of China and a suite of domestic and global policies that it has espoused, are a principal new danger.

The Geopolitical Threat

The post–Cold War world of a dominant US superpower and the supposed triumph of democracy over all other forms of government, packaged as the “end of history” by Francis Fukuyama (1989), has been superseded by a return to great power rivalry centred on the rise of China and a new era of intense technology competition, a phenomenon aptly described as “techno-nationalism.”[8]

The national security challenge China poses to Canada has both global and domestic dimensions. Globally, China’s model of authoritarian capitalism stands in sharp contrast to the forms of democracy and market capitalism in the West. China is now in the top rank of global economies, is the largest trading partner of almost every country in Asia and of many others around the world, and is at the centre of diverse global supply chains. It is not just a manufacturing giant; it is also increasingly a technological innovator in areas ranging from artificial intelligence (AI) and quantum computing through information communication technology (ICT) and financial technology (fintech). In recent years, the West has experienced a technology innovation race with China, with potentially dangerous ramifications for national security.

Chinese mega projects such as the Belt and Road Initiative, overseas trade and two-way investment, and technological innovation have coincided with an expanding Chinese presence and influence in regional and global diplomatic institutions. They have also undergirded the expansion and modernization of China’s military capabilities, which are altering the military balance in Asia.

Under the leadership of President Xi Jinping, China is more repressive and nationalistic domestically, and more assertive in promoting and defending its interests both in its immediate neighbourhood and internationally, including in multilateral institutions such as the United Nations. China should be regarded as a selective revisionist in challenging norms related to democracy and human rights and some aspects of international law, while being more assertive and influential in shaping rules and institutions to defend and promote its national interests. China is increasingly taking on the role of rule maker as well as rule taker.

[8] See Ostry and Nelson (1995).

China's rise poses a new set of issues for Canadian support of human rights and democratic values abroad, including advocacy against arbitrary detention as a tool of statecraft, a matter on which Canada has taken a global lead. The challenge for Canadian policy is to find a way to advance Canada's values and support for the rules-based international order, while recognizing the necessity of attempting to work with China to deal with global issues including climate change, public health, poverty reduction, and non-proliferation and arms control.

Domestically, China is no longer "over there" — it is on Canadian doorsteps, with new capabilities and interests. China's growing power and aggressiveness weighs on Canadian national security directly in areas such as espionage, undue penetration of Chinese commercial interests in sensitive sectors of the Canadian economy, concerns about IP theft and exfiltration, and covert interference in our social fabric and democratic processes. The Chinese government is interested in shaping Canadian views of China and the world and, in some instances, interfering in the lives of residents of Canada who are critical of its policies or practices or who are evading the Chinese legal system. Moreover, China has strategic, commercial and scientific interests in the Arctic, which must be closely monitored.

China's impact and the attendant rise of global insecurity is a key driver that defines a new national security threat for Canada. Getting the right balance of coexistence, cooperation, competition and countering China will be a major test for Canadian policy in the years ahead. It will be even more complex as we manage our relations with the United States, which is committed to a multi-dimensional strategic competition with China. Where and on what issues do we align or ally with Washington? To what extent do we concentrate on working with like-minded friends in pushing back or confronting China in a new Indo-Pacific context and in the specific form of the Quadrilateral Security Dialogue (the Quad)[9] or AUKUS?[10] On what issues do we seek common ground with China?

Understanding the dimensions of the China challenge and devising policy responses, in particular in terms of Canada's economic security and the defence of our democratic system, will be a key preoccupation of the national security system for years to come. An expanded intelligence capability, including intelligence sharing with allies, to better understand the China challenge will be critical to success.

Russia currently stands as a second-order threat to geopolitical stability. Russia, while aspiring to regain lost great power status, has proven to be a persistent disrupter, with its military intervention to shore up a failing Syrian regime, its seizure of the Crimea and its ongoing military pressure on Ukraine. Russia has proven an adept user of asymmetric power channelled through sophisticated cyber interference and aggression, particularly targeting Western democratic systems and elections. In a replay of the Cold War, Western observers fear an opportunistic alliance between China and Russia to advance their interests (Segal and Fitz-Gerald 2021).

Geopolitics has taken on a renewed dimension of ideological contest, pitting democratic regimes against authoritarian and even hybrid political systems. This contest not only affects confidence in democratic principles, but it also upends international stability and vastly complicates international consensus building and the maintenance of accepted norms of state behaviour. These impacts are concerning to Canada both as a country that strives to uphold democratic principles and as a power dependent on international stability for its economic security (Momani 2021).

[9] The Quad is an informal dialogue between Australia, India, Japan and the United States that shares a vision for "a region that is free, open, inclusive, healthy, and anchored by democratic values, and unconstrained by coercion." Together, the Quad aims to strengthen cooperation on the defining challenges of our time. This includes responding to "the economic and health impacts of COVID-19, combatting climate change, and addressing shared challenges, including in cyber space, critical technologies, counterterrorism, quality infrastructure investment, and humanitarian-assistance and disaster-relief as well as maritime domains" (The White House 2021b).

[10] AUKUS refers to a trilateral security pact between Australia, the United Kingdom and the United States. It is committed to expanding diplomatic, security and defence cooperation in the Indo-Pacific region. It aims to "foster deeper integration of security and defense-related science, technology, industrial bases, and supply chains. And in particular, will significantly deepen cooperation on a range of security and defense capabilities" (The White House 2021c).

The Economist Intelligence Unit, in its democracy index for 2020, noted a significant decline in global democratic practice, with COVID-19 responses a major contributor. The worst-affected regions were Africa and the Middle East. Among full democracies, Canada scored a highly respectable fifth, but the United States was rated as a "flawed democracy." Because of measures imposed by Beijing that curtailed rights, Hong Kong slipped into the category of "hybrid" regime (Economist Intelligence Unit 2021). This is the world in which Canada, a principled defender of democracy, now operates.

Freedom House, in its authoritative survey, found that "democracy's defenders sustained heavy new losses in their struggle against authoritarian foes, shifting the international balance in favor of tyranny. Incumbent leaders increasingly used force to crush opponents and settle scores, sometimes in the name of public health, while beleaguered activists — lacking effective international support — faced heavy jail sentences, torture, or murder in many settings" (Freedom House 2021).

Canadian political parties share a sense that Canadian foreign policy must be principled and operate to defend democracy, although they may disagree on more precise objectives. Fair enough. But Canadian foreign policy must also, in future, be much more closely integrated with national security policy. Simply put, our foreign policy should serve to advance our national security protections, which themselves are based on a framework of principles, including upholding democratic practices. This is especially true for our policy toward China. To advance an integrated foreign policy based on both principles and national interest requires a better understanding and predictive ability about global threats, as well as opportunities for global cooperation. These should be the raison d'etre of our foreign service.

Pandemics as a National Security Threat

In addition to rising geopolitical tensions, a major factor driving the need for a new understanding of national security has been the rise of non-traditional, transnational threats posed by pandemics. While Canada was hard hit by the severe acute respiratory syndrome epidemic in 2003, that experience was not enough to alter its approach to national security. The destructiveness of COVID-19 must force a change as we recognize the impact the pandemic has had on national security. In addition to contributing to geopolitical tensions, COVID-19 has affected our economic security, disrupted supply chains, required new thinking about how to integrate health security monitoring into border security measures, and injected new divisions and tensions into Canadian politics (Desai and Munroe 2021).

Canada must be better prepared for future pandemics, especially those likely to derive from zoonotic diseases that spread globally and can prove capable of dangerous mutations. National security measures cannot prevent pandemics, nor can they solve them. But they can contribute greatly to pandemic preparedness, especially through early warning capacity and an ability to properly assess the level of threat to Canada posed by infectious disease outbreaks, wherever in the world they might occur. Our system for early warning and for risk assessments, primarily based at the Public Health Agency of Canada (PHAC), failed in the early months of the COVID-19 outbreak, and must be reconstituted and strengthened for future emergencies (Office of the Auditor General of Canada 2021; Wark 2020).

A parallel failure occurred in terms of DND intelligence reporting on the dangers posed by COVID-19. While DND possessed advantages unavailable to PHAC, including a strong intelligence reporting system and a pandemic contingency plan, the Canadian Forces Intelligence Command and its associated medical intelligence capacity were unable to generate well-informed and accurate threat assessments or provide an early warning capacity for the department or the government at large. Like PHAC, DND grossly underestimated the risk COVID-19 posed to Canadians until after the disease had established its vicious beachhead in Canada (Levy and Wark 2021; Wark 2021a).

Correcting these problems will require a much greater ability to monitor and understand global health threats, which will need to include coordinated contributions from different elements of the Canadian security and intelligence system. Intelligence inputs should assist in generating higher-quality risk assessments to inform government decision making on necessary and timely actions on border restrictions, stockpiles of personal protective equipment, societal measures for mitigation such as mask wearing and social distancing, and public communications (Levy 2021). Understanding threats posed by pandemics and other biosecurity dangers must be a strong focus in a new approach to national security strategy.

Climate Change Security Impacts

Just as we need to better integrate health security and national security measures, there is an equal urgency to confront the security implications of global climate change impacts (Dalby and Lawrence 2021). The recently released US National Intelligence Estimate (NIE) on climate change assesses that it "will increasingly exacerbate risks to US national security interests as the physical impacts increase and geopolitical tensions mount about how to respond to the challenge" (National Intelligence Council 2021, i). The same assessment applies to Canada, even if we have, to date, failed to produce an equivalent of the US NIE to guide policy.

International insecurity driven by climate change impacts will rise in ways that matter to Canada, causing heightened global tensions, threatening conflicts over natural resources, accelerating the decline of failing and failed states, and generating climate-induced global migration. Canada's international development program needs to be refocused to assist the areas of the globe hardest hit by deepening climate change impacts.

Climate change also has an obvious direct bearing on Canada's domestic security, through extreme weather events, heat domes and drought, forest fires, environmental degradation and the associated critical infrastructure impacts. British Columbia has been hard-hit in recent months by the interlocking and compounding effects produced by climate change. Climate change is also being felt dramatically in Canada's Arctic region, where it is increasing human insecurity for the Arctic's Indigenous peoples as it threatens livelihoods. Climate change is exposing the Arctic as a new zone requiring the protection and projection of sovereignty, with increased domain awareness an important capacity. The Arctic demonstrates the interplay between the presence of new exploitable resources, especially critical minerals, and Canada's national interests (Dalby 2021b).

The US NIE on climate change finds that there will be rising competitive activity in the Arctic region but that such competition will be "largely economic"; however, over the longer term (out to 2040), it injects a concern about the risks of miscalculation "as commercial and military activity grows, and opportunities are more contested" (National Intelligence Council 2021, 8, i). Canada needs its own assessments on these trends. Such assessments need to have a public face to better educate Canadians about the dangers of climate change and their specific regional impacts.

The key contribution that national security capabilities can make to climate change adaptation is, in parallel with pandemics, to generate early warning intelligence and forecasts on global developments, and risk assessments, including longer-term studies, around impacts for Canada. The national security system can also plug into classified assessments being done by our allies in the Five Eyes intelligence partnership (Australia, New Zealand, the United Kingdom and the United States) and through other bilateral security partnerships. It will be particularly important to understand the security implications of climate change impacts for Canada's Arctic region. The announcement of Canada's decision to create a North Atlantic Treaty Organization Centre of Excellence on Climate and Security is an important indicator of the importance of the nexus between climate change and security for Canada, and also provides an opening for Canada to take a global leadership role (Prime Minister of Canada 2021).

The commitment in the Liberal Party election platform to strengthen the ability of the office of the NSIA to monitor the implications of climate change could be an important first step in establishing an essential central capacity in government, one that is currently missing.[11] Addressing threats from climate change impacts must move to the top of the national security agenda.

Technological Change: Implications for National Security

We think of technological change as a permanent feature of the national security landscape. Perhaps that familiarity is why it was not specifically addressed in the national security statement in 2004. Technological change has profoundly shaped military capabilities through the development of new offensive and defensive weapons and systems of war. The pace of change continues to accelerate in the military domain, including in drone development, hypersonic rocket systems and other weapons of war. Technological change has always

[11] See Liberal Party of Canada (2021).

been a driver of key intelligence capabilities and is the foundation of our modern intelligence systems.

Today's world involves an accelerated pace of technological change, signified principally by emerging and disruptive technology (EDT). There are significant developments in cyber, telecommunications, data processing and analytics, facial recognition, and AI and machine learning, among others. Some of these developments can be weaponized. All have implications for our national security capabilities and conduct (Araya and Mavinkurve, forthcoming 2022). As Shelly Bruce (2021) commented, "Canadians have been early adopters of technology and we are very comfortable online." She also noted, "we consider this kind of Canadian technological embrace a distinct national advantage" (ibid.).

However, the rapid embrace of EDT and the increasing ubiquity of connected and data-intensive technologies across the Canadian economy, and within government, creates several pointed challenges. One of the principal complexities of EDT in national security is that it creates significant opportunity for government to enhance operational efficacy while simultaneously increasing risk and the size of national vulnerabilities.

To better understand the nature of technological threats, four key issues will be explored: digitally enabled espionage; threats to critical infrastructure; the challenges of big data and AI; and new technology implications for the economy and national security.

Digitally Enabled Espionage Has Forever Transformed the Spy Game

Digitally enabled espionage creates several challenges for Canada. The first is economic. The downfall of Nortel, and the discourse surrounding possible causal links to Chinese economic espionage, was likely the first major example to capture public attention (CBC News 2012). However, this was also emblematic of a much larger trend. As CSIS Director David Vigneault (2021) has indicated, "Historically, spies were focused on obtaining Canadian political, military and diplomatic secrets. While these secrets are still attractive, today our adversaries are more focused on intellectual property and advanced research held on computer systems in small start-ups, corporate boardrooms, or university labs across the country." Defending our IP and advanced research will require new approaches and new partnerships.

The second is that the global public has become a source of intelligence, and this includes Canadians. Mass surveillance has deep implications for international human rights and came to global attention with the Edward Snowden leaks to the media in 2013. Some of the Snowden material drew controversial attention to Canadian practices involving CSE. Digitally enabled mass surveillance is now a reality of statecraft, including for Canada. National security policy will require a careful balance between the need to achieve national security objectives — where properly authorized mass surveillance may serve the purpose of ultimately allowing for more targeted and proportional surveillance — and the protection of individual privacy rights.

The third challenge mounted by new espionage practices is that they are building distrust into the core fabric of the still unfolding Internet of Things (IoT) and the cyber-physical world. In 2016, James Clapper, former US director of national intelligence, said: "In the future, intelligence services might use the [IoT] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials" (Clapper quoted in Ackerman and Thielman 2016). With the increasing ubiquity of facial and vocal recognition, iris and retinal scans, gait analysis, the use of fingerprints for biometric identification, and palm vein scans — among others — it is clear that the "future" Clapper was referring to is here. These new technologies are being deployed in an increasingly tense geopolitical environment, where both allied and adversarial states will seek advantage through their clandestine application and subversion (Bradshaw and Rohozinski, forthcoming 2022).

Connected Critical Infrastructure and Its Vulnerabilities

There is evidence all around us that we must pay increased attention to protecting the critical infrastructure on which daily life depends as a national security priority. The effort must go into hardening critical infrastructure, especially against cyberattacks. But equally we must seek some agreed global norms to support our social fabric. The Secretary-General of the United Nations established a Group of Governmental Experts (GGE) on Advancing Responsible State

Behaviour in Cyberspace. In its July 2021 report, the GGE stated that a "state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" (United Nations General Assembly 2021, 12).

While this was advanced as an important "norm" of responsible behaviour, some actual state practice may be pulling in the opposite direction. According to the most recent and measured CSE cyberthreat assessment: "We assess that it remains very unlikely that cyber threat actors will intentionally seek to disrupt Canadian critical infrastructure and cause major damage or loss of life in the absence of international hostilities. Nevertheless, cyber threat actors may target critical Canadian organizations to collect information, pre-position for potential future activities, or as a form of intimidation. We judge that state-sponsored actors are very likely attempting to develop the additional cyber capabilities required to disrupt the supply of electricity in Canada" (CSE 2020, 21).

Just how far offensive cyber capacity has developed globally is difficult to evaluate in its totality, but the indications are that it is taking on aspects of a dangerous arms race. As one US official put it, "This was pretty mind blowing…going to work everyday behind sealed doors, essentially trying to figure out if it was possible to cripple an entire nation's infrastructure without ever firing a shot or dropping a bomb" (quoted in Sanger 2018, 44). The hard part, the official said, was not getting malware onto another country's critical infrastructure, rather, the "hard part was keeping track of all of it" (ibid.).

States are pre-positioning themselves to respond to cyberattacks. This creates a tremendously destabilizing set of forces, raises the chance of miscalculation and leads to the spectre of a dangerous spiral of escalation in response to a cyberattack. According to the US 2018 National Cyber Strategy, all instruments of national power are available to respond to malicious cyber activity, including a kinetic military response (The White House 2018). But there are no clear guidelines on when a cyberattack will warrant a kinetic response. The same can be said for Canada, even though CSE now has a mandate to conduct pre-emptive, "active" cyber measures against foreign targets.[12] Sophisticated and measured policy guidance and strong control on the use of such measures will be vital, as will the intelligence base on which such decisions for kinetic response will be based.

Big Data and AI Are Changing Everything

As data flows increase in size and complexity, the challenges and risks of managing data security rise exponentially. In a public speech hosted by CIGI, Privacy Commissioner of Canada Daniel Therrien agreed with a previous observation made by Jim Balsillie that "data governance is the most important public policy issue of our time" (Therrien 2021). Therrien went on to say that where "the first industrial revolution was powered by steam, the fourth is driven by data" (ibid.). Yet the international governance of data remains woefully inadequate and the national security vulnerabilities remain poorly understood.

In a world where everything is increasingly connected, large volumes of data are collected, shared and stored in unprecedented ways at tremendous speed, enhancing the susceptibility for misuse. Along with a heavy demand for large data sets to advance research and development in technology sectors such as AI, there is rising potential for theft and manipulation by state and non-state threat actors. The global market for personal data also remains largely unregulated, heightening the potential for data brokers to bypass accountability measures while also failing to manage the risks connected to transborder data flows (Aaronson 2020). With few incentives to protect personal data, despite eroding consumer trust, companies continue to manipulate and monetize data assets, thereby favouring profits over people.

Data is being mobilized and weaponized by advances in AI. A clear warning about the dangers of unreadiness in the face of change fuelled by AI has been sounded in the final report of the US National Security Commission on Artificial Intelligence (2021):

> AI systems will…be used in the pursuit of power. We fear AI tools will be weapons of first resort in future conflicts. AI will not stay in the domain of superpowers or

[12] *Communications Security Establishment Act*, SC 2019, c 13, s 76.

> the realm of science fiction. AI is dual-use, often open-source, and diffusing rapidly. State adversaries are already using AI-enabled disinformation attacks to sow division in democracies and jar our sense of reality. States, criminals, and terrorists will conduct AI-powered cyber attacks and pair AI software with commercially available drones to create "smart weapons." It is no secret that America's military rivals are integrating AI concepts and platforms to challenge the United States' decades-long technology advantage.

No similar comprehensive study has been undertaken in Canada, but the extensive list of recommendations advanced by the US commission holds relevance for us, particularly in the calls for strategic thinking and leadership, the creation of new talent pipelines, innovation investment, resilient supply chains, and the need to work toward the establishment of international guidelines for the development and deployment of AI-enabled and autonomous weapon systems.

There is no question that the adoption of AI capabilities for national security and defence purposes will raise important legal, ethical and strategic questions, especially with regard to the lethal use of force and the nature of the human-machine interface in terms of chain-of-command responsibility. As authoritarian regimes deploy AI-enabled systems of surveillance and repression, democracies must demonstrate a different, responsible path. Privacy-protection standards and democratic norms must attend the rapid and unstoppable deployment of AI.

Economic Insecurity and Canada's Innovation Agenda

Canadians are not used to thinking holistically about economic security risks. As an open economy, devoted to free trade principles, and a global marketplace, a new emphasis on economic security marks an important departure from the past. This shift toward greater rigour in protecting Canadian economic security must also be driven by an understanding of the distinction between the traditional economy of tangible assets and the production of goods and the new "intangibles" economy, where wealth creation is driven by IP and data.

There is a dynamic interplay between economic security, commercializing domestic innovation, IP, technical standards, data and national security (Ciuriak and Goff, forthcoming 2021). Canada's innovation sector is strong but needs more support in moving from research to start-up applications to scaling companies, and to prevent an export of our talent and ideas.

As an economic security task force reported recently in a consultation paper: "Canadians have taken their place on the cutting edge of important emerging fields of technology which have become key drivers of economic growth and development. While this has brought new opportunities for Canada, it has given rise to new and potential serious national security vulnerabilities" (Public Safety Canada 2021a).

These vulnerabilities have inward and outward dimensions. Illicit inward concerns arise from heightened levels of economic espionage, as foreign state actors seek to penetrate sectors of the Canadian economy to steal valuable data and IP. They are also a product of cyber-enhanced capabilities in the hands of organized crime groups that utilize methods such as ransomware attacks to generate huge profits and fuel more attempts.

There are also inward concerns surrounding high levels of foreign investment, especially investment generated by companies based in adversarial nations, that might have an impact on critical sectors and infrastructure and harm national security. The Government of Canada released updated Guidelines on the National Security Review of Investments under the Investment Canada Act (ICA) in March 2021.[13] These guidelines set out factors that the government will use when assessing security risks posed by foreign investments and enumerates those sectors that will attract heightened scrutiny, including sensitive technology, critical minerals and personal data. While this is a welcome focus, it is not sufficient.

Given that the ICA is the primary mechanism for assessing the potential impact of incoming investment on the Canadian economy, the scope of review should be broadened to allow for an informed assessment of the prosperity and security implications of incoming investment into the innovation, knowledge-based and data-driven economy.

The ICA will increasingly be a key national security tool. To function properly, it will need proper resourcing and talent, the best possible intelligence basis for decision making, which will put a new onus on Canada's economic intelligence capabilities, sound decision making and strong political engagement. Once a formal national security review of a foreign investment is undertaken, the national security system can provide advice to Cabinet, but it is ultimately ministers who must be able to decide what is in Canada's national interest. Use of the ICA to block Chinese foreign investment in sensitive sectors or by Chinese state-owned enterprises must be considered as a likely persistent irritant in future Canada-China relations with potential blowback impacts on the activities of Canadian commerce in China. The Canadian government must be ready and willing to defend its national security decision making over foreign investment.

Outward-facing concerns revolve around trade and exports that might involve sensitive goods and technology, including the grey zone of dual-use materials, and about research partnerships that might not be beneficial to Canada's interest in terms of loss of IP and exfiltration of data and expertise. Both federal and provincial programs have been put in place that involve closer scrutiny of university-based research partnerships with foreign entities, but their efficacy and downsides have yet to be fully scrutinized, and there needs to be close attention to their benefits and costs before they are expanded (Innovation, Science and Economic Development Canada 2021; CBC News 2021b). As with use of the ICA, the focus of security scrutiny of research partnerships will primarily concern contacts with Chinese entities. Security scrutiny must be carefully and scrupulously managed, something that is unlikely to be possible in the current construct, where responsibility has been downloaded on university researchers and university administration, neither of which is well-equipped to conduct such scrutiny.

As is demonstrated by the requirements of the ICA and security screening of research partnerships, more attention needs to be paid to the national security system's economic intelligence capacity.

[13] See Government of Canada (2021).

Economic intelligence has always been a peripheral activity of the Canadian intelligence community, with uncertain priority. In the face of new economic security threats, it needs to be ramped up, not to engage in aggressive economic espionage abroad to mirror the activities of some foreign adversaries, but in terms of greater open-source knowledge and strengthened assessment capabilities to understand adversarial developments in economic policy and understand both state and private sector threat actors.

In addition to an enhanced economic intelligence capacity, the government needs to be able to map the key nodes of critical infrastructure of national importance that require security protection.

The COVID-19 pandemic has brought to the fore concerns about vulnerable supply chains. Canada has limited capacity on its own to reshore supply chains, but it needs a strategy to prioritize their protection and an industrial policy that would support such a strategy with an innovation lens. We know that critical minerals are going to be one key to the transition to a green economy. Canada's natural resource sector has untapped wealth in critical minerals but, with economic security concerns in mind, we need to develop a policy around their mapping, resource extraction, processing and export.

All of these recommended new approaches point to another issue relevant to national security. Successful technology adoption and defensive measures to protect our technology sector require an understanding of technology, especially by senior decision makers. The future capacity of decision makers in the national security system will depend on their knowledge of new technological capabilities, which will require a considerable rethinking of models of recruitment, training, executive learning and pathways for career advancement.

Persistent and New Threats and National Security Priorities

The threat environment that Canada faces is dynamic and fast changing. Amid the mix of persistent, if transformed, threats, and new or newly identified threats, the challenge of establishing priorities is deepened. The Canadian national security system has finite resources. Priority setting is ultimately a matter of political judgment but must be based on the best possible engagement between political decision makers and the national security community that serves them. Priority setting is a significant test of the cultural maturity of national security policy in Canada but currently operates in the dark. Accountability for priority setting needs to be enhanced; for this reason, this report advocates for an annual statement on Canada's high-level intelligence priorities.

These priorities must be guided by the intersection between Canada's national interest and the threats the country faces. Those threats that engage all dimensions of the definition of national security advanced earlier are the ones that deserve priority attention.

To repeat that definition: national security aims to protect Canada and its people from major threats that would undermine our democratic institutions and processes, our economy, our social fabric and values, and our interests.

In line with this definition, the most significant priority threats are: global, transnational threats from climate change and future pandemics; the rise of China and international insecurity; technological threats; and economic security threats.

Adaptation by the Government of Canada and a new understanding by Canadians will be crucial to a successful response to the new threat environment.

The National Security Threat Landscape and Canada's National Interest

National security has at its core, as the definition given earlier suggests, a protective function. The national interest in putting protection first — whether protection of our people, our governance system and democratic practices, our economy, our territory or our international objectives — should be crystal clear. But for too long, Canadian national security has not had a central place in our thinking about national interest. For too long, we have undervalued a sovereign capacity for national security, especially when it seemed relatively easy (and certainly inexpensive) to depend on allies, in particular on the United States in a geographically bounded concept of the protection of North America.

The necessity of building a greater sovereign capacity for national security is not an insular reflex. Rather it reflects the changing nature of national security threats. Canada is going to have to navigate its own way through a present and future of heightened geopolitical tensions. No doubt that navigation will require multilateral engagement and close alliance partnerships, but it will have to be driven by new Canadian capabilities to understand the world we live in. Dealing with climate change and pandemic threats also requires heightened Canadian capabilities and attention to direct Canadian impacts as well as close international cooperation. Better protection for our economy will be dependent on Canadian choices of where we strengthen our system with close attention to allied and adversarial developments. Our ability to manage technological change for the benefit of national security must be based primarily on new Canadian capabilities.

National security strength founded on a greater and targeted sovereign capacity must be our goal. We no longer live in a world where we can outsource our protection to others, as much as we benefit from multilateral cooperation and core national security partnerships such as the Five Eyes.

A sovereign national security capacity must be a demonstrable good for Canadians — which requires democratic engagement and legitimacy — and it must be a demonstrable good for Canada's allies, in particular in the context of taking a stronger role in the Five Eyes partnership to sustain our worthiness to our allies even while we remain a net importer of intelligence.

A Greater Sovereign Capacity for National Security

What are the contributors to a greater sovereign capacity for national security? They depend on these elements (Fyffe 2021):

→ an enhanced, made-in-Canada capacity to understand threats, which requires strong intelligence collection and assessment capabilities geared to new global threats;

→ an integrated and effective system for establishing intelligence priorities and for the sharing of threat reporting;

→ a strengthened capacity for the dissemination of intelligence reporting and threat assessments; and

→ an improved culture of decision-maker and political attention to intelligence and threat reporting.

If these sovereign capacities are in place, they can be used to our advantage in making a greater contribution to our intelligence partners in the Five Eyes. These are not piecemeal initiatives. Tying these elements together requires an integrated review of our current national security system, linked to defence, foreign policy, development, economic security and technology policy.

Guidance for a strengthened sovereign capacity requires a national security strategy, which, among other things, would offer a blueprint for national security renewal.

Two key messages were embedded in the 2004 national security policy, which deserve renewed attention. One was the importance of building an integrated national security system and effort — an intention that remains incomplete 17 years later. Building this system is now of renewed urgency, given the nature of the new threats Canada faces. It requires buy-in and leadership by the departments and agencies that comprise our national security system — it cannot be composed or imposed from without. The starting point for a strong push for integration should be a comprehensive review of capacity and objectives that sees national security as the centrepiece of an interconnected field of policy endeavours.

The other was a statement about the centrality of intelligence to the national security mission. This is how the 2004 policy framed the role of intelligence: "Intelligence is the foundation of our ability to take effective measures to provide for the security of Canada and Canadians. To manage risk effectively, we need the best possible information about the threats we face and about the intentions, capabilities, and activities of those who would do us harm. The best decisions regarding the scope and design of security programs, the allocation of resources and the deployment of assets cannot be made unless decision-makers are as informed as possible" (Privy Council Office 2004).

This statement would be unfamiliar to most Canadians because it is so rarely stated by governments. It needs to become embedded in our understanding of national security.

Updating this statement would require us to acknowledge two things. One is that while capabilities and intentions define the intelligence mission for state and non-state actors, they lose their salience in dealing with actorless threats posed by such things as pandemics and climate change security impacts. A second is that decision makers need something more than information from intelligence agencies — they need a true appreciation of both the value and limitations of intelligence and a willingness to utilize it routinely in decision making. Simply put, decision makers, including politicians, need education about intelligence, but there is another side to this: intelligence agencies need education, or understanding, about the needs and outlooks of decision makers.

There is a broad recipe for strengthening Canada's sovereign national security capacity, which begins with improvements to our intelligence system. These improvements include, first of all, pivoting our intelligence collection and assessment capabilities to the new national security threats described in this report: geopolitical tensions; pandemic and biosecurity threats; climate change security impacts; technological change and its weaponization; and economic threats. This pivot would need to include, on balance, a greater emphasis on global knowledge acquisition compared to domestic security intelligence, and a heavier reliance on OSINT collection. A recent report by the US Center for Strategic and International Studies, *Maintaining the Intelligence Edge* (Katz 2021), which called for a "dramatic reimagining and reinvention" of the US intelligence community (there is that phrase again), recommended as a major step the "elevation" of OSINT as a key intelligence collection tool. The report went so far as to consider the creation of a separate OSINT agency, alongside better integration of OSINT into collection and analysis across the US intelligence community. Demonstrating reimagination potential, it even advocated for the creation of an AI-OSINT exercise to test its unique critical ability to come up with new analysis of critical threats, including AI-enabled disinformation operations.

A pivot to greater global intelligence capabilities may even require the long-debated creation of a separate Canadian foreign intelligence service. The pivot would necessarily involve a better resourced and coordinated program for intelligence assessment that would break down separate mission silos, focus on issue assessment, and provide more emphasis on strategic intelligence and longer-term forecasting, alongside the current reporting mission that occupies most of the assessment community's attention.

An enhanced intelligence assessment capacity could also be furthered by Canadian willingness to promote and support the practice of joint intelligence assessments with our Five Eyes partners. Joint intelligence assessments seem particularly fruitful in dealing with complex transnational issues where multiple expert inputs would be valuable and any barriers to sharing relatively low.

Improvements in our intelligence assessment capacity will have to be matched by an ability to ensure decision-maker attention, understanding and respect for intelligence reporting.

As we move toward greater global collection and assessment, a new understanding of threats, more effective and sustained use of OSINT, a more centralized and integrated assessment machinery, and new intelligence reporting products with more strategic — and long-term — focus, the national security system will have to become less insular

and walled-off. Forms of information and personnel exchanges will have to be encouraged and made routine between the national security system and outside experts in many fields relevant to the key threats that inform intelligence priorities.

The national security system will have to develop a stronger capacity to work with the Canadian technology innovation sector to fully understand the implications and uses of new technological developments and to appreciate the value of made-in-Canada applications.

None of this is to argue for intelligence outsourcing, except in limited and managed ways. The value of an intelligence system embedded in government, close to decision makers, with privileged access, security classification standards, trusted reporting routines and products, and an ability to respond quickly to decision makers' needs remains paramount. This cannot be replicated in an outsourced system. But there is a golden mean between outsourcing and a traditional and hermetically sealed national security system, which could provide a much freer circulation of people and ideas without comprising the benefits of the more traditional system.

To begin a process of providing for greater infusion of outside expertise on a diverse range of national security issues, this report advocates for the creation of a series of expert advisory councils on the following:

- Canada-China national security issues;
- climate change and security;
- pandemic and biosecurity threats;
- cybersecurity and technological advances;
- economic security; and
- border security, including Canada-US policy.

Each of the expert councils should report to the prime minister through the NSIA. An annual report summarizing their work should be published. While the establishment of such councils would mark a significant departure from current practice and would be an ambitious enterprise, we believe it a necessary one that can learn from past, and promising experiments such as the Advisory Council on National Security, which operated from 2005 to 2011.[14] The key ingredient for success would involve the engagement of experts, a clear and focused agenda dedicated to generating new thinking and applied policy options, and decision-maker attention. Experience with such councils could ultimately lead to other governance change within the national security system, including consideration of the establishment of "national intelligence officers" focused on bridging the intelligence-policy divide on key national security issues in a way analogous to the model utilized in the US National Intelligence Council.

Implementation of an advisory council system might be done incrementally on one or two key issues to establish the model before expanding it.

Advisory councils of this nature will ultimately mark a significant change in the ability of the government to understand threats to national security. Managing this range of expert councils would require dedicated time by the NSIA, the possible creation of a deputy NSIA and new resources for the office of the NSIA. However, the value of this engagement is clear. It would create an effective mechanism for utilizing expertise from outside of government on a range of complex policy challenges.

Another key to achieving greater sovereign national security capacity involves major changes to the governance and culture of national security decision making. A series of cascading changes are envisaged that start from the very top of the governance system.

This begins with an acceptance that the prime minister holds ultimate responsibility for national security strategy and policy. In a Canadian Westminster system, the prime minister is not the "president" of national security but relies on the Cabinet and ministers with shared national security responsibilities. To begin with change at the top, a dedicated cabinet committee on national security should be created, normally to be chaired by the prime minister with the assistance of a vice chair held on a rotating basis by key ministers from the departments of Public Safety, Global Affairs and National Defence. This would re-establish a capacity at the Cabinet table that existed during the Cold War (the Cabinet Committee on Intelligence and Security).

The prime minister would have some unique responsibilities, including issuing an annual statement to Parliament on the worldwide threats facing Canada and allocating time in Parliament for discussion and debate by members of Parliament and senators.

The prime minister would hold ultimate responsibility for the issuance of a national security strategy to be revised and updated on a set schedule. The work of producing the national security strategy would be overseen and directed by the NSIA and this responsibility, among others, would be set out in legislation describing the NSIA role.

The prime minister and the cabinet committee on national security would receive a regular (on at least a weekly basis) and highly classified report on threat developments and national security challenges, which would provide the centrepiece for the cabinet committee's deliberations. This reporting product would be a Canadian equivalent to the US president's PDB (President's Daily Brief)[15] and the UK Joint Intelligence Committee's "Red Book."[16]

The further cascade of governance changes down the system, in particular an examination of the efficacy of a multi-tiered and often shifting array of committees from the deputy minister to the assistant deputy minister to the director general level should be one outcome of an integrated review of national security. Special attention should be paid to the role of the deputy minister committee on intelligence and the deputy minister committee on national security as important tables for integrated intelligence sharing and policy advice. The ability of the NSIA to fully contribute to the coordination of the Canadian security system and its reporting to Cabinet also needs to be examined as part of this review.

One key issue worthy of detailed study is the question of the value of establishing a Canadian-style NSC to ensure high-level decision making on

[14] Co-author Wesley Wark served on the Advisory Council for two terms from 2005 to 2009.

[15] See www.intelligence.gov/publics-daily-brief/presidents-daily-brief.

[16] See https://discovery.nationalarchives.gov.uk/details/r/C15403.

national security and intelligence issues, drawing on best practice adoption from counterpart organizations in Australia, the United Kingdom and the United States. An NSC-type structure would reshape both Cabinet deliberations and the organization of senior bureaucratic committees.

Thinking about organizational change, two things can be noted in conclusion: organizational change alone will not guarantee success; and organizational change depends on the lifeblood in the system, which consists of high-value intelligence products geared to top intelligence priorities and responding to a new threat environment, and an educated body of intelligence consumers, from the prime minister on down, who understand the value of intelligence. Organizational change without this lifeblood will be meaningless. But without organizational change, the lifeblood is blocked from circulation.

A greater sovereign capacity for national security that is rooted in an enhanced intelligence foundation and a functional system for integrating intelligence into policy making is a goal that must be pursued.

The Democracy Imperative

Making national security a demonstrable good for Canadians requires real democratic engagement to enhance public understanding, to underpin the protection of civil liberties and privacy, and to allow for accountability. Taking the national security strategy outside a zone of government paternalism and deeply entrenched cultures of secrecy poses a major challenge.

Important steps have been taken to meet this challenge, some exemplified by the greater willingness of security agency heads to address public audiences in recent years.

Two key advances are the publication of a National Security Transparency Commitment (NSTC) in 2017,[17] and the complete overhaul of Canada's national security and intelligence review system. Both speak to an understanding of the issue of creating a more informed and engaged public on national security matters.

The NSTC laid down a set of principles for achieving greater openness in the service of accountability and enhanced public knowledge in three areas: information transparency, essentially baseline information about the role of departments and agencies; executive transparency, to explain legal structures; and policy transparency. The third area is extremely significant, with promises to "inform Canadians of the strategic issues impacting nationals' security and its current efforts and future plans for addressing those issues" (principle 5) and consulting stakeholders and building transparency into the design of national security programs and activities (principle 6).[18] Many of the recommendations in this report align with the principles of the NSTC; however, the NSTC has no legislative force and its ability to move change along at speed is limited. The advisory group established to assist the government in implementing the principles of the transparency commitment has provided some recommendations in a recent report. Their recommendations are limited to working within the current framework, devolve responsibility on separate departments and agencies, and basically involve exhortations to greater effort on the transparency file. Such recommendations seem insufficiently ambitious and imaginative and are unlikely to result in significant change (Public Safety Canada 2021b). To give the NSTC the force required to match the importance of the principles committed to, its principles should be enshrined in legislation and the minister of public safety should be required to produce an annual report on the delivery of the commitment to Parliament (Public Safety Canada 2020; Wark 2021b). The transparency commitment needs to be matched in practice by public reports, including a national security strategy and annual statements on worldwide threats facing Canada and the government's intelligence priorities.

Independent review bodies, with access to sensitive records, can serve as important communicators of critical truths about the national security system. In recent years, there has been a major overhaul of the national security review system, beginning with the first-ever creation of NSICOP with a broad mandate and strong access to material covered

[17] See www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html.

[18] Ibid.

by national security confidentiality. NSICOP has undertaken important reporting since its creation in 2018 but has recently been mired in political and media controversy over its independence from the executive and its distinctive nature.

NSICOP was purposely designed in legislation to be a unique body of parliamentarians, in order for it to have routine access to classified material and briefings. One controversial feature of its legislation allows for the prime minister and officials to require redactions in its reports to Parliament on specified grounds of national security. This had led to a denial by opposition parties, mirroring their original criticism of the legislation, of the fundamental legitimacy of the committee. The current white-hot spotlight on NSICOP has been fuelled by the refusal of the government to hand over classified records to parliamentarians without proper security clearances to see them. Opposition parties and media commentators have argued that the committee is shackled to the prime minister's power and is not a proper committee of Parliament able to act on its behalf in pursuing studies of controversial issues, such as those raised by alleged security breaches at the National Microbiology Laboratory by scientists with research connections to Chinese counterparts (Wark 2021c).

These criticisms are ill-considered and overlook entirely the nature of the reporting, including on sensitive political issues, that NSICOP has accomplished since 2018.

NSICOP deserves to survive partisan wrangling in Parliament and may need rescuing through a revamping of its legislation to change the ways in which the committee's membership and chair are selected and to require formal responses from the prime minister to its reports and recommendations. Exaggerated notions of the exercise of a prime ministerial veto over the contents of reports need to be addressed. The Canadian practice is in fact very similar to that of the British model on which it is based, the Intelligence and Security Committee. There is a negotiated process concerning any necessary redactions that involves the advice of the security agencies that hold the records. The prime minister does not exercise a heavy hand. More transparency about the process may puncture the politicized dismissal of NSICOP's independence. The reality is that without a willingness on the part of Parliament to rely on NSICOP to delve into national security matters, Parliament would revert to being a body unable to properly study Canada's national security practices because of lack of expertise and access to sensitive documents. Without NSICOP, parliamentarians as well as Canadians would be deprived of one important channel of public reporting on Canada's national security system.

The creation of NSICOP was followed in 2019 by the passage of legislation that created new external review and oversight bodies focused on national security.[19] This new system is headed by the National Security and Intelligence Review Agency (NSIRA), with a mandate to report on the lawfulness of the performance of the key intelligence collection agencies, CSIS and CSE, as well as any other entity of the federal government with national security responsibilities, including the Royal Canadian Mounted Police. While it is too soon to gauge the effectiveness of NSIRA, its first annual report suggests it is being launched with considerable ambition and a desire to broach new subjects, including insider threats and counter-intelligence (NSIRA 2020). A promised review of medical intelligence would be a first in the history of external scrutiny of the national security community. The range of public reporting that NSIRA is mandated to produce should be an important contributor to increased public understanding, provided NSIRA is successful in making itself known to a public audience. Achieving this will require dedicated effort and a recognition that the public audience for review reporting is key.

The intelligence commissioner (IC) created alongside NSIRA in the 2019 reforms, is bound to be more low profile, but still represents a first for Canada in giving the IC oversight powers to determine the legitimacy of certain operations by CSE and CSIS. The IC stands as a dual key alongside the minister and can deny ministerial authorizations and thereby block operations that do not meet a threshold test of reasonableness. The IC will also report annually, adding yet another layer of information for a public audience.[20]

In addition to the existing promise and potential of review and oversight body reporting, and the importance of public statements by security agency chiefs addressing contemporary issues, a trifecta of official publications — a national security strategy, an annual worldwide threat assessment

[19] See www.parl.ca/LegisInfo/en/bill/42-1/C-59.

[20] See Office of the Intelligence Commissioner (2021).

and a statement on the government's intelligence priorities — should be produced. All this effort will combine, in time, to elevate the public discourse on national security issues and produce a circumstance in which the Canadian public can feel better informed and more engaged in a critical discussion of Canada's national security needs.

There will always be a healthy tension in democracies around national security issues as they inevitably brush up against concerns about government conduct and intrusive powers. George Orwell's dystopian vision of "Big Brother" will be forever with us. Democratic skepticism and questioning are the price to be paid for the acquisition by the national security system of reasonable levels of legitimacy or "social licence" for security and intelligence agencies. Beyond that, they can serve as inputs for an important process of improving performance, abiding by societal norms and maintaining lawfulness (Roach 2021).

The democratic imperative of our national security system includes the need for diversity and inclusion in hiring, promotion and access to senior positions. Security agencies should reflect our societal makeup, histories and identities; perform in accordance with societal norms; and be representative of the broader talent base of society. There is, at present, a gap between promise and delivery in that regard, which was detailed in an important report delivered by NSICOP.[21]

Among the factors that hinder greater diversity and inclusion in the national security system is the absence of standard performance metrics to judge the degree to which the system is meeting its human resources goals. As a prompt to the system, an annual report should be prepared by the NSIA on targets and progress toward diversity and inclusion among the security agencies. This would also provide another coordinating lever for the NSIA in an otherwise decentralized system.

As we confront new national security challenges in the coming years, it is vital that we do so alongside an informed public, and with a national security workforce that is truly a microcosm of our social fabric and its myriad talents.

National Security Law

National security law in Canada defines the mandates and permissible range of activities that can be undertaken by national security agencies. It is vital to the democratic conduct of national security. It is embedded in a key constitutional framework, the Charter of Rights and Freedoms, and overseen by a specialized Federal Court. While much attention has been paid since September 11 to the creation and refinement of national security law related to counterterrorism, other elements of our legal framework represent a very complex patchwork, with special legislative acts devoted to individual agencies and departments and particular regulatory regimes, such as the Security of Information Act (Forcese and West 2021). There is no comprehensive legislative framework binding this all together in a systematic way. Some important pieces of the legislative framework have not been substantially revised, such as the CSIS Act, which dates back to 1984.[22] DND intelligence operations are not subject to any legislation and take their authority from the Crown prerogative, a circumstance that the government has vowed to correct but has yet to take legislative action on. The Canada Border Services Agency, created in 2003, has no legislative mandate that defines its intelligence operations.

There is a need for a comprehensive review of the national security legal framework to ensure coherence, to study the possibility of introducing unifying legislation, to undertake a gap analysis, and to look at options for updating national security laws to meet a changing technological and threat environment, in particular in relation to CSIS. The most recent modernization of national security legislation, Bill C-59, did not touch the fundamentals of the CSIS Act. The director of CSIS has described the CSIS Act as "better suited for the threats of the Cold War era" (Vigneault 2021). He has argued that it "greatly impedes our ability to use modern tools, and assess data as information. We need laws that enable these types of data driven investigations, carefully constructed to reflect the values we share in our democracy, including assurances of robust privacy protections" (ibid.). Skeptics might argue that intelligence agency heads will always press for more intrusive powers — that

[21] See NSICOP (2021).

[22] *Canadian Security Intelligence Service Act*, RSC 1985, c C-23.

is their job. But we must take a serious look at antiquated legislation and decide where the balance lies between new authorities and rights protections.

The opportunity to conduct such a review is presented by the requirement for a parliamentary study of Bill C-59, the most recent national security legislation, scheduled to begin in 2024. But the groundwork needs to be laid now, as it will be a complex undertaking. Such a review should be led by the Department of Public Safety, with the support of the Department of Justice, be interdepartmental in nature, involve the Office of the Privacy Commissioner of Canada and also involve consultation with outside legal experts and scholars. This review could complement current studies of how the security agencies deploy legal advice to fulfill their "duty of candour," especially in warrant applications for intrusive surveillance to the Federal Court.

Conclusion

The saying, attributed to Winston Churchill, "Never let a good crisis go to waste," applies to the situation that Canada now faces. Our attention has been fixed, at least momentarily, on a fast-changing national security threat environment by the experience of the COVID-19 pandemic.

It has long been suggested in a Canadian context that no real change to our national security system would come about without the experience of an attack or dreadful piece of violence. This became a popular mantra among security professionals in the long aftermath of the September 11 attacks. It was surely too pessimistic but contained a grain of truth.

Now, we have been "attacked" by COVID-19 and that has opened our eyes, as the NSIA said, to the reality that we now confront an inflection point in global politics.

We need to change our policies and practices to respond to these new circumstances and we need to bring the public into the conversation. National security matters touch the lives of all Canadians, and they are, correspondingly, owed a serious public discussion about what their government plans to do about that.

A change agenda and an inclusive public conversation on Canadian national security is long overdue.

Works Cited

Aaronson, Susan. 2020. *Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves.* CIGI Paper No. 241. Waterloo, ON: CIGI. www.cigionline.org/static/documents/documents/no.241%202_0.pdf.

Ackerman, Spencer and Sam Thielman. 2016. "US intelligence chief: we might use the internet of things to spy on you." *The Guardian*, February 9. www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

Araya, Daniel and Maithili Mavinkurve. Forthcoming 2022. *Emerging Technologies, Game Changers and Impact on National Security*. Reimagining a Canadian National Security Strategy Report No. 9. Waterloo, ON: CIGI.

Arms Control Association. 2021. "Timeline of Syrian Chemical Weapons Activity, 2012–2021." www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity.

Bradshaw, Samantha and Rafal Rohozinski. Forthcoming 2022. *National Security Dimensions of Securing Canada's Digital Domain*. Reimagining a Canadian National Security Strategy Report No. 10. Waterloo, ON: CIGI.

Bruce, Shelly. 2021. "Chief Shelly Bruce's speech for Centre for International Governance Innovation, May 18, 2021." https://cse-cst.gc.ca/en/information-and-resources/chief-shelly-bruces-speech-centre-international-governance-innovation-may.

Canadian Centre for Cyber Security. 2020. *National Cyber Threat Assessment 2020.* Ottawa, ON: Government of Canada. https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf.

CBC News. 2012. "Nortel Collapse Linked to Chinese Hackers." February 15. www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591.

———. 2021a. "Cyberattack confirmed as cause of health-care disruptions in N.L." November 3. www.cbc.ca/news/canada/newfoundland-labrador/health-care-disruptions-day-5-1.6235229.

———. 2021b. "Alberta orders universities to pause partnerships with links to Chinese government." May 24. www.cbc.ca/news/canada/calgary/alberta-government-china-universities-partnership-1.6038701.

Ciuriak, Dan and Patricia Goff. Forthcoming 2021. *Economic Security and the Changing Global Economy*. Reimagining a Canadian National Security Strategy Report No. 8. Waterloo, ON: CIGI.

Conger, John and Shiloh Fetzek. 2021. *A Climate Security Plan for Canada: How the Government of Canada Can Combat the Security Risks of Climate Change.* Washington, DC: Center for Climate and Security.

CSE. 2020. *National Cyber Threat Assessment.* Ottawa, ON: Canadian Centre for Cyber Security. https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf.

CSIS. 2021. *CSIS Public Report 2020*. April. Ottawa, ON: Government of Canada. www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report.html.

Dalby, Simon. 2021a. "Canadian National Security Needs an Update for Climate." Opinion, Centre for International Governance Innovation, July 21. www.cigionline.org/articles/national-security-needs-an-update-for-climate/.

———. 2021b. "It's Time to Put Arctic Peoples at the Heart of Arctic Security." Opinion, Centre for International Governance Innovation, October 22. www.cigionline.org/articles/its-time-to-put-arctic-peoples-at-the-heart-of-arctic-security/.

Dalby, Simon and Leah Lawrence. 2021. *Climate Change Impacts on Canadian National Security*. Reimagining a Canadian National Security Strategy Report No. 5. Waterloo, ON: CIGI. www.cigionline.org/publications/climate-change-impacts-on-canadian-national-security/.

Department of Defense, Office of the Undersecretary for Policy (Strategy, Plans, and Capabilities). 2021. *Department of Defense Climate Risk Analysis.* Report Submitted to National Security Council. https://media.defense.gov/2021/Oct/21/2002877353/-1/-1/0/DOD-CLIMATE-RISK-ANALYSIS-FINAL.PDF.

Desai, Neil and Cathy Munroe. 2021. *Borders and the New Geopolitics.* Reimagining a Canadian National Security Strategy Report No. 7. Waterloo, ON: CIGI. www.cigionline.org/publications/borders-and-the-new-geopolitics/.

Economist Intelligence Unit. 2021. *Democracy Index 2020: In Sickness and in Health?* www.eiu.com/n/campaigns/democracy-index-2020/.

Forcese, Craig and Leah West. 2021. *National Security Law: Canadian Practice in International Perspective.* 2nd ed. Toronto, ON: Irwin Law.

Freedom House. 2021. "Freedom in the World 2021: Democracy under Siege." https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege.

Fukuyama, Francis. 1989. "The End of History?" *The National Interest* 16: 3–18. www.jstor.org/stable/24027184.

Gould Stephen, Jay. 2002. *The Structure of Evolutionary Theory*. Cambridge, MA: Belknap Press.

———. 2007. *Punctuated Equilibrium*. Cambridge, MA: Harvard University Press.

Government of Canada. 2021. "Guidelines on the National Security Review of Investments." March 24. www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html.

Innovation, Science and Economic Development Canada. 2021. "National Security Guidelines for Research Partnerships." https://science.gc.ca/eic/site/063.nsf/eng/h_98257.html.

Katz, Brian. 2021. *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation*. Washington, DC: Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

Levy, Adrian R. 2021. *After COVID: Global Pandemics and Canada's Biosecurity Strategy*. Reimagining a Canadian National Security Strategy Series Report No. 5. Waterloo, ON: CIGI. www.cigionline.org/publications/after-covid-global-pandemics-and-canadas-biosecurity-strategy/.

Levy, Adrian and Wesley Wark. 2021. "Opinion: The failure of Canada's pandemic early warning system — and how to fix it." *National Post*, July 28. https://nationalpost.com/opinion/opinion-the-failure-of-canadas-pandemic-early-warning-system-and-how-to-fix-it.

Liberal Party of Canada. 2021. *Forward for Everyone*. https://liberal.ca/wp-content/uploads/sites/292/2021/09/Platform-Forward-For-Everyone.pdf.

Momani, Bessma. 2021. *International Security: Canada's Role in Meeting Global Threats*. Reimagining a Canadian National Security Strategy Series Report No. 4. Waterloo, ON: CIGI. www.cigionline.org/publications/international-security-canadas-role-in-meeting-global-threats/.

National Intelligence Council. 2021. "National Intelligence Estimate: Climate Change and International Responses Increasing Challenges to US National Security Through 2040." www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf.

National Security Commission on Artificial Intelligence. 2021. *Final Report*. www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

NSICOP. 2019. *Annual Report 2018*. Ottawa, ON: Government of Canada. www.nsicop-cpsnr.ca/reports/rp-2019-04-09/2019-04-09_annual_report_2018_public_en.pdf.

———. 2021. *Annual Report 2020*. Ottawa, ON: Government of Canada. www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-en.html.

NSIRA. 2020. *2019 Annual Report*. Ottawa, ON: Government of Canada. www.nsira-ossnr.gc.ca/wp-content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf.

Office of the Auditor General of Canada. 2021. *Pandemic Preparedness, Surveillance and Border Control Measures*. COVID-19 Pandemic Report 8. www.oag-bvg.gc.ca/internet/English/parl_oag_202103_03_e_43785.html.

Office of the Director of National Intelligence. 2021. *Updated Assessment on COVID-19 Origins*. October. www.dni.gov/files/ODNI/documents/assessments/Declassified-Assessment-on-COVID-19-Origins.pdf.

Office of the Intelligence Commissioner. 2021. *ICO Annual Report 2020*. Ottawa, ON: Government of Canada. www.canada.ca/content/dam/oic-bcr/documents/Annual-Report-2020-ICO.pdf.

Office of the Prime Minister of Canada. 2018. "Prime Minister announces changes to the Cabinet Committees." August 28. https://pm.gc.ca/en/news/news-releases/2018/08/28/prime-minister-announces-changes-cabinet-committees.

Ostry, Sylvia and Richard R. Nelson. 1995. *Techno-Nationalism and Techno-Globalism: Conflict and Cooperation*. Washington, DC: Brookings Institution Press.

Permanent Representation of France to the Conference on Disarmament. 2018. "Joint Statement on the Salisbury Attack." https://cd-geneve.delegfrance.org/Joint-Statement-on-the-Salisbury-Attack.

Prime Minister of Canada. 2021. "Strengthening Transatlantic Defence and Security." June 14. https://pm.gc.ca/en/news/backgrounders/2021/06/14/strengthening-transatlantic-defence-and-security.

Privy Council Office. 2004. *Securing an Open Society: Canada's National Security Policy*. Ottawa, ON: Government of Canada. https://publications.gc.ca/site/eng/9.665565/publication.html.

Public Safety Canada. 2020. *National Security Transparency Advisory Group Initial Report: What We Heard in Our First Year*. November 25. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2020-nstag-irwwh/2020-nstag-irwwh-en.pdf.

———. 2021a. "Economic-Based Threats to National Security." February 11.

———. 2021b. *The Definition, Measurement and Institutionalization of Transparency in National Security*. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-dntn-msrmnt-trsprncy-ns/index-en.aspx.

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.

Roach, Kent. 2021. *Ensuring Democracy while Protecting Canadian National Security*. Reimagining a Canadian National Security Strategy Report No. 1. Waterloo, ON: CIGI. www.cigionline.org/publications/ensuring-democracy-while-protecting-canadian-national-security/.

Sanger, David E. 2018. *The Perfect Weapon*. New York, NY: Broadway Books.

Segal, Hugh and Ann Fitz-Gerald. 2021. *Emerging Security Challenges for Canada in the Coming Decade*. Reimagining a Canadian National Security Strategy Report No. 3. Waterloo, ON: CIGI. www.cigionline.org/publications/emerging-security-challenges-for-canada-in-the-coming-decade/.

Therrien, Daniel. 2021. "Strengthening National Security and Privacy in the Digital Era." Speech, October 14. www.cigionline.org/multimedia-series/speaker-series/strengthening-national-security-and-privacy-in-the-digital-era-a-discussion-with-privacy-commissioner-of-canada-daniel-therrien/.

The White House. 2018. *National Cyber Strategy of the United States of America*. September. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

———. 2021a. *Report on the Impact of Climate Change on Migration*. October. Washington, DC: The White House. www.whitehouse.gov/wp-content/uploads/2021/10/Report-on-the-Impact-of-Climate-Change-on-Migration.pdf.

———. 2021b. "Quad Leaders' Joint Statement: 'The Spirit of the Quad.'" March 12. www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/quad-leaders-joint-statement-the-spirit-of-the-quad/.

———. 2021c. "Joint Leaders Statement on AUKUS." September 15. www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/.

United Nations General Assembly. 2021. "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security." July 14. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

Vigneault, David. 2021. "Remarks by Director David Vigneault to the Centre for International Governance Innovation." February 9. www.canada.ca/en/security-intelligence-service/news/2021/02/remarks-by-director-david-vigneault-to-the-centre-for-international-governance-innovation.html.

Wark, Wesley. 2020. "The System Was Not Blinking Red: Intelligence, Early Warning and Risk Assessment in a Pandemic Crisis." Security, Intelligence and the Global Health Crisis Essay Series, Centre for International Governance Innovation, August 24. www.cigionline.org/articles/system-was-not-blinking-red-intelligence-early-warning-and-risk-assessment-pandemic-crisis/.

———. 2021a. "Pandemic Warnings: Taking Stock of the Canadian Military's Flawed Early Intelligence." Opinion, Centre for International Governance Innovation, October 27. www.cigionline.org/articles/pandemic-warnings-taking-stock-of-the-canadian-militarys-flawed-early-intelligence/.

———. 2021b. "Canada Made a Commitment to National Security Transparency. What Did It Change?" Opinion, Centre for International Governance Innovation, January 25. www.cigionline.org/articles/canada-made-commitment-national-security-transparency-what-did-it-change/.

———. 2021c. "Parliamentarians have undermined their own security and intelligence committee." *The Globe and Mail*, June 22. www.theglobeandmail.com/opinion/article-parliamentarians-have-undermined-their-own-security-and-intelligence/.

Wark, Wesley and Aaron Shull. 2021. "National security threats are changing, but Canada is mired in conventional thinking." CBC News, April 30. www.cbc.ca/news/opinion/opinion-national-security-1.6003674.

Acronyms and Abbreviations

AI	artificial intelligence
COVID-19	coronavirus disease 2019
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
EDT	emerging and disruptive technology
GGE	Group of Governmental Experts
IC	intelligence commissioner
ICA	Investment Canada Act
ICT	information communication technology
IMVE	ideologically motivated violent extremism
IoT	Internet of Things
IP	intellectual property
IRG	Incident Response Group
NIE	National Intelligence Estimate
NSC	National Security Council
NSIA	national security and intelligence advisor
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
NSTC	National Security Transparency Commitment
OSINT	open-source intelligence
PHAC	Public Health Agency of Canada

Centre for International
Governance Innovation

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