MAY 2022

A National Security Strategy for the 2020s

Report of the Task Force on National Security, Graduate School of Public and International Affairs, University of Ottawa

DIRECTORS Vincent Rigby and Thomas Juneau

MEMBERS Margaret Bloodworth, Kerry Buck, Ward Elcock, Dick Fadden, Masud Husain, Daniel Jean, Margaret McCuaig Johnston, John McNee, Roland Paris, Morris Rosenberg and Nada Semaan

EDITOR Madelaine Drohan

uOttawa

ÉSAPI GSPIA

A national security strategy for the 2020s

How Canada can adapt to a deteriorating security environment

A report by the Task Force on National Security of the Graduate School of Public and International Affairs (GSPIA) at the University of Ottawa

Project directors: Vincent Rigby and Thomas Juneau

Editor: Madelaine Drohan

Task Force members: Margaret Bloodworth, Kerry Buck, Ward Elcock, Dick Fadden, Masud Husain, Daniel Jean, Margaret McCuaig-Johnston, John McNee, Roland Paris, Morris Rosenberg, Nada Semaan

May 2022

This report was prepared in collaboration with a group of experts involved with the Graduate School of Public and International Affairs at the University of Ottawa. They include the director of the school, Professor Roland Paris, current senior fellows, and former senior fellows. All have significant experience in government, having served in the most senior positions in the national security, intelligence, foreign affairs, and defence communities. See the annex at the end of the report for their biographies. The project directors also interviewed, on background, several serving senior members of the national security and intelligence community.

Task force members contributed their views and expertise, and are generally in agreement with the key elements of this report. They do not necessarily agree with every aspect of it.

We are grateful for the financial support we received from the Alex Trebek Forum for Dialogue in the preparation of this report. We are also grateful to Fernando Aguilar, a student with the Graduate School of Public and International Affairs at the University of Ottawa, for his valuable research and logistical support.

Executive summary

- We are living in a time of intense global instability when the security of Canada and other liberal democracies is under growing threat. An increasingly aggressive Russia is only one of a series of threats, both old and new, that endanger national security in Canada. It exemplifies the worrying re-emergence of great-power rivalry. It also interacts with or amplifies other threats, such as the use of new technologies to wage cyber-warfare, an increase in ideological extremism at home and abroad, attacks on democratic institutions, and transnational threats such as climate change and pandemics. We witnessed a different constellation of such threats in the protests that blocked border crossings and disrupted Canada's capital in early 2022. Where once the state was the focus of these threats, individuals and societies have also become targets.

- When these and other threats reach the scale and potential to endanger what matters most to us as a country – our people, our democratic values and institutions, our economy, our society, and our sovereignty – Canadians expect their government to protect them. Yet Canadians and their governments rarely take national security seriously. Taking shelter under the American umbrella has worked well for us. This has made us complacent and paved the way for our neglect of national security.

- Our peers, including our partners in the Five Eyes partnership (Australia, New Zealand, the United Kingdom, and the United States) are reacting to this rapidly changing situation by revamping policies, identifying new tools and authorities, reforming institutions, devoting new resources to security, and seeking new partners. They possess not only a deeper appreciation of the threats facing the West but also a more sophisticated national security culture writ large.

- In this report, we make the case that Canada is not ready to face this new world. As a country, we urgently need to rethink national security. We identify those threats that are truly matters of national security, and we recommend how best to fill the most glaring gaps. Our core recommendations do not require massive amounts of new spending. Rather, they focus on making better use of tools we already have and improving co-operation among key partners. And they deliver the underlying message that governments must have the courage to look at national security issues beyond today's news cycle or the next election.

- We separate our recommendations into four broad categories:

    1. *Develop new strategies*: Canada needs a national security strategy that reflects today's realities. We can no longer count on some of the traditional pillars that have guaranteed our security and prosperity for decades. The rules-based international order is under severe stress. Yet a strategy by itself is meaningless unless politicians pay more deliberate attention to these issues. That is why the essential first step is to hold a public review of national security. A thorough and transparent review would help inform the public, highlight priorities, identify the policies and tools required to address them, and point to the required changes to governance. In reviewing its national security strategy, the government should also take a hard look at whether its foreign, defence, and development policies are adequate. This does not mean an isolated update in each case, but a holistic approach that examines all our national security assets in a coordinated fashion.

2. *Strengthen existing tools, create new ones*: Canada must build new tools, and make better use of existing ones, to deal with this diversifying and intensifying range of threats. More specifically, we believe that Canada should invest more in the following areas: sharing information within government, sharing information with other levels of government, reviewing outdated legislation, enhancing the use of open-source intelligence, strengthening cyber security, protecting economic security, guarding against foreign interference, and deterring organized crime and money laundering.

3. *Enhance governance*: Canada needs to rethink its national security governance framework – how decisions are made, policies developed, and information shared. We recommend that the government should establish a body at the cabinet level, chaired by the prime minister, with responsibility for national security. It should review the roles and resources of the national security and intelligence advisor to the prime minister and establish a strong central assessment function serving under that position. In addition, we make a number of recommendations to address human resources challenges in the national security community.

4. *Increase transparency and engagement*: Many Canadians today mistrust government. This has major implications for national security. This erosion of trust opens space for misinformation and disinformation to spread; this weakens democratic institutions and contributes to a vacuum that hostile actors do not hesitate to fill. In this context, the national security community's tradition of secrecy is outdated and counterproductive. As such, we strongly recommend that the national security community's recent engagement efforts be significantly ramped up, both with the public – with civil society, the private sector, the media and academia – as well as with Parliament. The community, moreover, must continue and intensify its efforts to increase diversity within its ranks.

- In drafting this report, we have relied on a group of advisors with first-hand experience in addressing national security issues. Some are former national security advisors to the Prime Minister, CSIS directors, deputy ministers of national defence or foreign affairs, and ambassadors. Others worked in senior positions throughout the security and intelligence community. Still others have expertise in border security, global financial flows, national defence, and foreign policy. All are associated with the Graduate School for Public and International Affairs at the University of Ottawa. Our goal is to leverage our combined expertise to raise awareness of these issues.

A NATIONAL SECURITY STRATEGY FOR THE 2020S

HOW CANADA CAN ADAPT TO A DETERIORATING SECURITY ENVIRONMENT

We are living in a time of intense global instability when the security of Canada and other liberal democracies is under growing threat. Russia's brutal invasion of Ukraine in early 2022, with its deliberate targeting of civilians and underlying threat of nuclear war, has jolted even the most sanguine of western democracies into thinking anew about security. Ahead lies a period of escalating tensions with no clear end in sight.

An increasingly aggressive Russia is only one of a series of threats, both old and new, that endanger national security in Canada. It exemplifies the worrying re-emergence of great-power rivalry. It also interacts with or amplifies other threats, such as the use of new technologies to wage cyber-warfare, an increase in ideological extremism at home and abroad, attacks on democratic institutions, and transnational threats such as climate change and pandemics. We witnessed a different constellation of such threats in the protests that blocked border crossings and disrupted Canada's capital in early 2022.

When these and other threats reach the scale and potential to endanger what matters most to us as a country – our people, our democratic values and institutions, our economy, our society, and our sovereignty – Canadians expect their government to protect them.

Yet Canadians and their governments rarely take national security seriously. This has led to reactive policies and widespread complacency. Canada's position on national security seems little changed since 1924, when Senator Raoul Dandurand told an international gathering that Canadians "live in a fireproof house far from inflammable materials." Our history and geography created and then reinforced this attitude. Since the start of European settlement, Canadians have relied on others – first France, then Britain, now the United States – for protection. Taking shelter under the American umbrella has worked well for us. We have not experienced a direct violent attack against out citizens in recent memory on the same scale as some of our allies, with the last major one being the Air India attack of 1985. This has made us complacent and paved the way for our neglect of national security.

Even before the first Russian tanks rolled across the border into Ukraine in February 2022, it was clear that our traditional approach to national security was no longer sustainable. Since Canada last reviewed its national security policy in 2004, the world has been destabilized by the worst pandemic in a century and the sharpest economic slowdown since the Great Depression. A polarized United States has become a less predictable partner in recent years. Barriers are growing to the movement of people, goods, and ideas. Authoritarianism is on the march. Russia is not the only powerful country threatening its neighbours. China is doing the same in its neighbourhood and further afield. On top of this, we face a host of non-traditional actors and threats. Where once the state was the focus of these threats, moreover, individuals and societies have also become targets.

Our peers, including our partners in the Five Eyes partnership (Australia, New Zealand, the United Kingdom, and the United States) are revamping policies, identifying new tools and

authorities, reforming institutions, devoting new resources to security, and seeking new partnerships. They possess not only a deeper appreciation of the threats facing the West but also a more sophisticated national security culture.

Canada, however, has failed to act. It has been over 15 years since we produced a national security or foreign policy statement. We have not seriously reviewed the *Canadian Security Intelligence Service Act* since CSIS was established in 1984. And we are falling behind our allies in taking practical, concrete steps to address national security threats.

In this report, we make the case that Canada is not ready to face this new world. As a country, we urgently need to rethink national security. What follows is not a catalogue of every threat facing Canadians. Rather, it is an attempt to identify those that are particularly severe, or new and different, and require a change in policy or practice. We identify those that are truly matters of national security, and recommend how best to fill the most glaring gaps. Our core recommendations do not require large amounts of new spending. Rather, they focus on making better use of tools we already have and improving co-operation among key partners. And they deliver the underlying message that governments must have the courage to look at national security beyond today's news cycle or the next election and make long-term investments that will protect Canadians now and many years into the future.

In drafting this report, we have relied on a group of advisors with first-hand experience in addressing national security issues. Some are former national security advisors to the prime minister, directors of the Canadian Security Intelligence Service, deputy ministers of national defence or foreign affairs, and ambassadors. Others worked in senior positions throughout the security and intelligence community. Still others have expertise in border security or global financial flows. All are associated with the Graduate School of Public and International Affairs at the University of Ottawa. Our goal is to leverage our combined expertise to raise awareness of these issues.

NATIONAL SECURITY TODAY

Not every problem is a matter of national security. When the federal government applies that label, it can invoke extraordinary and intrusive powers. As such, some matters are best dealt with outside the realm of national security, by departments not in the core security and intelligence community, other levels of government, the private sector, or civil society.

Defining what is a matter of national security has become more difficult as threats proliferate. A definition that attempts to cover the current array of threats risks becoming so broad that it includes everything and is meaningless. It also leads to national security imperialism, where everything and anything falls into its ambit and national security becomes *the* driver of government policy rather than *a* driver. At the other extreme, a definition that limits itself to traditional threats fails to keep up with the evolving environment.

At the most general level, a matter involves national security when it threatens Canadians, their democratic values and institutions, their economy, their society and their sovereignty. However, scale is important. The hack of a home computer threatens one household's privacy and financial security. Successful cyber-attacks on the country's key financial institutions pose a national threat. It is only when the potential impact of a threat exceeds a certain threshold that it demands a national response. The potential evolution of a threat is also important. There are issues that do not start as national security concerns but develop in that direction over time. The COVID-19 pandemic was not a national security issue in its earliest form, but became one as its health, economic, social, and geo-political implications grew more pronounced. Defining threats to national security must therefore be done on a case-by-case basis.

We use the following definition: national security deals with threats to the people, democratic values and institutions, economy, society, and sovereignty of Canada on a scale that demands a national response.

THE THREAT ENVIRONMENT

There are any number of ways to think about the threats that confront Canadians. We can consider them in terms of the intended target. In the past, national security threats tended to be directed primarily against federal and national institutions. Current threats, however, also impact individuals as well as a broader range of institutions, public and private, to an extent we have not seen before. Espionage targeting universities and research institutions and cyber-attacks against companies or individual Canadians are examples. We can also think of them in terms of the source. Some emerge from states, others from non-state actors such as terrorist or criminal networks. Or we can think of threats in terms of the time frame. Some pose an immediate danger, such as the COVID-19 pandemic. Others pose a longer-term danger, such as the melting of polar ice.

In this report, we focus primarily on the threats that are different from what we have dealt with in the past or are particularly alarming. What is especially concerning is how these threats reinforce each other. They are not isolated: responding to one – or failing to respond – will inevitably have a positive or negative ripple effect on others.

Great-power rivalry

The Russian invasion of Ukraine underscores the new reality of heightened geopolitical competition in an increasingly multipolar world. Even before its invasion of Ukraine, it was clear that a revanchist Russia was determined to play a disruptive role internationally through its efforts to undermine democratic elections and spread disinformation. But in the space of several weeks, the global security environment has been transformed. Moscow's recent actions pose a direct threat to Western interests and values and call for increased vigilance on the part of the members of the North Atlantic Treaty Organization (NATO) and other countries. Canada and its allies must seriously review their military capabilities and be prepared to resist further Russian aggression, whether in eastern Europe or the Arctic. We have no choice but to adapt to this new reality. Russia's increasing co-operation with China in recent years only exacerbates an already dangerous situation.

While western democracies are focussed on Ukraine, they are aware that China poses potentially a more serious, long-term challenge. Its political, economic, military, and technological ascendance over the last three decades has been the defining element in a changing geopolitical landscape. Over the last ten years in particular, China has become much more assertive in its region and beyond. It has expanded its power and influence, including with the Belt and Road Initiative, its global infrastructure development strategy, and actively attempts to undermine its competitors. China is watching developments in Ukraine closely as it continues to pursue its interests at the expense of the West.

China and Russia will continue to pose a significant threat to Canada through their foreign interference, disinformation, espionage, hostage diplomacy, and cyber-attacks. These activities directly threaten government institutions, but also individuals, businesses, universities, and research institutions. They reach into our homes through the intimidation of citizens who have come to Canada to escape tyranny. This is antithetical to their rights to live and speak freely, and their ability to contribute to the richness of public life. These governments have attempted to interfere in our elections by targeting, through social media, those who speak out against their interests. Such actions undermine our democracy. Our lack

of a firm response, moreover, presents a serious risk for our allies, and could affect our security and intelligence relations with them.

Revisionist or aggressive regional powers, especially adversaries such as Iran and North Korea but also allies and partners such as Turkey, Saudi Arabia, and India, are also engaged in a range of hostile activities that threaten Canadian interests at home and abroad, notably by intimidating members of their diaspora. Even though they do not have the means comparable to Russia and China to harm Canada, we must take their attacks on the Canadian government, the private sector, and civil society more seriously.

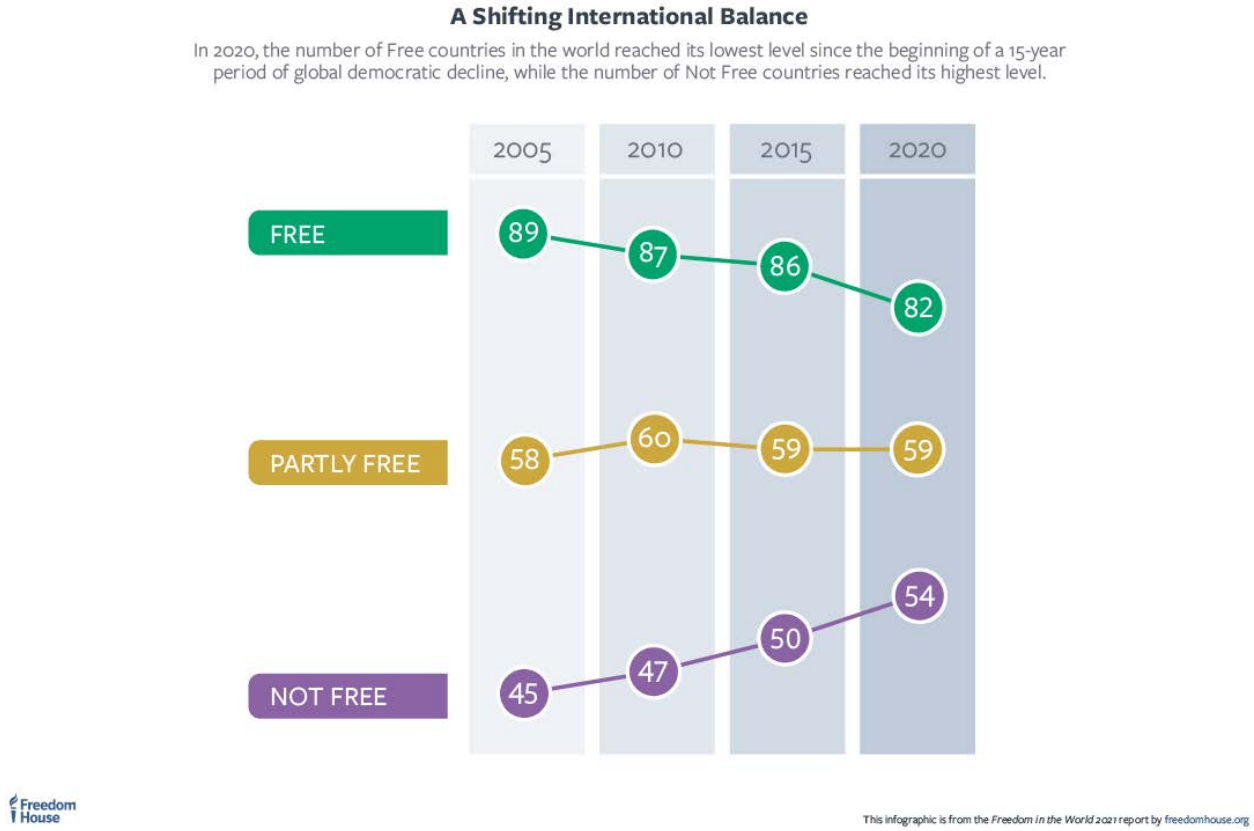
In this shifting international context, Canada has a strong interest in preserving the rules-based international order because we benefit from the collective security and prosperity that derive from it. Yet as this order weakens and is replaced by a less predictable, more power-based order, Canada faces difficult questions. Preserving our national security and protecting our interests means that we must develop stronger and more coherent strategies covering foreign policy, defence, and development that complement those at home. Domestic and international security are two sides of the same coin.

Democracy under siege

We are witnessing a renewed contest of ideologies, pitting liberal democracy against autocracy, which contributes to the further erosion of the rules-based international order. Liberal democracy is increasingly being challenged by authoritarian governments who seek to weaken the rule of law, open trade, multilateralism, and human rights. According to Freedom House, an American non-governmental organization, the number of free countries in the world dropped to 82 in 2020 from 89 in 2005, whereas the number of countries described as not free rose to 54 in 2020 from 45 in 2005. For Canada, such developments are especially concerning because they are occurring not only in states such as Hungary, Turkey, Poland, and Brazil, but also in the United States.

Liberal democracies are also being challenged from within, often as the result of the increased polarization of society driven by a range of grievances and fuelled by disinformation. The protests in Ottawa and the border towns of Windsor, Ontario, Emerson, Manitoba, and Coutts, Alberta, in early 2022 were a disturbing taste of the harm a small group of determined protestors could inflict on people and the economy. They were also an example of other trends we highlight in this report. The protestors were non-state actors, some of whom advocated for the overthrow of the democratically elected government. In Coutts, there were indications that organized criminal groups had infiltrated the protest. The protest leaders used social media to coordinate their actions and communicate with their followers. The protests also involved widespread intimidation of the media, discouraging objective coverage of the insurrection.

It also quickly became apparent that there were ties between far-right extremists in Canada and the United States. There was, moreover, open support from conservative media, including Fox News, and conservative politicians in the United States. This may not have represented foreign interference in the conventional sense since it was not the result of actions of a foreign government. But it did represent, arguably, a greater threat to Canadian democracy than the actions of any state other than the United States. It will be a significant challenge for our national security and intelligence agencies to monitor this threat, since it emanates from the same country that is by far our greatest source of intelligence.



Source: https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege

On the response side, the lack of coordination among levels of government prolonged the protests and further eroded trust in authorities. And while the stated target was the federal government, it was the people living in the immediate vicinity of the protests in the case of Ottawa, and the businesses dependent on cross-border trade in the cases of Windsor, Emerson, and Coutts, who suffered the harm. In the end, the protests did not amount to a major national security crisis. But they highlighted significant vulnerabilities. We would argue that we are not sufficiently prepared for a worse scenario down the road.

The protests also pointed to a broader and potentially existential question for Canada: the implications of democratic backsliding in the United States. Should scenarios of widespread political violence in our southern neighbour materialize, how should Canada respond? This question would have been fanciful only a few years ago, but it is very real today. Growing American trade protectionism also poses a serious threat to the Canadian economy, which remains highly dependent on exports to the United States, with little prospect for diversification. An increasingly unpredictable and unilateral United States – especially if Donald Trump, or a like-minded Republican, wins the presidency in 2024 – could raise difficult questions. The United States is and will remain our closest ally, but it could also become a source of threat and instability.

Transnational challenges

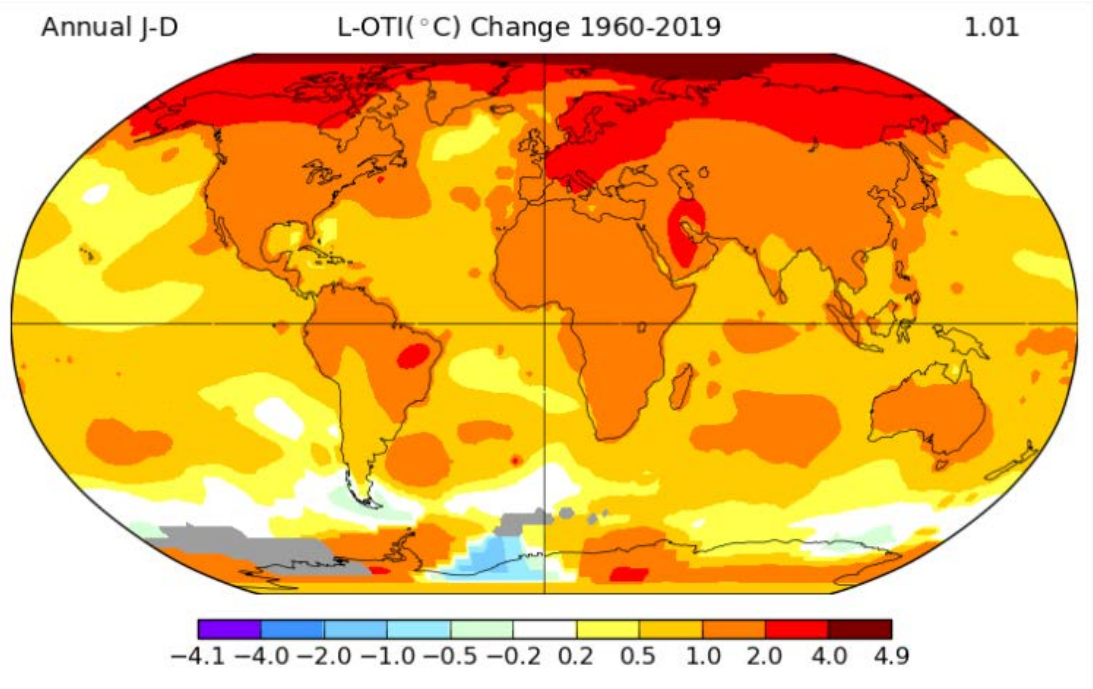
Transnational phenomena such as pandemics and climate change are primarily public health and environmental issues respectively, but they also carry important national security implications when their impact exceeds a threshold. They can also act as catalysts for many of the other threats we discuss in this report.

The COVID-19 pandemic has shown how this can be the case. We have already seen its immediate impact in the daily toll of cases and lives lost. As of early April 2022, COVID has killed almost 38,000 Canadians (and possibly as many as 20 million worldwide) and disrupted virtually every aspect of our society and economy. We are also seeing growing secondary impacts. It has increased social and political tensions and emboldened extremists, as witnessed by the protests in Ottawa and elsewhere in February. They were ostensibly about public health measures, but this stated motivation masked a host of other grievances. Internationally, the pandemic has heightened geopolitical competition, made the Canadian pharmaceutical sector more vulnerable to espionage by hostile states, and contributed to the radicalization of certain groups. Global health security will continue to be a key concern beyond the current pandemic. Changes in human activity, including mass displacement and migration, coupled with the effects of climate change, will create conditions favoring the emergence of new diseases.

Climate change threatens the security of Canadians. Past and future warming in Canada is, on average, about double the magnitude of global warming. A warmer climate will intensify weather extremes, meaning more heatwaves and increased drought, wildfires, and urban floods. It will put stress on critical infrastructure and emergency responders, while increasing the demands on the Canadian Armed Forces to assist civil authorities. It is already causing changes in the Arctic, threatening the livelihoods of some of the people who live there.

Internationally, threats to our security will increase as Canadian areas of the Arctic experience longer and more widespread ice-free conditions. Reduced ice cover will fuel competition over navigable waterways, energy resources, and mineral deposits. It will also have a geopolitical dimension. Russia and China are investing in their Arctic capabilities and will increasingly engage in the theft of intellectual property of critical technologies to adapt to climate change. The American insistence, over the objections of Canada, that the Northwest Passage is an international waterway works to the benefit of countries like China and Russia, which can exploit this opening. The Brookings Institution wrote in a 2021 report that China has established science and satellite facilities in Norway, Iceland, and Sweden, and that Chinese companies have pursued infrastructure projects that could have a military use in Greenland, Scandinavia, and Russia. China is adding to its fleet a third heavy icebreaker and a vessel capable of salvaging or rescuing vessels in the Arctic. Russia has long outpaced Canada in developing its Arctic region, including through the establishment of military bases, and is adding at least five nuclear-powered heavy icebreakers to its sizeable fleet. Given its invasion of Ukraine, Russia may well be considering further military steps in the Arctic.

These developments call for a serious review by Canada of its presence in the Arctic, including its military footprint and capabilities, which have received scant attention over the decades despite considerable government rhetoric to the contrary. The government's announcement in its 2022 budget that it is considering options to fulfil its commitment to modernize the North American Aerospace Defense Command (NORAD) through significant investments is welcome news in this regard, but it must be expedited. This upgrade is long overdue but will not be enough on its own to defend against emerging threats in the north.



Source: https://nsidc.org/cryosphere/arctic-meteorology/climate_change.html

Violent extremism and organized crime

Ideologically motivated violent extremism poses a growing threat to Canadian national security. The disruptive protests in Ottawa, Windsor, Emerson, and Coutts in early 2022 validated concerns that experts had been voicing for years. Cases are mounting of threats directed at Canadian politicians, officials, and vulnerable groups. Individuals and groups who adhere to a diffuse range of violent, far-right ideologies have become better organized and emboldened in the wake of the events of early 2022. They have developed or increased ties to like-minded actors in the United States and elsewhere. Whether anti-government, antisemitic, Islamophobic, anti-Asian, or misogynistic in nature, these groups reflect global trends that must be addressed at their roots. Closer co-operation between national security organizations and social actors in the public policy realm is necessary.

Foreign-based, religiously motivated, violent extremist groups, especially the Islamic State and al-Qaeda, have not disappeared. Though diminished, they maintain global networks and the ambition and possibly the ability to strike Western, including Canadian, interests. As we shift more attention and resources to far-right extremists, we cannot turn a blind eye to these groups.

Transnational organized crime is another enduring concern, made worse when it intersects with some of the trends noted here. Criminal activity normally does not fall in the realm of national security unless it crosses a certain threshold. Until that point, it usually remains a policing issue. Nevertheless, transnational organized crime distorts the global economy and enables corruption, notably through money-laundering practices, and can thus undermine democratic institutions and the rule of law. Organized crime also corrupts or undermines legitimate activities and institutions when it moves into areas like construction or political

financing. Organized crime can pose a distinct threat, or it can work in combination with other threats. An example of the latter is when there is collusion between criminal groups and a state such as Russia.

New technologies, new vulnerabilities

Technology has the potential to improve the lives of Canadians. But new technologies can also be a threat, or they can exacerbate other threats. For example, the use of new technologies by the leaders of the protests in early 2022 increased the threat of ideological extremism by allowing them to communicate with their followers and coordinate their actions. At the international level, rising geopolitical competition is driving a science-and-technology contest between states.

The objective for democracies is to keep a comparative advantage, as competitors attempt to use their technological and economic levers against us. It seems not a day goes by without a story about the use of technology by malicious actors, notably through cyber-attacks on critical infrastructure such as the banking system, hospitals, or the power grid. Technology also allows extremists from across the ideological spectrum to generate and spread hateful propaganda and conspiracy theories. Emerging technologies, such as artificial intelligence, including machine learning, as well as new weapons systems and quantum computing, deepen threats posed by hostile states or criminals. Much of the debate in Canada has focussed on 5G and the use of Huawei technology, leaving threats posed by these other powerful new technologies often unexamined.

This puts researchers and innovators in the private and public sectors in the crosshairs. We have seen strategic investments in sensitive sectors in Canada by companies who obfuscate their state ties. We have also seen the theft of intellectual property to advance the interests of foreign states and state-backed companies at the expense of the legitimate owners of that technology and Canada's economic security. Research collaboration between Canadian and Chinese partners is a case in point. Despite decades of constructive collaboration, there are several risks to partnerships between Canadian and Chinese scientists and engineers. Legislation in China, which combines domestic controls with extraterritorial provisions, obliges Chinese individuals and institutions to support, assist, and co-operate with the Chinese intelligence apparatus. This means that Canadians with Chinese partners could see their innovations supporting, without their knowledge, China's military. This includes partnerships researching artificial intelligence, biotechnology, photonics (the physical science of light waves), quantum computing, and genomics. This is a real risk: Canada's top research universities have some of the most frequent collaborations with China's military universities among institutions worldwide.

POLICY IMPLICATIONS

Canada is simply not ready today to deal with this range of threats. One indication of our unreadiness is that the federal government has not produced a strategic threat assessment for the Canadian public in years. It has not set out an international strategy since 2005. In the absence of a major review, there has been no thorough assessment of national security tools and authorities, and whether we are using existing tools to maximum effect. There was important new legislation in 2019, Bill C-59. It replaced the fragmented system for reviewing national security activities with a more comprehensive one and amended the *Anti-terrorism Act* to better comply with the Canadian Charter of Rights and Freedoms. But it left much uncovered. The *Canadian Security Intelligence Service Act*, for example, has not been thoroughly reviewed since 1984. Internal governance structures are out of step with those of our allies. The federal government needs to improve how it works with other levels of government. Transparency with Canadians has improved but remains far too limited.

This has several implications. It means, first, that more actors need to be involved in national security than has traditionally been the case. Core national security agencies must increasingly work closely with other, non-traditional partners in the federal government, including economic and social departments, but also with partners outside Ottawa, including other levels of government, the private sector, academia, civil society, racialized communities, and allies.

This in turn means much more information sharing – an area in which the national security community has historically not performed well given its deeply entrenched culture of secrecy. There have been improvements within the federal sphere since the Air India disaster in 1985. But much remains to be done. It also means that a more effective and sophisticated coordinating and executive function is necessary at the center of government.

It also underlines the need for more transparency and better public understanding of what is national security. It is not enough for a group of ministers and their departments and agencies to work behind closed doors. The public must be informed and consulted. This means the government must be more open so that Canadians better understand the threat environment.

The bottom line: Canada needs to take national security much more seriously than it has done to date. Collectively, we have neglected national security for decades, largely because we could afford to do so. Shielded from major threats, we generally suffered little or no cost for our complacency. Whenever we dealt with national security issues, it was largely in a reactive way, in response to events, and not through a more proactive, structured approach.

THE WAY AHEAD

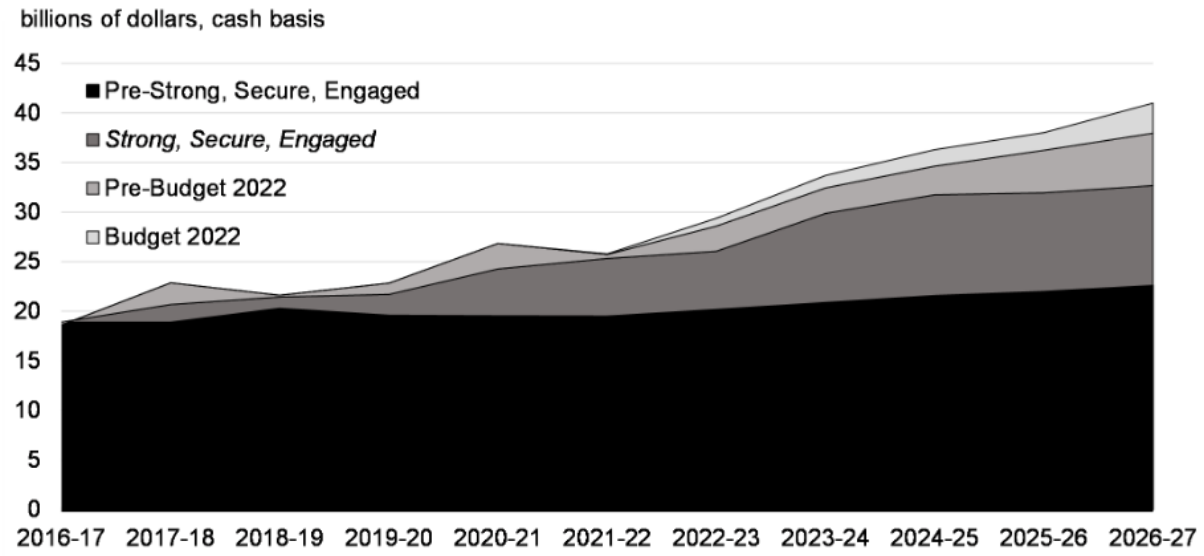
In this section, we offer recommendations for the federal government to address gaps in Canada's ability to address these new and evolving threats. Many of the initiatives we suggest here are cost-free, and others would carry only a limited financial cost. Most, moreover, should be viewed as investments, as society will benefit from their adoption. We organize our recommendations into four categories: the need for Canada to develop forward-looking national security strategies; the need to strengthen existing tools and create new ones; governance; and trust, transparency, and engagement.

Develop new strategies

Canada needs a national security strategy that reflects today's realities. We can no longer count on some of the traditional pillars that have guaranteed our security and prosperity for decades. The rules-based international order and the multilateral system that supports it are under severe stress. Our house is no longer "fireproof".

Yet a strategy by itself is meaningless unless politicians pay more conscious and deliberate attention to these issues and commit to broader and more open engagement. Politicians respond to the concerns of their constituents. That is why the essential first step in readying Canada for this new world is to hold a public review. A thorough and transparent review would help inform the public, highlight priorities, identify the policies and tools required to address them, and point to the required changes to governance. Occasional budget announcements of new, scattered funding for initiatives related to national security will not suffice in the absence of an over-arching strategy.

Funding for the Department of National Defence



Source: https://budget.gc.ca/2022/report-rapport/chap5-en.html#2022-1

One of the underlying assumptions of this review should be that national security does not necessarily differentiate between domestic and international threats. As this report shows, domestic threat actors often have ties internationally, whereas what may seem to be purely international crises can rapidly impact Canada domestically. In this context, even if this report does not focus on defence and foreign policy *per se*, in practice government efforts – or lack thereof – in these realms are closely intertwined with those in the realm of national security. Canada's neglect of foreign and defence policy in recent decades therefore hurts national security. Russia's invasion of Ukraine, for example, has shone a light – again – on the inadequacy of Canada's hard power.

In reviewing its national security strategy, the government should therefore take a hard look at whether its foreign and defence capabilities are adequate, given known and anticipated threats. This does not mean an isolated update of Canada's defence policy, as announced in Budget 2022, but a holistic approach that examines *all* of our national security assets in a coordinated fashion. This includes the issue of defence funding. Should Canada reach, or at least approach, NATO's aspirational target of two percent of GDP committed to defence spending? While such metrics are useful, if politically driven, hard power is not in the end about percentages. The government's recent decision to finally acquire the F-35 fighter aircraft, as well as the budget announcement to spend $6.1 billion over five years to "meet our defence priorities," are welcome. But much more needs to be done urgently.

Recommendations:

- Conduct a thorough *public* review of national security policy. The review should better inform Canadians of the threat environment, expose areas of concern, and suggest policies, authorities, and tools needed to close existing gaps, while remaining faithful to Charter and privacy rights.

- Address, as part of this public review, such national security threats as hostile activities of state actors (e.g., foreign interference, espionage, economic threats), non-state actors (e.g., terrorism and organized crime), cyber-security, pandemics, and climate change. The review should examine how Canada can best respond to these threats, including specific tools (e.g., legislation, authorities, and information and intelligence sharing), governance, and public engagement.

- Explore as part of this process the close connections between national security and foreign policy, defence, and international development. Canada cannot fully protect its citizens at home as long as its ability to protect and advance its interests abroad is inadequate.

- Be more selective when it comes to foreign policy, defence, and international assistance, with fewer, more targeted priorities. Making more meaningful investments in fewer areas would strengthen Canada's ability to pursue its interests.

- Focus, in terms of military and diplomatic tools, on greater Arctic capabilities beyond NORAD modernization (e.g., acceleration of the delivery of Arctic and offshore patrol ships and the construction of the Nanisivik naval station on Baffin Island), increased foreign intelligence capability, enhanced ability to deploy expeditionary forces to foreign trouble-spots, greater co-operation with allies on key security issues (such as joining the Australia/United Kingdom/United States AUKUS pact) and increased support to non-proliferation and arms control initiatives.

- Ensure that a new national security strategy is fully funded from the outset.
- Update this strategy every five years, conducting a full review when circumstances significantly change.

Strengthen existing tools and create new ones

Canada must build new tools, and make better use of existing ones, to deal with this diversifying and intensifying range of threats.

1. **Sharing information within government**

The core security and intelligence community within the public service consists of ten departments and agencies:

Canada Border Services Agency (CBSA)
Canadian Security Intelligence Service (CSIS)
Communications Security Establishment (CSE)
Department of National Defence and the Canadian Armed Forces (DND/CAF)
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
Global Affairs Canada (GAC)
Integrated Terrorism Assessment Centre (ITAC)
Privy Council Office (PCO)
Public Safety Canada (PSC)
Royal Canadian Mounted Police (RCMP)

It is a large community, although not nearly as large as that in the United States. Given the dynamic and global nature of national security challenges we face, national security work can involve virtually every single department across Ottawa on any given day, including:

Agriculture and Agri-Food Canada
Canadian Commercial Corporation
Canadian Heritage
Environment and Climate Change Canada
Finance Canada
Health Canada
Immigration, Refugees and Citizenship Canada
Innovation, Science, and Economic Development Canada
Justice Canada
Natural Resources Canada
Public Health Agency of Canada
Transport Canada

It is crucial that everyone works with the same information to the maximum extent possible. Yet many Canadians would be surprised to realize how difficult and painstaking routine information sharing can be within government. This acts as a major obstacle for intelligence and law enforcement agencies. We should be able to both protect Charter rights and strengthen

our national security at the same time. Yet the debate is too often framed in either/or terms, i.e., that the removal of some of the unnecessary bureaucratic or legislative barriers to effective information sharing would necessarily lead to an erosion of fundamental rights. This is a legitimate concern. Protecting privacy will be even more important as surveillance by public and private actors becomes easier and as they have access to larger databases of people's activities. We believe, however, that it is possible to preserve fundamental rights while improving how we share information. Indeed, the need to defend Canadians' Charter rights from internal and external threats is not separate from national security; it is essential to national security.

Recommendations:

- Ensure that *every* department and agency across the federal government better understands national security and the connection to its work. This starts with ensuring that all relevant information and intelligence, both classified and open source, is shared to the maximum extent possible. At the same time, given the whole-of-government reality of policy making on key files, it is equally essential that core national security and intelligence departments agencies themselves gain a better understanding of the work of the rest of the federal apparatus, notably economic and social departments.

- Overcome cultural barriers to collaboration. These include overclassifying intelligence material and relying excessively on need-to-know distribution.

- Strengthen the connective tissues between departments by improving information-sharing mechanisms. One example would be to invite more departments and agencies to core national security governance bodies (such as the key deputy minister and assistant deputy minister committees) where and when their presence is appropriate.

- Consider the creation of a government-wide, top-secret cloud, as many of our allies have done in various forms, that would include vast amounts of data stored by every department and agency. Each would be responsible for managing the data it would upload, based on respective authorities and responsibilities. This would represent a major improvement over the current system, an ineffective and clunky patchwork that imposes major time and resource obligations on community members.

2. Sharing information with other levels of government

Responding to many of the threats that Canada faces today involves, or should involve, other levels of government as well as the private sector and civil society. Few can be handled by core national security agencies alone. Yet the national security and intelligence community is not used to dealing with other levels of government. Cooperation has increased in recent years, but there remains scope for much improvement. This was illustrated, for example, at the time of the protests in Ottawa, Windsor, Emerson, and Coutts, when the different levels of government struggled to share information and coordinate their work.

Recommendations:

- Normalize national security co-operation with other levels of government. It should be routine, not exceptional.

- Establish permanent mechanisms to share information and coordinate policies and operations between different levels of government. There is a need, in particular, for stronger and broader mechanisms to bring together federal and provincial public safety officials (and these could include, for example, regular intelligence briefings).

- Sponsor security clearances for key individuals at other levels of government, so that a larger number of non-federal officials can receive classified information. In addition, the national security community – notably the Integrated Terrorism Assessment Centre – should prepare more threat assessments and provide advice at lower levels of classification, including at the unclassified level, to ensure that information gets circulated to the widest possible audience beyond the federal government.

3. Reviewing outdated legislation and legal approaches

The *CSIS Act*, passed in 1984, predates the digital revolution. It is not the only piece of legislation that should be modernized, but it is a good example of how our legislation has not kept pace with a changing world. There have been small adjustments. The *Anti-terrorism Act of 2015*, for example, amended the *CSIS Act* to give the Service the mandate to disrupt terror plots while they are being planned, among other things. Beyond CSIS, the National Security and Intelligence Committee of Parliamentarians (NSICOP) was established by legislation in 2017 and given a broad mandate to review all aspects of national security. The *National Security and Intelligence Review Agency Act* of 2019 set up a review body of that name (NSIRA). The *Intelligence Commissioner Act*, also passed in 2019, established an independent intelligence commissioner.

These changes were meant to maintain public confidence in our national security bodies. Yet overall, legislation has not kept up to date with changes in the digital world. As a result, the Federal Court and review bodies must apply a pre-digital legislative lens to a brand-new digital domain. Technological advances have created opportunities for CSIS in intelligence collection, but they also pose new challenges for an aging statute. Information is increasingly stored outside Canada, or in an encrypted format that cannot be readily accessed or used. Jurisprudence, including the evolving privacy landscape, also has an impact on intelligence operations. Old legislation, in sum, limits the ability of CSIS to achieve its mandate – and sometimes prevents it from doing so.

The ability of CSIS to advise its partners and inform decision making, without disclosing its sensitive tradecraft, sources, and methods, remains a major challenge. CSIS uses the intelligence it collects to advise the government and inform its decisions. But in doing so, this intelligence can become subject to disclosure in administrative, civil, or criminal proceedings. This can be a challenge, as the disclosure of sensitive information can sometimes be injurious to national security and damage foreign partnerships. This is a longstanding challenge for CSIS and has often impeded its relations with key partners. CSIS and the RCMP have undertaken initiatives to enhance their operational collaboration, while minimizing such disclosure of sensitive information, but much work remains to be done. CSIS has also been working with the Department of Justice and with Public Safety Canada to develop policy and legislative options to address the dilemma of having intelligence used as evidence in court proceedings.

While we have used the *CSIS Act* to illustrate the problem of outdated legislation not being fit for purpose, the same problem can be found in other legislation, including the *Emergencies*

Act. The public review should study which legislation should be re-examined. It should also look at how to solve the thorny problems of using intelligence as evidence in court cases and gaining lawful access to communications when serious crimes are investigated.

Recommendations:

- Review key legislation related to national security with an eye to determining whether it still serves its intended purpose. This could be done as part of the upcoming, five-year review of Bill C-59. Priority should be given to the *CSIS Act*, the *Emergencies Act* and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* of 2000, which established the financial intelligence unit called the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The protests in Ottawa, Windsor, Emerson, and Coutts revealed that changes were needed to the legislation governing emergencies and proceeds of crime.

- Develop a framework to intercept communications by lawful means in the investigation of serious crimes, such as terrorist plots, drug trafficking, money laundering, smuggling, child pornography, and murder. Such a regime, known as lawful access, must stay true to our values but allow the investigation and prosecution of terrorist and criminal organizations. Civil liberties groups should be actively engaged in the process.

- Develop, in close co-operation with the legal community, a credible regime that allows the use of intelligence as evidence in the prosecution of criminal activities while remaining faithful to the principle of suspects receiving a fair defence. Our inability to develop such a regime for using intelligence as evidence has prevented us from living up to our international commitments and our own domestic imperatives to prosecute people at home.

4. Increasing use of open-source intelligence

More information is available openly today than ever before. Open-source intelligence researchers, for example, have been able to track and analyze with astonishing precision and timeliness the movement of Russian troops before and during the invasion of Ukraine. This holds important lessons for the intelligence community, which still perceives open-source intelligence as inherently less valuable than classified intelligence obtained via clandestine means. The situation has improved in recent years, but as long as the intelligence community fails to maximize its use of open-source intelligence, it ignores valuable data. It also fails to optimally serve its clients. Policy makers will often go to social media for a quick overview of an evolving crisis as opposed to waiting for intelligence analysis to make its way to them through cumbersome approval processes.

One of the key challenges in this area, however, is collection. Who in the government should be responsible for monitoring social media? Different parts of the national security community have the partial mandate to do so. The Rapid Response Mechanism at Global Affairs Canada, for example, monitors and analyzes potential cases of foreign interference, including by observing content shared through social media. But as we saw during the protests across Canada in early 2022, when protest organizers were openly telegraphing their intent on various social media platforms, government mandates are strictly limited. This impedes, and sometimes prevents, the ability of national security agencies to do their work. To provide another

example, interference by China in a recent election in British Columbia happened extensively on WeChat, a social media platform. Intelligence and law enforcement agencies should be able to monitor this activity, while protecting Charter and other fundamental rights. This is a delicate balance that is difficult to manage.

The paradox for the intelligence community is that it will be criticized for scrutinizing the social media posts of Canadians, but also for failing to do so and missing warning signs of impending threats. If we agree that Canadians must be protected, but not at the expense of their Charter rights, it begs a fundamental question: where should such a capability be housed, and under what authorities? In the absence of an adequate answer to this question, vulnerable people – such as Chinese-Canadians – remain victims, and threats go unaddressed.

Recommendations:

- Devote greater resources to open-source intelligence throughout the national security community. Gathering and analysing open-source intelligence and then incorporating it into the broader intelligence collection and analysis process is complex. It requires specific skillsets, which despite recent improvements, are often lacking. This requires the hiring of analysts with the necessary skills (e.g., imagery analysis) as well as a broader cultural change, to move analysts away from a mindset that still often perceives such intelligence as inferior to classified intelligence.

- Explore the establishment of a stand-alone unit that collects and analyzes open-source intelligence, as some of our allies have done. While every department and agency should boost its capabilities in this domain, there should also be a centre of excellence with the mandate to research social media postings internationally but also by Canadians, while respecting their privacy and Charter rights. One option would be for this unit to be housed in Public Safety Canada, perhaps alongside the Canada Centre for Community Engagement and Prevention of Violence. The unit should be at arms-length from the intelligence community, to ensure that appropriate safeguards are in place, but still connected with it and the rest of the government, including departments such as Canadian Heritage (which has an interest in the spread of online hate). The announcement in Budget 2022 to provide $10 million over five years to the Privy Council Office to "coordinate, develop, and implement government-wide measures designed to combat disinformation and protect our democracy" may go some way towards achieving this objective, though more detail is required.

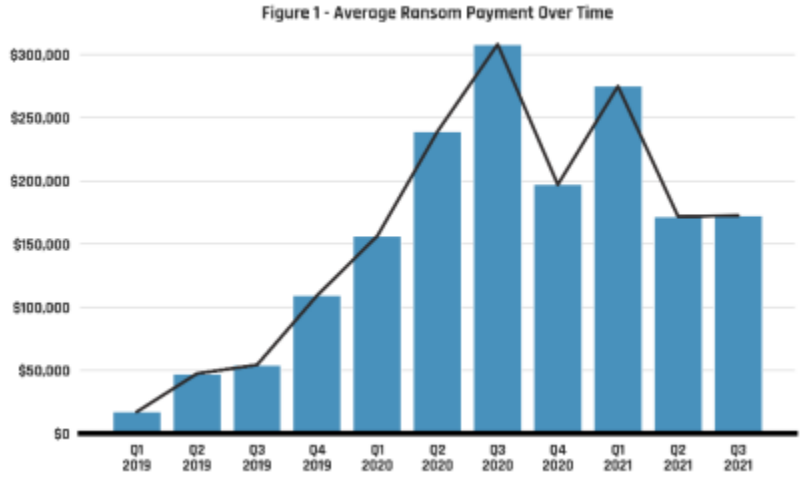
- Better leverage the vast amounts of diplomatic reporting gathered by Canadian embassies, including through the Global Security Reporting Program (GSRP). Diplomatic reporting is not technically open-source intelligence but is usually classified at a lower level than intelligence obtained through clandestine means. The Global Security Reporting Program includes about 35 diplomats posted in countries in which Canada has security interests. They spend the bulk of their time meeting interesting and relevant contacts and then send reports back to Ottawa. This reporting is not always distributed as widely across government as it should be, notably because of silos between departments, institutional rivalries, and a lack of shared information systems.

- Ensure that discussions about open-source intelligence are open and transparent. The government in general, and the national security community specifically, need to patiently build the social licence necessary for this debate to truly progress.

5. Strengthening cyber-security

Canada's 2010 cyber-strategy helped make Canadian government systems some of the most effective in the world against cyber-attacks. The government continued to improve our cyber-defences in the immediate years following the strategy, including by applying lessons learned from incidents like the 2014 Chinese cyber-attack on the National Research Council.

The *National Security Act* of 2017 created new authorities so that CSE can now actively defend critical infrastructure and economic sectors against cyber-attacks and can engage in offensive operations, with the appropriate safeguards reflecting foreign policy considerations. The 2019 National Cyber Security Strategy recognized the need to boost public awareness of digital crimes and other sophisticated threats, like espionage or foreign interference, and the need to increase government support to the private sector for cyber-security. This led to the creation of the Canadian Centre for Cyber Security and measures to help law enforcement increase its capacity to combat cyber-crime. The announcement in Budget 2022 of $875 million in new funding over five years to strengthen Canada's cyber-defences was further encouraging.



Source: https://cyber.gc.ca/sites/default/files/2021-12/Cyber-ransomware-update-threat-bulletin_e.pdf

In short, our cyber-defences are strong. CSE, the lead agency, has the appropriate authorities, world-class capabilities, and a growing ability and willingness to use them. But cyber-threats continue to evolve, and the government has not always kept up. Many departments still have a poor understanding of CSE's mandate and capabilities, or are reluctant to recognize its work. Beyond the government, moreover, it is often at the level of civil society and the private sector that Canada is most vulnerable to hostile cyber-activities from abroad.

Recommendations:

- Ensure that all departments and agencies understand and make use of the skills and tools provided by CSE.

- Implement the recent recommendation of the National Security and Intelligence Committee of Parliamentarians to extend advanced cyber-defence services, notably the Enterprise Internet Service of Shared Services Canada and CSE's cyber-defence sensors,

to all federal organizations, including crown corporations. Budget 2022 provided funding for this initiative. It should be carried out on a priority basis.

- Update legislation and resulting regulations, authorities, and programs across all levels of government to improve the whole-of-Canada ability to deter and respond to cyber-threats.

- Develop stronger protocols and hold regular exercises involving the Canadian Centre for Cyber Security, other federal partners and levels of government, and key critical infrastructure and economic sectors, to enhance our preparedness to respond to major cyber-incidents.

- Develop a strategy to support small- and medium-sized enterprises in their ability to prevent and mitigate cyber-risks, given the importance of reliable supply chains.

- Ensure that cyber-systems underpinning critical infrastructure, including in such federally regulated sectors as telecommunications, finance, transport and energy, remain safe and reliable. This includes setting mandatory minimum standards of cyber-defence.

6. Protecting economic security

Most foreign investments increase Canadian prosperity, but some also pose a national security threat. The government updated its guidelines in March 2021 on how it reviews investments for national security implications under the *Investment Canada Act* (ICA). These guidelines outline how a review is initiated and update the areas that could represent national security concerns. These include sensitive personal data, certain technology areas, critical minerals, and investments by state-owned or state-influenced investors.

The December 2021 mandate letters from the prime minister to relevant ministers also mentioned the introduction of legislation to safeguard critical infrastructure, such as 5G networks, an expansion of collaboration and intelligence sharing among all levels of government and Canadian partners to address security risks in research and investment, and the elaboration of a strategy that ensures the development and protection of critical minerals. Budget 2022 provided just under $160 million over five years to help the Research Support Fund identify, assess, and mitigate potential risks to research security in post-secondary institutions, and to establish a Research Security Centre that will provide advice and guidance directly to research institutions. The national security review that we propose should explore further opportunities to build on these initiatives as a way of ensuring that there are measures in place to protect all critical components of our economy.

Recommendations:

- Review the *Investment Canada Act*. As it stands, the national security provisions in the Act are vague. They give significant discretion to the government but cause frustration in the private sector, which would appreciate more clarity. The proposal to provide an option for non-Canadian investors to obtain pre-implementation regulatory certainty with respect to a national security review of investments that do not require a filing under the *Investment Canada Act* is welcome in this respect.

- Work closely with private sector firms, universities, and research institutions to protect against the acquisition, licit or illicit, of leading-edge research in sensitive sectors. While the current attention is on 5G infrastructure, the race for technology that can be of dual use (civilian and military) has already shifted to artificial intelligence, quantum computing, space, biomedical technology, and photonics. There has been significant improvement in protecting intellectual property in recent years, much of it precipitated by the pandemic. But obstacles remain. Inside the intelligence community, there is also a need to build better awareness and understanding of the research world.

- Consider sponsoring security clearances for key actors in the private sector, universities, and research institutions so they can receive classified threat information and take appropriate steps to protect their research.

- Quickly implement the recent budget decisions to establish a Research Security Centre and to use the Research Support Fund to build capacity in post-secondary institutions to identify, assess, and mitigate potential risks to research security. Building such capabilities imposes a financial burden on universities, which have neither the skill nor the personnel to implement them.

- Take immediate steps to ban the use of Huawei equipment in Canada's 5G networks, including by amending the *Telecommunications Act* to include security requirements. The risks associated with the use of this equipment have been known for some time, so firms should be given a maximum of one year to replace it.

7. Guarding against foreign interference

Technology has given foreign governments and non-state actors new tools to interfere in the affairs of other countries, harass or disrupt private sector companies, and intimidate individuals. More broadly, it has given these actors the means to spread disinformation and amplify its impact, for example by exacerbating polarization. The recent Budget 2022 decision to provide the Privy Council Office with funding to combat disinformation is a positive, if preliminary, step.

As an open democracy, Canada has found itself susceptible to interference from adversaries such as China, Russia, and Iran, but also from allies or partners such as Turkey, Saudi Arabia, and India. Such interference can include threats, intimidation, and harassment of Canadian citizens and permanent residents, in some cases pressuring them to stop criticizing the human rights and other policies of those states. While Canadian law enforcement and intelligence agencies have been aware of these concerns for years, individuals who face such harassment are often bounced between local police, the RCMP, CSIS, and other organizations, and express frustration that their appeals for help are lost in interagency processes.

Recommendations:

- Develop, as part of a broader strategy to address the hostile activities of state actors (including cyber, espionage, and economic threats), a comprehensive plan to counter foreign interference.

- Explore the creation of a National Counter Foreign Interference coordinator, as the Australians have done.

- Commit to a campaign of awareness-building across the country. Public understanding of the intensity and intrusiveness of foreign interference in the democratic process and in communities is worryingly low. The goal should not be to stoke fear, but to explain to Canadians what foreign interference is, how it can be recognized, and what can be done about it. Law enforcement and intelligence agencies must also be better able to distinguish it from standard diplomatic activity, which is acceptable.

- Brief parliamentarians, especially new ones, on the threat, as well as legislators and senior officials at the provincial and municipal levels. These individuals are often a primary target of foreign state actors.

- Pass legislation to establish a foreign influence registry to make transparent the activities of individuals acting on behalf of a foreign principal or government.

- Develop, with other levels of government and as a matter of urgency, mechanisms to support Canadians who have been subjected to harassment and intimidation for their activism and exercise of free speech. This should include designating specific federal and provincial offices to coordinate the tracking of such threats.

- Help universities develop plans to support foreign students who come under unwanted foreign harassment on Canadian campuses.

- Undertake a comprehensive analysis of interference and disinformation in the 2021 election, particularly on social media and community platforms, with a view to identifying well in advance of the next election those concrete measures that will be required to prevent such foreign interference in future.

8. Deterring organized crime and money laundering

Organized crime and money laundering are not traditionally included in the national security realm and are primarily policing issues. However, these threats can reach a level where they seriously undermine our national interests, the rule-of-law, and our international reputation as a reliable partner. This is partly the result of the legislative authorities of law enforcement agencies not keeping pace with technological advances surrounding digital networks, encrypted telecommunications, and crypto currencies. Money launderers can exploit with impunity the loopholes in the reporting requirements for financial transactions. These gaps have allowed organized criminal groups to benefit from a variety of crimes that they outsource to street gangs, while they migrate their official activities to mainstream economic sectors. This allows them to distance themselves from a potential prosecution. The Budget 2022 announcement that FINTRAC would receive $89.5 million over five years is a preliminary step toward addressing some of these issues. It will also enable FINTRAC to implement new anti-money laundering and anti-terrorist financing requirements for crowdfunding platforms and payment service providers. However, more needs to be done.

Recommendations:

- Update legislative authorities in terms of lawful access to encrypted telecommunication and financial reporting requirements to keep pace with the new digital reality, while staying true to Charter and privacy rights. Engage with key stakeholders, like bar associations and civil liberties groups, to ensure that fundamental rights and privacy are protected but not used as loopholes for serious criminal transactions.

- Adapt RCMP hiring and training to allow the agency to strengthen its expertise and capacity to deal with such sophisticated crimes.

- Follow up on the proposals the prime minister cited in mandate letters to ministers. These include establishing a Financial Crimes Agency, whose purpose would be to investigate these complex crimes, and strengthening legislation and investigative powers relating to financial crimes. We also note that Budget 2022 gave Public Safety a small amount of funding to conduct initial design work for this new agency.

Enhance governance

The governance framework for national security – how decisions are made, policies developed, and information shared – has evolved significantly in recent years. But to maximize the use of new and existing tools, Canada needs to rethink its national security architecture.

This raises the question of whether there is a governance gap at the political level. Canada is the only country in the Five Eyes and in the Group of Seven industrialized countries (G7) without some form of national security body led by a prime minister or president. These bodies come in different shapes and sizes but at their core they provide government with a permanent and in some cases legislated body to hold regular discussions on national security. They allow the prime minister or president and their closest advisors to be briefed collectively. Such bodies deal with short-term crises but also longer-term, strategic matters. They are also critical to building national security literacy within government.

Canada's partners are broadening and strengthening their cabinet-level national security bodies. For example, the United States has expanded the National Security Council under President Biden to include the Office of Science and Technology Policy and the US Agency for International Development. As threats increasingly emerge from non-traditional areas like climate change or pandemics, the architecture also needs to be flexible enough to bring in players, on an as-needed basis, who were not previously core national security actors.

At the cabinet level in Canada, core ministers, such as those for public safety, defence, and foreign affairs, are usually up to speed on national security issues. The prime minister is briefed by the National Security and Intelligence Advisor. But discussions are often driven by events. The Incident Response Group, an ad-hoc group of cabinet ministers and senior civil servants, is a good example. As its name implies, it is a responsive body that meets to react to events. Canada needs a core group of ministers and senior public servants who are not just in response mode, but who engage in sustained and forward-looking discussion of national security.

The same can be said about the sub-cabinet architecture. The governance framework for national security in Canada relies on a pyramidal structure of committees of civil servants to

support Cabinet. There are three committees at the deputy minister level (for policy, operations, and intelligence analysis) and a suite of support committees down the organizational chart. Yet this structure is heavy and not always sufficiently flexible. There is a need to inject discipline and stronger risk management, and to streamline the architecture. Senior committees need to delegate more responsibilities to lower-levels, especially day-to-day operational decisions, to allow higher-level committees to focus on strategic issues.

The National Security and Intelligence Advisor to the prime minister plays a central role in this structure. Yet there has been no consistency in this role since the position was created more than 15 years ago. The advisor has three roles: advise the prime minister, coordinate the work of the security and intelligence community, and conduct outreach to domestic stakeholders and allies. Yet how the advisor performs those roles varies with each person who holds the position. At times, the job has encompassed providing advice on defence and foreign policy. At other times, those areas have been removed from the list of responsibilities.

There is also a need to revisit the governance of the intelligence analysis function. Currently, every department or agency with national security functions has its own analysis and assessment unit. Some are small, such as the new assessment team at Global Affairs Canada, while others are larger, such as the analytical teams within the Canadian Forces Intelligence Command. This structure is far from ideal. Too often, individual units work in silos and fail to coordinate their work. There is, moreover, no strong, central assessment body that can act as a fusion center to produce intelligence assessments that reflect whole-of-government priorities and coordinate the work of the community as a whole. Two units partly perform this function, the Intelligence Assessment Secretariat in the Privy Council Office and the Integrated Terrorism Assessment Centre, housed within CSIS. Neither, however, is equipped to consistently perform a strong, central assessment function. As a result, Cabinet does not get the consistent analytical support that it needs to truly raise the level of debate on national security matters.

People are the foundation upon which the entire security and intelligence community is built. It will therefore not be possible to fully implement the recommendations in this report if the national security and intelligence community continues to struggle with and neglect human resources issues. The community is beset with a range of challenges in this area, including in recruitment, retention, and morale. We therefore urge the community's leaders, at the deputy minister level and below, to pay significant attention to these problems.

As we emerge from the pandemic, national security practitioners also continue to grapple with a return to normal or "new normal" working conditions. Unlike other public servants, who do not necessarily rely as much on classified information for their jobs, those in the security and intelligence community cannot function as easily without access to the required technological infrastructure. The community's leadership will need to ensure that these men and women can perform their duties under new, flexible working conditions, and gain the necessary skills to operate in the current national security environment.

Recommendations:

- Establish a body at the cabinet level, chaired by the prime minister, with responsibility for national security. This would bring Canada into line with allies such as Australia, New Zealand, and the UK. The body should have a core membership of ministers with direct responsibility for national security but be flexible enough to include other ministers when issues arise affecting their departments.

- Review the structure of committees supporting Cabinet on national security, with a view to streamlining it and increasing its efficiency and focus.

- Review the roles and resources of the National Security and Intelligence Advisor to ensure they are fit-for-purpose in the current threat environment. This would include articulating the role of the advisor to ensure consistency in how it is performed. Moreover, we recognize that there is a certain tension in the position's double-hatted role as both advisor on national security, foreign, and defence policy and as provider of intelligence analysis. That said, we see value in keeping these two functions integrated under a single individual providing comprehensive advice to the prime minister. As one of the key players in the national security community, the advisor is supported by a small, over-stretched staff. Additional resources would allow the advisor to play a stronger role in coordinating policy and intelligence and increasing engagement with external stakeholders.

- Enhance the policy capacity of the national security branch inside Public Safety Canada. Currently, this capacity is weak even as demand increases. A more robust model would see the department act as a stronger center of policy expertise on national security. This would allow the National Security and Intelligence Advisor to focus more on coordination, issues management, and support to the prime minister and cabinet.

- Merge the Intelligence Assessment Secretariat in the Privy Council Office and the Integrated Terrorism Assessment Centre to create a unified, strong, central assessment function under the National Security and Intelligence Advisor. This new unit would serve as a fusion center, providing all-source analysis. This would reflect the whole-of-government reality of decision making in Cabinet. It would also offer a stronger coordinating function for the intelligence analysis community, strengthening the coherence of the intelligence cycle as a whole – from priorities, to requirements, to collection, analysis, dissemination, and feedback. This unit should offer an intelligence briefing to start each Cabinet committee session on national security, linking these briefings to the government's intelligence priorities.

- Review the security clearance process, which is widely viewed as slow and dysfunctional. This causes significant frustration among staff and impedes flexibility in managing human resources.

- Prioritize recruitment: this important function has been neglected, leading to long delays. Senior management should be more involved, making sure that recruitment becomes the priority that it deserves to be.

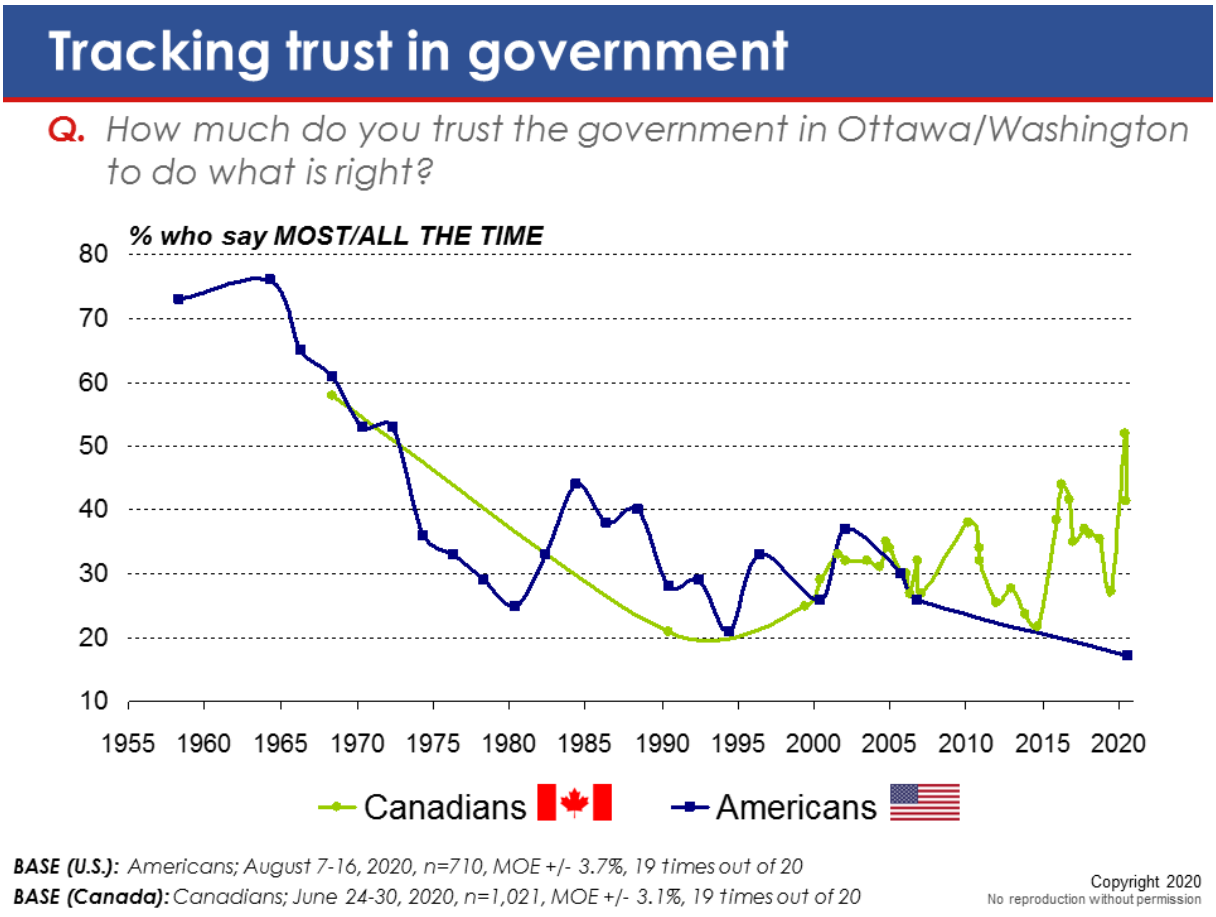
- Broaden the skillsets and experiences of those working in the security and intelligence community, including through interchanges with other departments and agencies.
- Explore ways to ensure flexibility in the work conditions of those serving in the community, especially as it relates to technology.

Increase transparency and engagement

Many Canadians mistrust government. They are wary not just of politicians and public servants, but of other institutions as well, particularly the media. This has major implications for every

facet of life, and national security is no exception. This erosion of trust opens space for misinformation and disinformation to spread. This weakens democratic institutions and contributes to a vacuum that hostile actors do not hesitate to fill. When Canadians mistrust law enforcement and national security agencies, they are also less likely to share information on threats. This lack of trust, in other words, is a major national security problem.

More transparency and engagement with Canadians by the national security community are essential. But on their own they are far from sufficient. Nevertheless, the community's tradition of secrecy has become outdated and counterproductive. There has been much progress in recent years, but there is an urgent need to continue ramping up transparency and public engagement. It is essential for the national security community to acquire a stronger social licence, which is itself essential if we are to develop the societal resilience that has to be one of the main lines of defence against today's threats.



Source: https://www.ekospolitics.com/wp-content/uploads/20200827_slide01.png

1. Engaging with the public

We live in a world where the government is no longer the main target of threats: individuals, institutions, and private sector organizations have all been placed in the crosshairs. Yet the government often fails to keep them fully informed of threats, in part because our security and intelligence practice and culture are overly secretive and inward looking. National security

needs to be more accessible, with the appropriate safeguards in place, if we are to truly bring on board the Canadian population in developing a whole-of-Canada response to security threats.

To do this, we need greater transparency with the public and better coordination with entities outside the core federal government. This is essential to ensure that the government has the support and trust of Canadians. It will also increase public awareness of national security. The public review we recommend will be a start, but engagement must be ongoing.

The national security community has done significant work recently to be more public about its activities. For example, the creation of the Canadian Centre for Cyber Security has represented a good initial step in leveraging the expertise of an elite cyber-intelligence organization to help protect private sector firms and Canadian citizens. CSIS's Academic Outreach and Stakeholder Engagement branch is working with private sector firms and academic institutions to help them become more aware of threats and better protect their research. But much more is needed. The national security and intelligence community has significantly underestimated, for decades, the costs of its poor record of communications with Canadians.

Recommendations:

- Invest significantly in the national security community's ability to better engage with the public. The community possesses engagement capabilities, but they remain small and somewhat isolated from the centers of decision making. A two-way dialogue is necessary if engagement is to build trust. Too often government officials view it as a unidirectional process by which they offload information of their choosing on stakeholders and fail to listen to the concerns and views of others in response.

- Institutionalize engagement. Engagement units need the proper authorities and staff with the necessary skills. These units also need to be connected to broader processes. The results of engagement cannot fall into a dead-end, siloed structure, but instead be circulated inside government, and used to inform and improve policy and operations. One way to encourage greater transparency and make engagement efforts routine would be to include it in the performance agreements of deputy ministers and heads of agencies, as recommended by the National Security Transparency Advisory Group in its second report, published in 2021.

- Publish an annual threat assessment by the National Security and Intelligence Advisor.

- Publish intelligence priorities, as our allies do.

- Increase the presence of national security and intelligence agencies on Twitter and other social media. There has been much progress in recent years. CSIS and CSE now have popular Twitter accounts, for example. But much more could be done. Some agencies, such as the Integrated Terrorism Assessment Centre, do not have a Twitter account, while those who do could be more proactive in the information they share.

- Use intelligence disclosures, like the United States and United Kingdom have been doing in the context of the Russian invasion of Ukraine, to share assessments of key national security challenges. This raises public awareness and helps counter disinformation. We note with encouragement that CSE and the Canadian Armed Forces started doing this in April 2022; we strongly encourage this to continue and intensify.

- Increase public engagement on national security issues by senior government officials, including substantive speeches by the prime minister, key ministers, the national security and intelligence advisor, and the heads of CSIS, CSE, the RCMP, CBSA, and other agencies. While there has been improvement in this area in recent years, this trend should intensify. These senior officials should also meet on a regular basis with journalists from national and local media and civil society leaders for in-depth discussions both on and off the record.

- Establish an independent national security advisory group that includes academic, think-tank, and business representatives. The group could provide regular advice to government on relevant and timely issues.

2. Sharing information with parliament

Some national security issues cannot be discussed publicly because of their sensitive nature. The National Security and Intelligence Committee of Parliamentarians (NSICOP) was intended to create a space for all political parties to have access to classified information in their review of security and intelligence activities. The committee's work, however, has increasingly been paralyzed by political battles. This has hindered its ability to do what should be essential work.

Recommendations:

- Use the upcoming five-year review of legislation governing the National Security and Intelligence Committee of Parliamentarians to consider making it a parliamentary committee, as opposed to a committee of parliamentarians, the current construct. This would align it with the UK Intelligence and Security Committee, which reports to parliament and not to the British prime minister. It would also remove any suspicion that the government somehow unduly influences the committee's work.

- Produce government responses to reports by the National Security and Intelligence Committee of Parliamentarians. These responses should be public, detailed, and timely. This would help the government build awareness about the essential, but still poorly understood, national security review and oversight process. It would also allow it to announce plans on how it intends to respond to the committee's recommendations, ensuring public accountability for its efforts.

- Examine ways to have party leaders cleared to receive classified briefings on the evolving threat environment from other senior officials.

- Provide all members of parliament with detailed and regular intelligence briefings on threats to their own security, notably related to digital security and foreign interference. These briefings, while unclassified, should be concrete. They should explain what these threats look like, and include advice on how parliamentarians can protect themselves and what they should do when threatened.

3. Enhancing diversity

The national security and intelligence community today is more diverse than it was only a few years ago. That said, it still has a long road to travel, especially at more senior levels. Even today, many initiatives to increase equity, diversity, and inclusion are viewed as bureaucratic boxes to tick, as defensive mechanisms to avoid external criticism. This is wrong. Diversity in national security organizations is – or should be – mission-critical. Beyond the poor headlines that it can attract, a lack of diversity genuinely damages an organization's ability to achieve its mandate, including because of unconscious biases. CSE, for example, has made significant strides over the years, and is reaping the benefits today. More diversity is not only essential to foster a healthy workplace, but also a productive one. Without it, innovation is stymied, and agencies fail to understand and work with minority and racialized communities or productively engage with Canadians. This is a topic, importantly, that the National Security and Intelligence Committee of Parliamentarians extensively analyzed in its 2019 annual report.

Recommendation:

- Continue making progress on enhancing diversity in the security and intelligence community, including in its senior ranks. This should include a commitment to publish more data on equity, diversity, and inclusion issues.

CONCLUSION

We live in an increasingly dangerous and unpredictable world, a reality driven home by recent events like the Russian invasion of Ukraine, the pandemic, and domestic protests against government health measures. Canada cannot isolate itself from the many and varied security threats facing the world. Our "fire-proof" house has vanished. So too must our complacency. We must acknowledge and face up to these threats, whether they originate overseas or within our borders. We need to reach out to Canadians and respond as a nation, not just as a government.

This report is an effort to identify serious threats and suggest ways we might improve our collective ability to address them. Whether it is in crafting grand strategy, strengthening specific tools, enhancing governance, or increasing transparency and trust with Canadians, we have tried to chart a path forward for Canada that would give our men and women on the front lines of national security the ability to do their jobs efficiently. We hope it will generate debate not just within government circles, but amongst Canadians from coast to coast to coast. This is a topic that deserves attention. It also demands action.

CONTRIBUTOR BIOS

Vincent Rigby is a senior fellow with the Norman Paterson School of Internal Affairs at Carleton University and a non-resident senior advisor with the Americas Program at the Center for Strategic and International Studies in Washington, DC. He has more than 30 years of experience in public service. Most recently, he was appointed National Security and Intelligence Advisor to the prime minister of Canada in January 2020. He retired in September 2021. He was previously associate deputy minister of foreign affairs at Global Affairs Canada (2019-2020), associate deputy minister of Public Safety Canada (2017-2019), assistant deputy minister of strategic policy at Global Affairs Canada (2013-2017), and vice president of the Strategic Policy and Performance Branch of the former Canadian International Development Agency (2010-2013). From 2008 to 2010, he was the executive director of the International Assessment Secretariat and the lead official on Afghanistan intelligence at the Privy Council Office. In 14 years at the Department of National Defence, Mr. Rigby also held a number of other positions, including assistant deputy minister (Policy), director general of policy planning, director of policy development, and director of arms and proliferation control policy.

Thomas Juneau is associate professor at the University of Ottawa's Graduate School of Public and International Affairs. His research focuses on the Middle East, in particular Iran and Yemen, on the role of intelligence in national security and foreign policy making, and on Canadian foreign and defence policy. He is the author of *Squandered Opportunity: Neoclassical realism and Iranian foreign policy* (2015) and of *Le Yémen en guerre* (2021), co-author of *Intelligence Analysis and Policy Making: The Canadian* Experience (2021), editor of *Strategic Analysis in Support of International Policy Making: Case studies in achieving analytical relevance* (2017), and co-editor of *Middle Power in the Middle East: Canada's Foreign and Defence Policies in a Changing Region* (2022), *Stress Tested: The COVID-19 Pandemic and Canadian National* Security (2021), *Top Secret Canada* (2021), *Canadian Defence Policy in Theory and Practice* (2019), and *Iranian Foreign Policy Since 2001: Alone in the World* (2013). He is a non-resident fellow with the Sanaa Center for Strategic Studies. He is also the non-government co-chair of the National Security Transparency Advisory Group. From 2003 until 2014, he worked with Canada's Department of National Defence as a policy officer.

Margaret Bloodworth completed her distinguished public service career as National Security Advisor to the prime minister and associate secretary to the cabinet, a post she held from 2006 to 2008. Prior to that she was deputy minister of Public Safety, deputy minister of National Defence and deputy minister of Transport. Currently she is a member of the boards of the Hospice at May Court, the Community Foundation of Ottawa, World University Service of Canada, and the Canadian Ditchley Foundation. A member of the Order of Canada, Margaret has been awarded the Public Service of Canada Outstanding Achievement Award and the Vanier Medal of the Institute of Public Administration of Canada.

Kerry Buck was, until recently, assistant secretary, economic sector at the Treasury Board of Canada Secretariat. Prior to that appointment, she was Canada's ambassador to the North Atlantic Council (NATO). She held senior executive positions at Global Affairs Canada: political director and assistant deputy minister for international security and political affairs; assistant deputy minister for Africa and for Latin America and the Caribbean; head of the Afghanistan Task Force; director general for the Middle East and Maghreb, for Afghanistan, and for public diplomacy and federal-provincial affairs; and director for human rights.

Ward Elcock spent more than 40 years in the Canadian public service. He was special advisor on human smuggling and illegal migration in the Privy Council Office (2010-2016). Prior to that appointment, he was the federal coordinator of Olympic and G8/G20 security (2007-2010), deputy minister of National Defence (2004-2007), director of the Canadian Security Intelligence Service (1994-2004), deputy clerk for security and intelligence, Privy Council Office (1989-1994). Prior to that last appointment, he was general counsel for the Privy Council Office, and before that assistant secretary to the cabinet (legislation and house planning) in the Privy Council Office and general counsel, legal services in the Department of Energy, Mines and Resources.

Richard Fadden was National Security Advisor to the prime minister of Canada (2015-2016). Previously, he was deputy minister of National Defence (2013-2015) and served as director of the Canadian Security and Intelligence Service (2009-2013). He also served as deputy minister for Citizenship and Immigration Canada (2006-2009) and Natural Resources Canada (2005-2006). He was president of the Canadian Food Inspection Agency (2002-2005) and deputy clerk and counsel in the Privy Council Office (2000-2002), during which he assumed the additional duties for security and intelligence coordinator in 2001. Over the course of his career, Richard worked in a variety of positions in the Department of External Affairs, the Office of the Auditor General of Canada, Natural Resources Canada, and the Treasury Board Secretariat.

Masud Husain retired from Canada's foreign service in 2021. Upon his retirement, he was director general and deputy legal advisor at Global Affairs Canada. Prior to this appointment, he was Canada's ambassador to the United Arab Emirates and special envoy to the Organisation of Islamic Cooperation. His other foreign postings include Canada's Permanent Mission to the United Nations in New York and embassies in the Netherlands, Jordan, and Syria. He also served at Global Affairs in Ottawa as director general for the Middle East and executive director of the criminal and diplomatic law division.

Daniel Jean served as National Security and Intelligence Advisor to the prime minister of Canada (2016-18). Previously, he was deputy minister of Foreign Affairs (2013-2016) and deputy minister of Canadian Heritage (2010-2013). From 2007 to 2010, he held a number of deputy minister positions, first as associate secretary at the Treasury Board and as deputy secretary (operations) at the Privy Council Office. Before that, Daniel worked on international and migration issues in Canada and abroad, including two postings in Haiti, two assignments in the United States in Buffalo and Washington, and one in Hong Kong.

Margaret McCuaig-Johnston served in senior management positions in the governments of Canada and Ontario over a 37-year public-service career. Most recently, she was executive vice-president of the Natural Sciences and Engineering Research Council. Prior to that appointment, she was assistant deputy minister for energy technology and programs at Natural Resources Canada. She also served as assistant deputy minister at Finance Canada. She has had management positions at Industry Canada, the prime minister's National Advisory Board on Science and Technology, the Ministry of State for Science and Technology, and the Privy Council Office.

John McNee was secretary general of the Global Centre for Pluralism from 2011 to 2019. A career diplomat, he served as Canada's permanent representative to the United Nations in New York from 2006-2011. During his career, he also served as ambassador to Belgium, Luxembourg, Syria, and Lebanon, and Canada's representative to the Council of Europe. In addition, he was posted to Tel Aviv, London, and Madrid. John joined the Department of External Affairs in 1978

and worked in various capacities including as assistant deputy minister for Africa and the Middle East. He also served in the foreign and defence policy secretariat of the Privy Council Office.

Roland Paris is a professor and the director of the Graduate School of Public and International Affairs (GSPIA) at the University of Ottawa. He is also an associate fellow of the Royal Institute of International Affairs (Chatham House) in the United Kingdom. He was the founding director of the Centre for International Policy Studies and previously served in several advisory roles in government, including as foreign and defence policy advisor to the prime minister of Canada. His research on international security, civil conflicts, peacebuilding, and Canadian and American foreign policy has appeared in leading academic outlets and earned several prizes, including the Grawemeyer Award for Ideas Improving World Order.

Morris Rosenberg is a former president and chief executive officer of the Trudeau Foundation. Prior to this appointment, he was deputy minister of Foreign Affairs (2010-2013), deputy minister of Health Canada (2004-2010) and deputy minister of Justice and deputy attorney general of Canada (1998-2004). Mr. Rosenberg began his public service career with the Department of Justice in 1979. From 1989 to 1993 he served as assistant deputy minister, corporate affairs and legislative policy in the Department of Consumer and Corporate Affairs. From 1993 to 1996, he served as assistant secretary to the cabinet, economic and regional development policy, at the Privy Council Office. He was appointed deputy secretary to the cabinet (operations) in 1996.

Nada Semaan had an illustrious career across a broad range of assignments at the highest levels of the Canadian federal government: director and chief executive officer of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada); associate deputy minister of Agriculture and Agri-Food Canada, executive vice president of the Canada Border Services Agency; associate deputy minister at Canadian Heritage; assistant secretary, economic sector at the Treasury Board Secretariat; assistant deputy minister, farm financial programs branch at Agriculture and Agri-Food Canada; and assistant deputy minister, systems, at Human Resources and Skills Development Canada.

Madelaine Drohan is an award-winning author and journalist who has covered business and politics in Canada, Europe, and Africa. She was the Canada correspondent for The Economist magazine between 2006 and 2020. Her book, *Making a Killing: How and why corporations use armed force to do business*, won the Ottawa Book Award and was short-listed for the National Business Book of the Year Award in 2004. She has held research fellowships with the Public Policy Forum (2015-2016), the Chumir Foundation for Ethics in Leadership (2004-2005) and the Reuters Foundation at Oxford University (1998-1999), and has written a series of reports on Canadian public policy. She is a former director of The North-South Institute, Partnership Africa Canada, and Transparency International Canada. She was the first woman to win the Hyman Solomon Award for Excellence in Public Policy Journalism in 2001.

120 University
Room / pièce 6005
Ottawa, Ontario, Canada K1N 6N5
613-562-5689
api@uottawa.ca