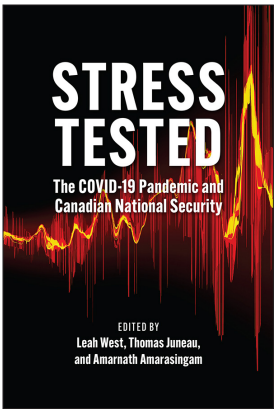
UNIVERSITY OF CALGARY
Press



STRESS TESTED: THE COVID-19 PANDEMIC AND CANADIAN NATIONAL SECURITY

Edited by Leah West, Thomas Juneau, and Amarnath Amarasingam

ISBN 978-1-77385-244-7

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

6

Canadian National Security Operations during COVID-19

Stephanie Carvin

Introduction

The COVID-19 pandemic hit shortly after a profound period of change for the Canadian national security and intelligence community. Between 2017 and 2019, the Trudeau government engaged in the most extensive overhaul of the community's architecture since 1984. In this sense, many departments and agencies were still coming to grips with new authorities, legal regimes, and requirements as the lockdown took hold in March 2020.

This chapter uses interviews with members of the Canadian national security and intelligence community (or what I refer to as "the community") to examine how departments and agencies managed their operations during the COVID-19 crisis. It provides insight into how the community dealt with and responded to changes in the work environment and the threat environment. It concludes by examining how senior-level members of the national security and intelligence community think the pandemic experience may affect their future operations.

Methodology

This chapter is based on semi-structured interviews with ten senior management-level individuals in the Canadian national security and intelligence community, ranging from the Director General to the Assistant Deputy Minister levels. The advantage of interviewing senior managers is

that they were generally familiar with the organization-wide response of their department or agency. Four interviewees were part of their organization's COVID-19 task force, established to manage employee safety while ensuring the continued operation of their organization's critical functions. The organizations represented in this study include the Canada Border Services Agency (CBSA); the Communications Security Establishment (CSE), including its outward-facing entity, the Canadian Centre for Cyber Security, or "Cyber Centre"; the Canadian Security Intelligence Service (CSIS); the Privy Council Office's Intelligence Assessment Secretariat (PCO IAS); and Public Safety Canada (PSC).[1]

Limitations

For reasons of time and availability, this study has certain limitations that the reader should bear in mind. First, I did not interview working-level employees of the agencies. Thus, it is essential to note that these individuals' experiences may be different from that of management. Second, I conducted interviews for this project in January and February of 2021. At this time, a second wave was cresting in Ontario and Quebec, where all of the organizations in this study are headquartered; this fact was captured in the interviews. However, the National Capital Region was also hard hit by a third wave in April and May 2021. Therefore it is important to note that the information in this article reflects the views of interviewees during a specific time during the pandemic, which may have evolved later. Finally, the small number of interviews means that this study provides a window into how national security organizations managed this crisis rather than a comprehensive overview.

National Security Organizations in "Phase Zero"

Unsurprisingly, one of the first significant challenges for the community as they turned to face a radically new working environment was their inability to access the classified networks necessary to send or receive intelligence products. This restriction made it impossible to hold basic conversations about classified or sensitive issues as regular telephone and internet communication channels are not secure. Even when employees could work in a secure compartmented information facility (SCIF), they often did so with reduced staff operating on a rotating schedule. These rotations

meant that urgent messages sent to employees might not be read as soon as necessary if they were not scheduled to work in the SCIF that day. This section looks at how the community dealt with these challenges and the rapidly evolving technology issues by adapting business continuity plans, managing staffing, and addressing the stress and anxieties of employees.

Business Continuity

The majority of interviewees indicated that their department or agency had some kind of business continuity plan (BCP) in the case of a major disruption. Unfortunately, such plans proved to be inadequate almost immediately. In particular, many BCPs assumed that incidents preventing access to classified networks would be temporary, and that it would be possible to establish themselves at an alternative location within a few days or weeks. No organization had plans for a long-term disruption of employee access to classified networks or spaces to hold secure conversations. Therefore, as employees were sent home on the evening of 13 March 2020, plans to adapt existing BCPs to new realities were set in motion.

Even if existing BCPs were inadequate, organizations with BCPs benefited from the fact that their plans clearly identified which employees are "critical" and "essential." As one interviewee noted, at the very least, BCPs are good at "identifying critical systems and critical services." Therefore, while existing BCPs were often "not the correct playbook," the work of designating the agencies' critical functions was already complete. Other organizations seem to have relied on their ability to assess a worsening situation. Two interviewees reported situations where managers took it upon themselves to begin purchasing cleaning supplies by early March. As one interviewee noted, "Managers went out to find hand sanitizer at Walmart to ensure that critical staff had it."

After identifying the inadequacy of existing BCPs, organizations took various approaches to managing the business of national security in the early days of the pandemic, or, as several organizations referred to this period, "Phase Zero." CBSA, CSE, CSIS, and PSC interviewees reported that their organizations quickly set up a pandemic management committee, often including representatives from human resources, occupational health and safety, IT security, and senior executives. While most interviewees added that they incorporated the advice provided by the Public

Health Agency of Canada (PHAC) and the Treasury Board, some felt that the advice about procedures was "very slow" in terms of dissemination, leading them to establish their own processes to keep critical functions operating. One interviewee expressed frustration that there was sometimes an effort to ensure that things were done evenly across agencies, even if responsibilities may differ across units. In one case, an interviewee noted that there was pressure to conform to universal policies, even if units had vastly different tasks, responsibilities, and operating environments, or had put in place their own mitigation measures to reflect the working conditions in their office. In this sense, the interviewee felt that senior leadership wanted managers to "be creative," "but there was not a lot of serious options given."

Interviewees indicated that some organizations also turned to their international partners to exchange information on best practices. In particular, two interviewees noted that CSIS stayed in contact with international allies to "compare notes" as to how to function and maintain operations. As one observed, "We've stayed in close touch with all of our partners around the world. And I would say that all of us are tracking with the same challenges and the ways of being able to address them." CBSA stayed in contact with its "Border 5" (Five Eyes) partners to share advice on border management.

Staffing

Interviewees indicated that the most immediate critical task was figuring out staffing. According to one interviewee, maintaining "critical" functions at CSIS required 25 per cent operational capacity. Maintaining this capacity did not require 25 per cent of staff in the building at once, but over shifts, including evenings and weekends. Ultimately, every organization represented in this study adopted some kind of shift/rotation approach to staffing as it allowed staff to more safely access classified networks. Beyond this, individual organizations adopted other unique approaches to overcome this problem. One interviewee reported they were able to use their personal contacts with other government entities to use their SCIFs, augmenting the number of people that could access classified systems at one time. PSC looked at the jobs performed by staff and recombined them according to those that could be done entirely at home

in an unclassified environment and those that required access to classified networks. Relocating tasks in this way allowed PSC to reduce the number of individuals who required access to a SCIF to do their work.

Managing Stress and Anxieties

Beyond being physically safe, a major concern reported by all interviewees was the mental health and well-being of the employees in their organizations. As one interviewee noted, individuals in the intelligence community "are used to uncertainty. But this was about their own circumstances and their work environment." Another noted, "it's not like a sustained crisis where it's a terrorism attack . . . and you're working on adrenaline. It's something outside our control."

Of course, the national security and intelligence community is not exceptional in this regard. Many of the issues and concerns are the same as those faced by other Government of Canada employees. These include anxieties about whether their workplaces were safe and having to work while home-schooling their children. However, the nature of some employees' work, especially those who needed to continue in-person meetings with sources or clients, raised additional concerns, particularly if they lived with vulnerable people at home.

Additionally, employees working on highly classified files still needed to come into the workplace. As one interviewee noted, sensitive discussions around cabinet conversations and most national security issues are, at a minimum, classified at the secret level. While top secret phones exist, interviewees described them as limited in their usefulness and connectivity. Moreover, some employees, such as client relations officers, have jobs that require them to meet with different people in secure locations across the government. This facet of their work increased their risk of coming into contact with someone who may have COVID-19. In such cases, interviewees indicated they needed to make sure that individuals undertaking this work did not put their families at risk.

Employees who were not coming into work also felt stressed. Interviewees from three organizations noted that staff told to stay home felt anxiety about their inability to do their jobs. Indeed, while their work may have been important, it was not required for the most critical functions of their respective agencies. "Some people were feeling like 'I need to

get into the office. I need to do my job.' And they were really not feeling happy about being told, 'No, stay at home until we call you in.' "

On the other hand, some employees were "resentful" of their critical status. For example, there were cases where administrative assistants to senior managers were deemed critical, but senior managers overseeing high-level counterterrorism operations were not. In describing this issue, one interview said, "Even though you were essential in the BCP, we don't really need you. And even though you are not essential in the BCP, we do need you. That was a really, really tough thing to manage."

Different organizations took different steps to at least partially address these issues. Within the first few weeks of the pandemic, leadership sent frequent messages to staff about what was happening in the organization and different plans and procedures for moving ahead. CSIS set up unclassified speaking events and workshops on various topics, such as the 1918–19 Spanish flu, cyber vulnerabilities that come from working at home, and food supply chains, and child psychologists address how to handle working at home with kids and dealing with home-schooling. PSC reportedly surveyed individual employees about their personal circumstances and preferences to help re-prioritize and redistribute work. A high response rate to the surveys "helped us figure out what we have to tackle to get where we need to be." Where employees worked in a unionized environment, managers worked with the unions and labour relations to try and ensure that employees felt safe.

IT Services

Of note is the fact that almost all interviewees commented on the efforts of their IT teams to get individuals set up with equipment that allowed them to work with at least a very basic level of security. This equipment included phones, safes, secure video links, and computers secure to the "Protected B" level in most cases, and to the "Secret" level in others. One interviewee remarked that 99 per cent of their organization is now working with a protective device. "Once the pandemic hit, [IT Services] were shovelling out laptops very quickly. . . . It was a phenomenal ramp-up that worked really well." However, beyond being secure, these devices also meet archival requirements for oversight and review, so there continues to be a record of activities and decision-making while employees are working remotely.

It is not possible to come to definitive conclusions about the success of the efforts made to adjust to working in a pandemic environment. However, certain organizations appear to have been able to quickly return to a level of normalcy. PCO IAS returned to between 50 and 60 per cent capacity in the office within a month of the initial shutdown. CSIS reported that they returned to 80 per cent capacity by the beginning of January and, as noted above, a quick IT response meant that the Canadian Centre for Cybersecurity was able to adapt to a work-from-home environment within a few weeks.

A Different Kind of Threat Environment

As the pandemic continued, intelligence and national security agencies found themselves having to adjust to a new operating environment that impacted how they collected and assessed intelligence, raised new intelligence questions, and brought about a sudden surge in threat-related activities. In the words of one interviewee, the pandemic "amplified" vulnerabilities in Canada's critical infrastructure. Therefore, departments and agencies had to adapt quickly to an evolving threat landscape.

Collection Challenges

Intelligence collection is dependent on a number of sources, including information exchanged in meetings and via the movement of people and goods within Canada and across the border. In the immediate aftermath of the imposition of travel bans and lockdowns, the movement of illicit goods and intelligence targets slowed considerably. In some ways, these restrictions were an immediate security benefit: it became very difficult to engage in threat-related activities as malicious actors and contraband could not move about quickly or easily. As one interviewee noted, "our adversaries also dealt with COVID." For example, targets could not meet up in person, impacting their capacity to advance their operations. As another interviewee observed, "Certainly, a lot of the adversary behaviour, whether it's state actors or terrorists, if you can imagine, they can't travel. . . . That impacts us, and it impacted our adversaries equally."

However, interviewees pointed out that this positive side effect of the lockdowns also had two downsides, both of which manifested quickly. First, it is hard to target individuals who are not doing very much. As one

interviewee noted, fewer people involved in activities means "that there is less intelligence. It is harder to fill in patterns and do risk assessments." Second, despite initial setbacks, actors involved in threat-related activities did not waste much time adapting to the new environment. "Eventually, malicious actors find new ways as a result of the pandemic." In the view of one interviewee, there are fewer malicious actors entering the country as a result of the pandemic. However, there has been an increase in the flow of many types of goods entering the country, raising a new set of security challenges. In particular, a significant increase in the volume of goods being shipped into the country means there is more to inspect and more opportunities for contraband to get through. Criminals realize this and try to take advantage of the situation.

Securing the Supply Chain

Related to the change in the flows of illicit goods is a series of challenges to the supply chain. In the first instance, there was concern that items coming into Canada, particularly personal protective equipment (PPE), were counterfeit. Unfortunately, while CBSA officers are trained in recognizing contraband, in the spring of 2020, they were less prepared to recognize fraudulent medical and health-related supplies. As one interviewee asked, "How do you know if PPE and testing kits coming into the country are fraudulent? We didn't have this expertise at first." The second issue of concern is the integrity of supply chains, especially as they relate to vaccines. At the time of writing, there was concern that malicious actors may seek to steal vaccines or damage or destroy them. In addition, given the urgency under which authorities are trying to bring vaccines into the country, there is a risk that malicious actors may attempt to exploit this process and use it to bring in contraband.

Cybersecurity

Most interviewees highlighted the pandemic's negative impact on cybersecurity as a particularly urgent threat. As one noted, "If there's a second pandemic, it is cybercrime." Importantly, interviewees pointed out that there was not necessarily an increase in the number of threat actors operating in this domain, but the methods they employed nonetheless became far more effective. As many individuals were worried about the pandemic and shortages, they were more likely to click on malicious links promising

information on COVID-19, which then compromised their computers, networks, and/or data. Of particular and immediate concern in the initial weeks and months of the pandemic were techniques that impersonated Government of Canada websites and news outlets, and spam emails that appeared to contain urgent information about the virus, lockdowns, food and supply shortages, or other pandemic-related information. The effort to detect false information was complicated by the sudden and unprecedented transformation in how Canadians were now working—remotely, away from their IT departments and protected systems, on their home networks with unsecured Wi-Fi devices. This new environment created more opportunities for individuals to be targeted by malicious cyber actors while logging on to their work networks from home.

New Partners and Clients

The nature of the threat to medical goods and devices during the pandemic meant that national security and intelligence departments and agencies had to work with new and unconventional partners in the government, research, and private sectors. Although the PHAC has been recognized as a member of the broader national security and intelligence community for some time, there were few interactions between it and, for example, CBSA or CSIS. In addition, some departments that are wholly outside the community, such as Public Services and Procurement Canada, needed intelligence to guide their pandemic response.

Consequently, one of the obstacles to overcome was the fact that some of the core audiences for intelligence in the pandemic were unfamiliar with the products and how intelligence might inform policy-making. As one interviewee noted, "Some partners were very new at trying to manage this." Another interviewee noted that many of the new partners in the government sector did not have points of contact with collection agencies and had few employees with top secret clearance who could be briefed. "There's these new [client] departments, but we're probably not consumers of intelligence five years ago that sure need to be consumers of intelligence now."

However, working together is about more than providing intelligence analysis—some departments and agencies were actively involved in managing the transition to operating online. For example, CSE is responsible for the defence of Government of Canada systems. As such, they were

responsible for assisting in the acceleration and acceptance of technological modernization, including cloud computing. They also provided support to departments and PHAC, who suddenly required a new set of tools and communication mechanisms.

The problem was arguably worse outside of the government sector. New threats put industries that had seldom been in contact with national security agencies and that employ few individuals with security clearance in the immediate spotlight. Intelligence collected in the early weeks of the pandemic indicated a surge in cyber attacks and interest from foreign governments in the biopharmaceutical and health sectors (Lathem 2020.) Companies and research institutes (both in the private sphere and at universities) did not understand the extent to which foreign governments would be interested in or target their work. However, unlike government departments and agencies, there is little support either in terms of advice or mitigation for private and academic entities. While the CSE may provide cybersecurity support to systems deemed critical to the Government of Canada with certain authorizations, most of the private sector falls outside this protection. Moreover, while the Cyber Centre can provide advice on threat mitigation, small and medium-sized enterprises may not have the resources to quickly or efficiently implement that advice.

Response

Given the changes to both the physical work environment and the threat environment, how did the Canadian national security and intelligence community respond? Interviewees indicated that although there was no overarching or coordinated strategy for the community, there were similarities in at least three respects: re-prioritization and adjustment, the development of new products, and reaching out to new audiences.

"Ruthless Prioritization" and Readjustment

One interesting finding of this study was that interviewees felt that their organizations had the appropriate mandates and authorities to counter the main threats posed by the pandemic. Although there was some discussion of the need for clarification in some respects (discussed below), no interviewee indicated that their organization required a new or enhanced mandate to cover their activities specifically related to the pandemic.[2]

Instead, interviewees indicated that from an intelligence-requirements perspective, the authorities to collect intelligence on the pandemic already existed while requirements shifted in significance. In this sense, the pandemic "was a new area to explore in terms of what the government was interested in . . . so we did shift to that."

However, the sudden "surge" in pandemic-related intelligence collection and analysis in a novel area required "ruthless prioritization." As one interviewee noted, "we have a whole production line and we had to go through an exercise of 'what do we really need'?' " Another interviewee noted, "we had to drop certain things because the most important thing was for senior executives to know what was going on. It went back to normal as the summer went on." As an example of such a compromise, PCO IAS turned a product typically distributed daily into one distributed every two to three days. CBSA analysts found themselves writing pieces that were more tactical than strategic, a transition described as "hard" but necessary.

In addition, to support these new priorities, there were changes in the kinds of information that clients wanted and, in turn, what units provided. One interviewee noted that senior clients were not necessarily looking for highly classified intelligence so much as briefings on what was happening from people expert at synthesizing information. More than usual, analytical intelligence units were valued for their skills, not just the intelligence they could provide.

New Products

Given the above-noted difficulties accessing classified spaces, most interviewees indicated that their department or agency developed new open-source intelligence products for their clients. The first kinds of products provided synthesized information for consumers. For example, PSC temporarily designed products to help amalgamate all of the different reports coming from the community to make the information more useful and accessible. CSIS's Academic Outreach and Stakeholder Engagement branch also created an open-source product that was a "two-page" roundup of think tank reports, podcasts, webinars, and various scholarly sources called "Need to Know." After it reportedly "exploded in popularity," CSIS turned the roundup into an official product put out every couple of weeks.

Open-Source Intelligence

However, the real transformation came with the increased use of open-source information to inform intelligence analysis. Even agencies that typically work at lower classification levels, such as CBSA, developed new open-source products. Products included a bi-weekly COVID-19 "snapshot," focused on border issues, written by the strategic intelligence team for senior management, and shared with partners.

One of the biggest shifts in this area was made by PCO-IAS. As one interviewee noted, "We had always tried to be all-source," but "many analysts believe that if it is not classified it is not an assessment." The pandemic forced a cultural transformation on this front: "Our ability to use open source meant that we had more information and that it was more timely." As the interviewee noted, "80 per cent of what we do is well covered in [open-source]. Twenty per cent of intelligence adds depth and colour to the understanding of an issue," but very little is truly unique information. As such, PCO IAS developed "commentaries" on topics such as the pandemic's impact on the economy, geopolitics, "mask diplomacy," and disinformation that were well-received and ultimately expanded its client base.

CSIS's intelligence assessment unit, the Intelligence Assessment Branch (IAB), was required to go through a similar transformation, particularly as senior leaders emphasized the need for outreach to the broader research and life sciences communities and their supply chains to help mitigate threats. As one interviewee noted, the Branch is very good at providing classified information or briefings but "they are maybe a little bit less comfortable doing the open-source stuff." The interviewee noted that IAB is "getting really good at [such work]," but that most of the unclassified briefings ultimately were provided by CSIS's Academic Outreach and Stakeholder Engagement branch.

Similarly, the Canadian Centre for Cyber Security worked to produce more content at the unclassified level. They adopted the "Traffic Light Protocol" for many of their products. Designed to facilitate information sharing between the government, the private sector, and other key stakeholders, the Traffic Light Protocol uses four colours to indicate expected sharing boundaries for recipients of the information. Used by national security agencies in other countries, such as the United States, it enabled

the Cyber Centre to pass on sensitive information. Information flagged as "red" may not be shared beyond the direct recipient; "yellow" is information that may be shared within an organization and certain clients on a need-to-know basis; "green" information may be shared with peers and partner organizations; and "white" information may be distributed without restriction. Adopting this protocol enabled the Cyber Centre to provide more meaningful advice and information to those outside the government.

Similarly, interviewees indicated that CSE developed lower-classified products (Protected B) that built on knowledge informed by intelligence that could be distributed to clients in order "to remain relevant and helpful and to really find out where our value added is." These products have reportedly received good feedback from clients who are working from home: "They appreciated it, they could use it, they could communicate it, they could make decisions based on it. . . . There was a benefit to folks to receive those things, so absolutely we want to continue that work." However, it was also clear that there were limits to the open-source transformation. In the view of one interviewee, the clear and obvious specific value proposition of CSE for the Government of Canada is the provision of information from the global information infrastructure. "I'm very mindful that our business is special," reported one interviewee, "and we should . . . make sure we maximize that."

Educating and Understanding New Audiences

As noted above, most national security agencies made efforts to reach new audiences within the government and the private sector. An increase in the number of intelligence products and briefings that are unclassified or of low classification appears to have helped drive this interest. However, the process of serving new clients can generate certain challenges. Interviewees spoke of a need to "educate stakeholders, both in government but also in the private sector." According to one interviewee, "Initially, it was, frankly, ensuring that decision-makers know that intelligence plays a role. That may not be their first instinct, typically." As such, agencies needed to expend time to "better inform key stakeholders, government stakeholders, of the type of intelligence that can be produced and why it would play such a key role."

Importantly, interviewees stressed that the developing relationship between national security and intelligence agencies, non-traditional government partners, and the private sector is mutually beneficial. Interviewees indicated that there were at least three benefits for the community from these exchanges. First, one interviewee noted, "for us, it is a two-way street," meaning that meeting with new partners helped provide a better understanding of what and where the vulnerabilities are and allowed agencies to tailor their intelligence requirements. Providing threat briefings also helped intelligence-collection agencies better understand their policy clients' needs: "When they see what we can bring, it's really a partnership because they explain their processes, the procedures, and then we can help fill those gaps."

Second, knowledge from the policy community helped educate and better prepare the community for certain tasks or fill intelligence gaps. An example of this is the need to protect the integrity of supply chains. As noted above, intelligence and law-enforcement individuals did not have training or expertise in recognizing fraudulent medical devices. Therefore, a lot of effort in the first weeks of the pandemic went toward finding the expertise necessary to stop goods at the border, often from non-traditional or policy partners.

Finally, following briefings and exchanges with non-traditional partners, clients better understood and recognized threat-related activities. Armed with this new knowledge, clients would often contact intelligence and national security agencies when they spotted something suspicious. An interviewee noted that collection agencies were also "getting leads from those organizations" due to these exchanges. Once educated on what threat-related activities are and whom they should contact, new partners were "phoning us because they've come across information of concern and they want our feedback on it. They benefit, we benefit."

Conclusion: Future Implications

Findings from the interviews indicate that—as is almost certainly the case in other areas of government—senior managers and executives within the Canadian national security and intelligence community are evaluating the future implications of the pandemic in terms of how their organizations

will fulfill their mandates. This final section provides an overview of these assessments, beginning with trends in how threat information is conveyed, followed by expectations for the working environment, and concluding with challenges the community is likely to face.

Acceleration

One of the most consistent findings is that the pandemic accelerated changes that were already taking place in the community. As one interviewee noted, all of the changes planned for 2023 were in place by April 2020. In the case of the CSE/Cyber Centre, interviewees identified three key areas of acceleration: accepting and modernizing new technology; the kinds of advice the centre provides to Canadians; and engagement with critical infrastructure and private sector stakeholders in the face of sophisticated cyber threats.

Out of the Shadows

Whether it was interest driven by new open-source, unclassified, or low-classification products, outreach to new partners in the private sector, official statements and speeches, or engaging with the media, the community has arguably never engaged so thoroughly with others. In 2020, CSIS's Academic Outreach and Stakeholder Engagement branch gave threat briefings to over 400 companies, representing over two thousand people. These numbers include briefings to over forty universities in each of the ten provinces. The branch also gave an interview to discuss its activities to the Public Policy Forum (Lathem 2020). In February 2021, CSIS's Director gave a speech hosted by the Centre for International Governance Innovation (CIGI) in which he publicly acknowledged China and Russia as threat actors engaged in economic espionage and foreign influence activity (CSIS 2021). This was the first time in decades—if ever—that someone in his position made such a declaration. Early in the pandemic, CSE also publicly noted that it was involved in taking down websites involved in COVID-19 fraud—the first public acknowledgement of this kind of action (Tunney 2020). Additionally, CSE publicly attributed a cyber-espionage campaign to Russia (CSE 2020).

There are several reasons for this increase in the level of public interaction. First, in recent years, as the targets of threat-related activities moved from the government to the private sector, there has been a gradual

recognition that there is a need for the community to be more publicly engaged and to speak clearly to stakeholders. Building on the point made above, this, too, has been accelerated by the pandemic. As one interviewee noted, "The media stuff is just stuff we do now. It's just life. It's weird and we live with it." Second, interviewees noted that when intelligence agencies make statements or attribute malicious activities, it generates media attention and interest from members of the private sector, who become concerned that they may be targeted. This concern makes public outreach to the private sector easier and more likely to continue.

Exploiting Open-Source Resources

To facilitate more engagement with non-traditional partners and the private sector, to augment their capabilities, and to produce products that can reach a larger number of clients, it is very likely that many parts of the intelligence and national security community will continue to use more open-source information. While interviewees noted that there are still pockets of resistance in intelligence analysis units, open-source information means simply having more resources and often more timely information since analysts do not have to wait on collection. One interviewee noted that Canada's allies are opening centres of excellence to exploit this information, which will likely increase the incentive to develop similar capabilities in Canada and to increase the legitimacy of open-source information as a resource more generally. Importantly, this does not necessarily mean that agencies are switching to producing unclassified products; open-source assessments often remain classified because they have foreign policy implications. However, this will likely make the sharing of such products easier. In this regard, the Cyber Centre's use of the Traffic Light Protocol may be a model for the rest of the community.

Spying from Home?

An interesting finding is the extent to which most interviewees felt that national security and intelligence departments and agencies operate will change. In particular, many of the interviewees felt that the work environment would be far more flexible in the future. The main reason they gave for this is that the private sector is heading in a similar direction, and so

national security and intelligence agencies will need to offer more flexible conditions to attract and maintain talent. As one interviewee asked, "How does the service remain competitive? Our Intelligence Officers are probably going to still come in the door and our analysts, maybe. But human resources, finance, policy people. . . . How do I recruit a really good policy person who is getting a similar job offer at the Department of Fisheries and Oceans and just would prefer to be able to have time to be able to work from home?"

Indeed, it seems clear that working from home or a more flexible workday/workweek is very popular in some parts of the national security and intelligence community. A survey conducted by PSC in July 2020 found that only 9 per cent of employees wanted to return to working in an office full-time. As an interviewee noted, "the work situation will never return to the way it was, and this is a great thing. It will free people to be more productive." They noted, for example, that many employees were spending less time commuting.

However, not everyone interviewed was convinced that this would happen. One interviewee noted that they were hopeful that the more flexible arrangements would remain but said that "this experience should change the way things work, but I am cynical." Another remarked that there were advantages to adopting a more flexible approach to work, such as the ability to recruit talent from across the country more easily, but that it will ultimately depend on the preferences of high-level officials, such as Deputy Ministers. Given that many senior managers like having their people around them, "in a lot of other areas we will see business as usual." Of note, even where individuals were optimistic about change, they suggested that the community has been "slow off the mark" because "it does require a significant investment of resources, time, and energy." Thus, while there is a clear desire for change, what the future of work looks like for the Canadian intelligence and national security community remains to be seen.

Widening National Security?

A final trend identified through the interviews concerns the belief of many in the community that the scope of national security and the kinds of intelligence that they collect should expand. As noted above, all agencies

interviewed faced new requirements (or a change in priorities) to support government decision-making and to counter threats related to the pandemic. Yet, interviewees overwhelmingly indicated that they had the mandate and authorities to collect the intelligence needed by the government. So, what is the case for expansion?

First, information from the interviews indicates that conversations are taking place within their organizations about the need to change the way the community is managed. In an age marked by hyperconnectivity, increasing threats to critical infrastructure, and our dependencies on the Internet, interviewees argue that the government needs to improve the integration and enhance the centralization of the national security and intelligence community. One interviewee noted that the community needs to review how it manages early warning, how intelligence assessment informs policy-making, and how the community works with non-traditional partners. However, the community's future success also depends upon whether it can improve the way its intelligence products inform decision-making. This will require efforts to maintain the ad hoc relationships and arrangements created during the pandemic so that they are carried forward into the future.

Other interviewees felt that Canada needs to widen the scope of its intelligence activities from a narrow threat focus to one more closely tied to Canada's broader national interests. In the words of one interviewee, "the discussion needs to be about what are, and how do we protect, our national interests and get away from a security-service mentality to an intelligence-service discussion. What do we want from our intelligence service? What do we want from intelligence? What do we need as policy-makers from an intelligence service?" In other words, to be more relevant to government decision-making and to better understand future threats, the community needs to move beyond its current approach of (mostly) focusing on threat intelligence and instead adopt a wider approach that looks at future disruptive challenges coming over the horizon.

At What Cost?

As noted above, interviewees confirmed that the pandemic required the community to collect intelligence and/or develop expertise in new areas or areas that had not been the focus of much attention in the past. However,

they also noted that this came with a price: long-term strategic planning was dropped in favour of generating immediate tactical information. One interviewee offered the following observation: "You're just, like . . . 'We're going to do the things that are the most important, and that's the way it's going to be.' . . . The downside of that is clearly that those other things, like nice-to-do things . . . had to drop off because they require time, attention. . . . I think those are the things that we had to let drop that folks are anxious to get back to." As such, while there may currently be interest in widening the mandate of the intelligence and national security community to look at issues such as health intelligence, or other larger strategic issues, if this is done without community coordination and an allocation of appropriate resources, there may be a cost in terms of losing focus on other more traditional areas of concern. This may be a positive change for some, but re-prioritization without care may leave new gaps where old requirements once existed.

A widened approach that draws the community's focus away from threats toward interests—the latter being a more contestable concept given that the former is defined in law—is a significant, if not radical, step for Canada. It would almost certainly require new legislation, new authorities, and, ultimately, a new debate about what we want our national security and intelligence agencies to do. I have already expressed concerns that widening the community's mandate to include areas like health and the environment could entail the securitization of these issues—political problems that require political solutions (Carvin and Davis 2020). Nevertheless, this chapter's' findings are indisputable: a widening of mandates is on the minds of community leaders. Although it is far from clear whether the Canadian government wishes to tread such a path, it will be an important post-COVID-19 development to observe in the coming months and years.

NOTES

1 This project was subject to ethics approval by Carleton University's Office of Research Ethics (Project #115056). Interviewees were promised anonymity, but permission was sought to identify organizations where it was deemed important for clarity.

2 However, it should be noted that in interviews and in public statements, CSIS officials have indicated that they believe that, generally speaking, their authorities are increasingly out of date and that this is a problem when it comes to fulfilling their mandate. In interviews, CSIS officials confirmed they believed they could collect for the new intelligence requirements related to the pandemic. Nevertheless, they stress that there are presently challenges that need to be addressed, such as technological limitations on intelligence collection that was not foreseen by the drafters of the *CSIS Act* in 1984. See CSIS (2021).

REFERENCES

Carvin, Stephanie, and Jessica Davis. 2020. "National Security and Pandemics: The Limits of Early Warning." *Policy Options*, 24 April 2020. https://policyoptions.irpp.org/magazines/april-2020/national-security-and-pandemics-the-limits-of-early-warning/.

CSE (Communications Security Establishment). 2020. "CSE Statement on Threat Activity Targeting COVID-19 Vaccine Development." Government of Canada, last modified 16 July 2020. https://www.cse-cst.gc.ca/en/media/2020-07-16.

CSIS (Canadian Security Intelligence Service). 2021. "Remarks by Director David Vigneault to the Centre for International Governance Innovation." Government of Canada, last modified 9 February 2021. https://www.canada.ca/en/security-intelligence-service/news/2021/02/remarks-by-director-david-vigneault-to-the-centre-for-international-governance-innovation.html.

Lathem, Catherine. 2020. "A Pivotal Moment: CSIS Steps Out of the Shadows to Protect Canada's Biopharmaceutical and Healthcare Sectors during the COVID-19 Pandemic." *Public Policy Forum*, 23 November 2020. https://ppforum.ca/publications/a-pivotal-moment-csis-steps-out-of-the-shadows/.

Tunney, Catharine. 2021. "Canada's Cyber Spies Taking Down Sites as Battle against COVID-19 Fraud Begins." *CBC News*, 23 March 2021. https://www.cbc.ca/news/politics/cse-disinformation-spoofing-1.5504619.