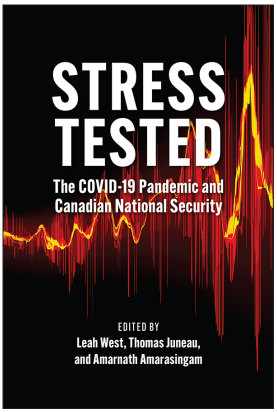
UNIVERSITY OF CALGARY
Press



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

Conclusion

Thomas Juneau

This short conclusion draws out some of the key themes that emerged in the chapters throughout this edited volume. In particular, it highlights:

- the extent to which the national security and intelligence community was ready—or not—to face the pandemic;
- how the threat environment changed during the pandemic;
- how the community adjusted; and
- the longer-term implications for the community going forward.

Preparedness

When the pandemic hit Canada in March 2020, how ready was the national security and intelligence community? In answering this question, it is important not to set an impossible standard. To some extent, the pandemic has been a unique and unprecedented crisis for which no government could have been reasonably expected to be fully prepared. Nevertheless, security agencies understand that the world is unpredictable, and it is undeniably appropriate to expect them to plan for a range of contingencies.

Not surprisingly, therefore, when the pandemic struck, many agencies and departments were ready to implement business continuity plans that

they had already prepared. However, as meticulous as these plans might have been, they did not survive unscathed from their first contact with the virus. As Carvin explains in her chapter, such plans were often helpful in allowing senior officials to rapidly identify critical missions that had to continue, even with reduced staffing levels. Still, they were of less use to guide more tactical decisions, notably on sanitary procedures.

The Department of National Defence and the Canadian Armed Forces (DND/CAF) had a detailed counter-pandemic contingency plan, which, once activated, became Operation LASER. This preparation is not surprising given that the CAF's very nature demands that it be ready to operate in crisis environments. As Cox explains in his chapter, there have been two aspects to this operation: the first focusing on force protection, integrity, and effectiveness, and the second providing military support to civil authorities. According to Cox, this preparedness allowed the Defence Intelligence Enterprise to adapt rapidly and, after important adjustments, to meet its priority intelligence requirements.

The national security and intelligence community was ready—to some extent—to face the pandemic. Rayes and Sahloul argue, however, that the pandemic has shone a light on the specific public health, economic, and political challenges facing minority communities, including migrants and refugees, in the United States and Canada. In their view, governments were not prepared to understand the disproportionate impact the pandemic would have on these communities, notably because of the unavailability of ethnic and racial demographic breakdowns of COVID-19 incidence and mortality. Without such data, governments cannot build a more holistic view of the security challenges facing these communities.

Turning to the legal system, Nesbitt and Hansen identify in their chapter three systemic challenges in criminal law that the COVID-19 pandemic exposed. First, they argue that Canada's criminal justice system has been stress tested by the pandemic, notably due to increases in certain types of criminal behaviour and the introduction of new public health regulations. Second, they write that Canada saw a rise in ideologically motivated extremism, especially of the far-right type, and conspiracy-driven threats like QAnon (discussed below). Third, this shift occurred in the context of an already overstretched criminal justice and national security apparatus. In other words, Nesbitt and Hansen argue that an already strained

criminal justice system has had to respond since March 2020 to increased security threats while operating with fewer resources because of the imposition of pandemic-related public health measures.

Threats

One of the main themes that emerges from the chapters in part 1 is that the pandemic did not so much lead to the emergence of new security threats as foster conditions that allowed pre-existing threats to intensify.

Conspiracy theories often thrive in times of crisis, and the recent pandemic has been no exception. Early on, various theories—concerning 5G technology, the accusation that vaccines include microchips, or, more broadly, that the pandemic is a vast conspiracy to establish a new global order—emerged and have since multiplied. Their spread was already a concern before March 2020. Yet the pandemic (and more specifically, measures taken by governments to limit its spread) contributed to an unprecedented rise in conspiracy theories and the merging and blending of different conspiracies. As Argentino and Amarasingam explain, there may be no better example of this trend than the QAnon movement, which grew in popularity partly because it rode the wave of COVID-related conspiracies. Until 2020, the Canadian government rarely looked at conspiracy theories through the prism of national security. This approach, however, is changing as the risk increases that conspiracy theories will motivate domestic extremists to commit violent acts. The problem has attracted significant attention in the United States, most visibly with the 6 January 2021 insurrection at the Capitol in Washington, DC. But, as Argentino and Amarasingam note, Canada has not been immune from the phenomenon.

Similarly, Babb and Wilner explain that the pandemic has emboldened terrorist and extremist groups worldwide, providing them with new opportunities. Far-right groups, in particular, have taken advantage of the COVID-19 pandemic to aggressively promote their cause in cyberspace and on social media. As with the spread of conspiracy theories, this is not a new trend but it intensified after March 2020. It has also been a global phenomenon, with direct implications for Canada. Yet as Babb and Wilner explain, as much as the trend is worrying, the concrete national security

implications of these online activities are still poorly understood. Like the pandemic, the online threat environment is fast evolving in unpredictable ways, making it a constant challenge for Canada's national security agencies to keep track and do more than react. The authors, moreover, expect these trends to continue: malicious actors mobilized and emboldened after March 2020 will need to adapt as the pandemic subsides, but they will not disappear.

The pandemic has also opened additional space for threats to Canada's economic security. As with the spread of conspiracy theories and the mobilization of far-right groups, these threats predate the pandemic, but events since March 2020 have allowed them to intensify. As Momani and Bélanger argue in their chapter, the long-standing shift by the Canadian economy and society toward the digitalized world has rapidly accelerated during the pandemic, forcing the national security and intelligence community to be even more vigilant about foreign and domestic cyber attacks on critical infrastructure. Indeed, there has been a significant increase in cybercrime and more advanced attacks since the start of the pandemic. Critical infrastructure, according to Momani and Bélanger, is the "soft underbelly" of Canada's cybersecurity defences. The health-care system, in particular, has been the target of ransomware attacks, both in Canada and elsewhere in the world. The situation is especially complicated in the Canadian context because critical infrastructure has steadily shifted from public to private ownership and control. As a result, efforts to shore up defences involve a growing number of actors at all levels of government and in the private sector.

Similarly, as Carvin and a group of her students from the Infrastructure Protection and International Security Program at Carleton University explain, Canada's supply chains, especially in the food and personal protective equipment sectors, experienced difficulties during the pandemic. Again, this was not a new phenomenon: concern about the security of supply chains in strategic sectors predates the pandemic. Events since March 2020, however, have demonstrated how weaknesses in critical supply chains can have negative economic consequences that can quickly spill over into the security realm. In their chapter, Carvin and her students thus identify five reasons why Canada's supply chains experienced difficulties during the pandemic: a lack of domestic manufacturing and

production capacity, short time frames, non-diversified sources for materials and consumers, vulnerabilities to global disruptions, and a lack of redundant systems in place.

Adjustment

The pandemic forced the national security and intelligence community to adapt in new and unforeseen ways. However, a consistent finding throughout this edited volume is that the pandemic also accelerated changes already taking place inside the community. It has forced departments and agencies to hasten their adoption and use of certain technologies, change their management of human resources, and engage with new partners both inside the federal government and beyond.

The community, most obviously, had to revise expectations of what it could and could not do, both upward with its political masters and downward with staff. It then had to target its suddenly limited resources toward critical priorities in what is labelled in Carvin's chapter a "ruthless" exercise. The community's leaders had to make difficult choices at every stage of the intelligence cycle. Collection, analysis, and dissemination of intelligence could not continue at a normal pace, and less essential activities had to be abandoned or slowed down. Moreover, it rapidly emerged that this re-prioritization exercise could not merely involve the reduction of resources dedicated to less critical activities; it also had to include the commitment of additional resources to new priorities as they emerged.

The precise impact on the community's departments and agencies varied. In his chapter, Wallace explains how deporting unwelcome migrants is, like prosecutions discussed in the chapter by Nesbitt and Hansen, a critical tool for the federal government to fulfill its national security mission. Wallace emphasizes that before the pandemic, the Canada Border Services Agency (CBSA) regularly initiated terrorism and security inadmissibility proceedings. Unlike the limited use of criminal prosecutions for terrorism or other national security offences, this is a power that the government in Canada uses widely. Wallace finds, however, that the pandemic negatively impacted CBSA's ability to enforce deportation orders, notably because of remote working conditions and reduced air travel. Yet he argues that the pandemic also created conditions that permitted CBSA

to reform its deportation posture, which will allow it to emerge, once normal life resumes, with more capacity.

The COVID-19 pandemic also imposed adjustments on the CAF. They have had, in particular, to engage in more operations on the domestic front, notably by deploying to long-term care facilities in Ontario and Quebec and by assisting with vaccine distribution. Interestingly, Saideman, von Hlatky, and Hopkins note in their chapter that the impact on international operations has not been evenly distributed. Maritime and air operations only required modest changes. Land operations, however, often had to be curtailed, especially when they involved a capacity-building component, since training foreign troops presents a higher risk of COVID-19 transmission.

Cox's chapter details how the Defence Intelligence Enterprise conducted this re-prioritization exercise. On the analytical side, risk management decisions within the Canadian Forces Intelligence Command were delegated down to mid-level managers. These managers then determined which strategic intelligence products were essential—and therefore required that analysts come into the office to work on classified systems—and which ones could be delayed.

Human resources thus became an urgent preoccupation. As Cox explains, managers in the Defence Intelligence Enterprise have tried to strike a complex and constantly shifting balance between evolving intelligence priorities, sanitary measures which capped the number of employees in the office, and the needs of employees, many of whom had children at home. Similarly, Robinson analyzes in his chapter how the Communications Security Establishment (CSE) managed to balance the need to maintain a fast operational tempo in a highly classified environment with its obligation to protect its workforce.

The pandemic has also imposed an unexpected burden on the community's IT staff as thousands of employees suddenly started working from home, creating an enormous surge in demand for various services. As Robinson explains, CSE's Canadian Centre for Cyber Security, in particular, played a critical role in supporting the efforts of Shared Services Canada (the federal department responsible for the public service's communications systems) to provide secure and reliable access for online work for federal employees.

In recent years, the intelligence analysis community in Ottawa has slowly but steadily grown more comfortable with incorporating more open-source information into its work. Even if some resistance remains, analysts and their managers have increasingly understood that the best analysis is based on both classified and openly available sources. Here again, the pandemic accelerated this pre-existing trend. In her chapter, Carvin explains how various analytical units, notably the Intelligence Assessment Secretariat in the Privy Council Office and the Intelligence Assessment Branch in CSIS, had to adjust to the reality of a proportion of their analysts working from home—first by consuming more open-source information and then producing more unclassified reports.

A final trend that predates the pandemic but has intensified since March 2020 is the level of co-operation between the national security community and non-traditional partners. In recent years, the community has had to significantly ramp up its co-operation with other departments and agencies in the federal government such as Elections Canada and Innovation, Science and Economic Development to deal with emerging threats such as foreign electoral interference and foreign investments of concern. It has also had to learn to work more closely with actors in other levels of government and the private sector. CSIS and CSE, for example, have expanded their ability to work with universities and private companies to warn them against the growing threat of economic espionage.

The pandemic has led to a rapid intensification of the national security and intelligence community's efforts to expand its ties with non-traditional partners. Robinson's chapter, for example, explains how CSE's Canadian Centre for Cyber Security, in addition to its standard activities in support of the rest of the federal government, has increasingly provided cybersecurity advice and services to public and private health institutions, notably those involved in vaccine research and development. Similarly, in her chapter, Carvin reports that CSIS's Academic Outreach and Stakeholder Engagement branch gave threat briefings to more than 400 private-sector entities in 2020.

Finally, just like other sectors of the workforce, the national security and intelligence community has had to deal with significant mental health and well-being challenges for its personnel, as discussed by many authors in this volume. Like everyone else, national security personnel have had to

deal with the anxiety caused by having children at home because of school closures and the possibility of family members falling sick. Those who had to continue physically showing up at the office also struggled with concerns regarding workplace safety. Many struggled with the additional work pressures stemming from having to do more with less. For managers, this has represented an additional burden as they have had to juggle the new demands created by the pandemic with the genuine emotional stress of a large proportion of their staff.

The Future

The pandemic forced the national security and intelligence community to make many adjustments. Some of those changes will undoubtedly revert to the pre–March 2020 *status quo ante* eventually. Should some of those adjustments be retained, even if only partially? What lessons, more broadly, can the community learn from its experience during the pandemic?

An early question the community will have to ponder is the issue of remote work. A few chapters in this volume suggest that at least some employees might want to keep the option of working from home, even if only on a part-time basis, once the pandemic subsides. For many employees in the national security and intelligence community, this is an option that, at most, they can only adopt on a very partial basis since much of their work requires access to classified material and spaces. Nevertheless, even in their case, events since March 2020 have shown that, with some planning, many employees can organize their week to use a specific day to focus on unclassified work at home. Certainly, the frequency of remote work could be higher for other employees less dependent on access to classified material and spaces. For many employees, this can bring significant benefits, notably for mental health and avoiding commuting.

Beyond human resources issues, the national security and intelligence community will face a series of questions regarding its mandate, how it conducts operations, and the nature of its co-operative relationships with partners and stakeholders.

Looking ahead, the most important high-level debate for the community might be the place of health intelligence in its work. Should the collection and analysis of health intelligence be given greater priority than

before 2020? Should analytical units deliver more products focusing on threats to health security? In theory, answering these questions in the positive is appealing, but in practice, this would lead to difficult choices. In a context of scarce resources and with agencies' collection and analytical capacity already stretched by the diversification of the threats Canada faces, calling for more focus on health intelligence is far easier said than done. Would CSIS, CSE, and others receive budget increases to support a greater focus on health intelligence? This funding might be unlikely in the difficult economic and fiscal context that will follow the pandemic. Without additional resources, what other priorities would the agencies downsize to allow for a greater focus on health intelligence?

At the very least, what does seem clear from many chapters in this volume is that the core members of the national security and intelligence community will need to strengthen and institutionalize some of the links they have built with non-traditional partners since March 2020. Outreach by CSIS and CSE with private- and public-sector research, particularly discussed in chapters by Carvin and Robinson, offers a valuable model for the future—in the health intelligence realm and perhaps beyond.

More broadly, as Davis and Corbeil assess, the pandemic has shown the value of improving co-operation and information sharing between the national security and intelligence community and various other sectors of government—in health, but also in the social and economic spheres. These channels of communication and governance structures had been improving and diversifying in the years before the pandemic; one can only hope that this maturation and institutionalization will continue. As Davis and Corbeil emphasize, Canada, like its allies and partners, learned the hard way that a public health emergency such as a pandemic has profound national security consequences. The answer, according to them, is for the actors involved to learn to better work together and share more information.

Beyond the issue of mandates, the pandemic offers lessons at a more granular level of the tool kit the federal government has at its disposal. In her chapter, West argues that existing legal authorities and emergency legislation in Canada do not allow the federal government to collect the personal information of Canadians (like location data) for public health purposes. Where authorities do allow for collecting or analyzing data necessary to trace the spread of communicable disease or enforce public

health measures, it is only in very narrow and specific circumstances that are not necessarily sufficient in a pandemic. Whether a future government will want to give themselves greater authorities is another important question to ponder.

Another tool in the federal government's portfolio to deal with public health crises is the military. As Saideman, von Hlatky, and Hopkins highlight in their chapter, some in the CAF leadership already lamented the high pace of domestic operations before the pandemic. However, events since March 2020 have shown the value of calling on the Forces to deploy in assisting civil authorities during public health crises, be it to help out in long-term care facilities or to lend their logistical expertise to support vaccine distribution. Saideman, von Hlatky, and Hopkins therefore argue that one of the main lessons of the pandemic, from the military's perspective, is that requests for assistance to civil authorities are unlikely to decrease in the future, especially if—or when—other public health crises emerge. Therefore, as the government considers the future of defence policy, it is essential to reflect on the balance between domestic and international operations. This calculation, of course, has significant implications for procurement, force structure, doctrine, human resources, etc.

The COVID-19 pandemic has also highlighted the importance but also the limits of warning. In their chapter, Lee and Piper explain how effective surveillance, monitoring, and reporting are essential for early warning of outbreaks. Efforts to strengthen Canada's ability to face future public health crises must therefore strengthen and renew the capacities that used to reside under the Public Health Agency of Canada, especially the Global Public Health Intelligence Network. Here again, the devil will be in the details: What should be the precise objectives of such a warning function? What specific skills should its staff possess? What should be its relationship with other partners in the federal government, in other levels of government, with private sector and civil-society actors, and with international partners? In their chapter, Davis and Corbeil emphasize that such a health intelligence warning capability needs to be able to work more closely than in the past with the national security and intelligence community. Yet as students of warning intelligence understand well, Davis and Corbeil also caution that a better warning capability is far from a guarantee of future success: timely and accurate warning is a necessary

first step in mounting an effective response, but getting political leaders to act, and act on incomplete and fragmentary information, is, here again, easier said than done.

Finally, the pandemic has forced the community to think hard about burden-sharing with allies and partners. As Cox discusses in his chapter on the Canadian Forces Intelligence Command, before 2020, members of the Five Eyes partnership (Australia, Canada, New Zealand, the United States, and the United Kingdom) already often agreed to a certain division of labour for specific collection and analytical tasks (although little is known publicly about the details of these arrangements). However, given the constraints of the pandemic, they agreed in some cases to divide their work even further, notably on assessments and daily briefs, and to rapidly share the products of this burden-sharing. In this context, it will be interesting for Canada and its closest national security and intelligence partners, especially in the Five Eyes, to reflect on how this type of burden-sharing could be further broadened and routinized post-pandemic.

Canada's national security and intelligence community, in sum, has faced unprecedented stress since March 2020. Its many departments and agencies had contingency plans in place, but the intensity of the pressure it was suddenly under meant that large parts of these plans were inadequate to face the system-wide shock caused by the COVID-19 pandemic. With a combination of hard work, trial-and-error adaptation, and ruthless re-prioritization, the community modified its human resources management practices, assessed the evolution of the threat environment, and adjusted its operations. As the pandemic steadily subsides, the next set of challenges for Canada's national security and intelligence community—and for its allies and partners—will be to carefully read the post-COVID threat environment and ensure that it learns and applies the appropriate lessons.