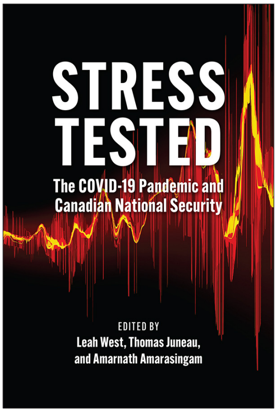
UNIVERSITY OF CALGARY
Press


STRESS TESTED
The COVID-19 Pandemic and Canadian National Security
EDITED BY
Leah West, Thomas Juneau, and Amarnath Amarasingam

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

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

Introduction

Leah West, Thomas Juneau, and Amarnath Amarasingam

The role of Canada's intelligence and national security community has been widely debated since the onset of the COVID-19 pandemic. Some describe its emergence as an intelligence failure or a failure of early warning. Those in this camp argue that Canada should expand the mandates of its security and intelligence agencies to monitor and respond to global health threats. Others argue that the role of intelligence and national security in health matters is and should remain limited. Pandemics have traditionally been considered a public health issue with national security consequences, not a national security issue in and of itself. Tasking security and intelligence agencies with a health intelligence mandate might cause more problems than it solves, duplicating existing capabilities and overstating the utility of early warning to policy-makers.

While this debate continues, traditional defence and security threats have evolved rapidly during the pandemic. We have seen a rise in extremist violence, foreign interference, economic and political espionage, and civil unrest in Canada and around the world. What is more, conspiracy theories related to the pandemic, sometimes perpetuated or augmented by adversarial nations seeking to undermine democratic states, have made it harder to get the virus under control.

All of this raises important questions. How ought we prioritize national security threats during a public welfare emergency? Should Canadian intelligence agencies engage in "health intelligence"? Do our defence, security, and intelligence agencies have the appropriate tools and mandates to take on new roles or adapt their existing missions in a pandemic? How are threats evolving in response to the global crisis, and what are the challenges in countering them in a pandemic? What limits are Canadians willing to accept on their privacy, rights, and freedoms to counter those threats? How well did Canada's security and intelligence community balance the increased demands on its workforce tied to working in a pandemic environment, and did those demands compromise operational effectiveness?

Our collective effort to break down and answer these questions is the result of a Partnership Engage Grant funded by Canada's Social Sciences and Humanities Research Council. Additionally, the funding to ensure that this work is available in an open access format results from a Targeted Engagement Grant from the Department of National Defence's Mobilizing Insights in National Defence and Security (MINDS) program. We thank both organizations for their funding and support.

Our partner in this grant was the Privy Council Office's Intelligence Assessment Secretariat (IAS). The IAS is a central unit tasked with providing non-partisan, all-source analysis to the Prime Minister, cabinet, and the broader federal government. It produces intelligence assessments on a wide range of topics, including, since March 2020, those that help inform the government's response to the pandemic. The need for this research was obvious. Not only is Canada facing an unprecedented health and economic crisis, but when we started this project there was virtually no rigorous academic research explicitly focused on the role of the Canadian intelligence and security community in monitoring public welfare emergencies and managing their consequences. Furthermore, there is limited literature on health intelligence from national contexts other than the United States. This work seeks to add to this small body of literature, not only to expand its scope, but also to offer workable policy solutions for lawmakers and security and intelligence practitioners in Canada and across like-minded states.

In the summer and fall of 2020, the editors worked with the IAS to hold a roundtable with senior officials from across the national security and intelligence community to discuss the challenges they faced six months into the pandemic. Following this broad conversation, and as the situation evolved, several chapter authors continued the discussion with relevant government officials on a direct basis. Ultimately, these discussions spawned the research questions that each author set out to answer.

Not only is the interdisciplinary team of experts assembled in this text highly esteemed, but it is also rare to have such a diverse field of expertise analyze a single, timely, and relevant issue that has a direct impact on the lives of Canadians. Each author employs the methodology best suited to answer their specific research question, which is rooted in the project's overarching question: How well did Canada's national security and intelligence community respond to the COVID-19 pandemic? We are proud that this team is not only diverse in terms of the fields of study and academic lenses they bring to bear on their topics, but it is also gender-balanced and includes scholars from the Black, Indigenous, and People of Colour (BIPOC) community. Many of our contributors also had significant practical experience in the national defence, security, and intelligence community, whether in government or the private sector, before joining academia.

The result combines insights from intelligence studies, political science, international relations, sociology, public health, and law. Together, the chapters in this book provide a deeper understanding of how the intelligence and security community can improve and better integrate its capabilities into federal efforts to prepare, identify, manage, and respond to public health and welfare emergencies. By improving and refining the conceptual and methodological study of the links between security and public health, this work also represents a significant advancement in the broader security and intelligence studies literature.

Plan of the Book

We have arranged this book in two parts. The first contains four chapters and examines some of the new challenges facing those working in Canadian national security. The first chapter, by Argentino and Amarasingam, looks at the interplay between COVID-19 lockdowns, conspiracy theories, and political violence. Using social media data across multiple platforms, arrest records, and digital ethnographic research, they show the ways in which the pandemic has impacted individuals and movements, how they are mobilizing, and what future threat trajectories may look like. The second chapter, by Wilner and Babb, examines how established extremist and terrorist groups have become emboldened worldwide, including in Canada, finding opportunities to exploit the situation, incite hate, (re)mobilize, and promote their ideologies online in new and novel ways.

The following two chapters focus on the nexus between the national security and economic realms. The third chapter, by Stephanie Carvin and students from the Infrastructure Protection and International Security Program at Carleton University, explores the heavy strain placed on supply chains in Canada by the pandemic. They analyze the policies and market dynamics that guide the production and distribution of goods and essential components in Canada and find that supply chains are still not sufficiently resilient against future disruptions. Their chapter calls for Canada to re-examine its food, manufacturing, and distribution policies, and potentially reshape the landscape to improve resilience. The final chapter in part 1, by Momani and Bélanger, examines how the pandemic has shed light on the vulnerabilities related to Canada's critical infrastructure. They argue that the digitalization of critical infrastructure—including energy and utilities, the financial system, food systems, transportation, health systems, etc.—combined with the pressures of the pandemic expose these systems to cyber attacks and therefore needs added policy attention.

The second part of the book contains ten chapters and looks at how several sectors of the Canadian government responded to the pandemic. Davis and Corbeil, in chapter 5, examine the use of intelligence collection and surveillance techniques against the pandemic, and explore the ethics of this type of surveillance. They conclude by delving into the potential utility of a health intelligence priority for Canada. In the next chapter, Carvin examines how the pandemic and subsequent lockdowns impacted national security operations. Based on interviews with individuals who work in the intelligence community, Carvin explores how national security agencies managed the need to revolutionize the way they do business while facing an unprecedented surge in demand for security advice and assistance. She concludes by examining the lessons learned and the implications for the future. Robinson, in the next chapter, examines the impact of the pandemic on the Communications Security Establishment (CSE). One of the challenges, he notes, was the urgent task of ensuring the electronic security of the Government of Canada as public servants shifted overwhelmingly to working from home. Additionally, he describes how protecting the country's health system and research institutions from pandemic-related cyber threats became a top priority.

Moving on to the impact of the pandemic on the Canadian Armed Forces (CAF), Saideman, von Hlatky, and Hopkins compare and contrast domestic and international operations, noting that while the pandemic dramatically influenced how the CAF operates within Canada, the external effects varied based on the type of unit involved and what they were doing. They conclude the chapter by examining some of the implications for present and future CAF operations. Cox, in the next chapter, examines the Defence Intelligence Enterprise, which provides strategic and operational intelligence to deployed CAF military missions at home and abroad. With the pandemic, authorities imposed decisive health-care restrictions across the Department of National Defence and the CAF. Initially, defence intelligence activity was dramatically slowed and reduced. By the end of the summer, 2020, Cox argues, the Defence Intelligence Enterprise had found its "sea legs" and, thanks to several procedural and workforce adjustments, returned to a more comfortable, but no less hectic, level and pace of activity.

In the next chapter, Lee and Piper delve into the Global Public Health Intelligence Network (GPHIN), an initiative launched two years after the 2003 SARS outbreak. GPHIN, Lee and Piper argue, underwent political and financial challenges just when such a network was needed most. They identify key lessons learned and ways forward for reviving GPHIN's role as a critical component of Canada's core public health capacities and global health security. In the next chapter, West unpacks the debate about whether existing legal authorities and emergency legislation permit the Canadian government to retool state resources—especially the surveillance apparatus—to help with public health demands, such as contact tracing and enforcement of public health measures.

Nesbitt and Hansen, in the next chapter, take a close look at how the pandemic "stress-tested" the criminal justice system in Canada. The result, they argue, is that the system has been asked to show its capacity to respond to *increased* national security threats—be they foreign espionage and disinformation campaigns, politically or ideologically motivated extremism, and pandemic-specific enforcement actions—all while operating with a *reduced* capacity to respond and prosecute.

Next, Wallace looks at the impact of the pandemic on the Canada Border Services Agency. He argues that while the pandemic all but required a total suspension of the agency's deportation program, things will not simply go back to normal after the pandemic is over. According to Wallace, there are real legal and practical impediments to deportation that will emerge as the pandemic fades. In the last chapter, Rayes and Sahloul argue that should another large-scale disease threaten the health and safety of the global community, the national security apparatus of the United States must work closely with its Canadian counterparts as well as the global community at large to engage BIPOC communities. The goal, they argue, is to create best practices that reduce the disproportionate impacts of any disease, as such action is key to maintaining the economic strength and security of marginalized and vulnerable communities.

Finally, in the conclusion, Juneau provides an overview of the key questions this edited collection sought to answer: the extent to which Canada's national security and intelligence community was ready to face the pandemic at its onset; how the threat environment changed during the pandemic; how the community adjusted; and the longer-term implications.

Recommendations

We conclude this introduction with a series of recommendations for the Canadian national security and intelligence community on how it could better prepare for future public health emergencies. These recommendations, based on the more detailed analysis in the following chapters, are divided into three categories: threat assessments, tools, and lessons learned.

Threat Assessments

This collection demonstrates that many of the threats Canada faced during the pandemic were not new but rather arose from the intensification of pre-existing trends. This is especially true in the online space. Wilner and Babb thus recommend that Canada's national security and intelligence community should continue to pay close attention to online activities seeking to undermine the Government of Canada, to recruit new members to terrorist organizations and extremist groups, and to incite or motivate acts of violence. These threats are proliferating worldwide, and Canada is no exception.

The 6 January 2021 insurrection at the Capitol in Washington, DC, as well as multiple other acts of violence since March 2020, also make clear that the spread of disinformation and conspiracy theories represents a threat to national security. Canadian policy-makers should therefore consider how to take a more proactive approach to fostering critical thinking and digital literacy. Amarasingam and Argentino emphasize that the pandemic may, in hindsight, be a practice run for other disasters to come. As a result, they recommend that the government take an inventory of the lessons it has learned.

Critical infrastructure can be particularly vulnerable to cyber attacks. Of course, this exposure existed before 2020, but it intensified as the pandemic accelerated the shift to the digitalized world. As Momani and Bélanger explain, some of these risks are further complicated by the fact that Canada's critical infrastructure has shifted from public to private ownership and control, adding new actors to the equation. Momani and Bélanger therefore argue that there is a need for better coordination among these multiple actors, both public and private, since a lack of information sharing and co-operation often represents a vulnerable point in cyber attacks on critical infrastructure.

Additionally, the pandemic intensified pre-existing concerns about the security of supply chains and, more broadly, about the links between the economy and national security. Carvin and a group of her students thus raise the thorny question of the appropriate role of governments in protecting elements of the economy with strategic or national importance, especially the manufacturing of personal protective equipment and the security of food supplies. They argue that the federal government must do more to prepare supply chains for long-term global disruptions in an era of adversarial geo-economic strategies. In particular, they recommend that the government implement initiatives to increase the economy's resilience and self-sufficiency in specific sectors. More broadly, they recommend that, given the likelihood of future disruptions of the type seen during the pandemic, future national security discussions should give greater weight to concerns around the management of supply chains.

Tools

To date, Canada has not employed national security tools and practices to track the spread of COVID-19. However, the pandemic has provided further impetus for the national security and intelligence community to intensify a trend of recent years: increased collaboration with non-traditional partners elsewhere in the federal government, in sub-national levels of government, and in the private sector.

There has been much media attention on GPHIN in particular, a Canadian initiative to gather and disseminate epidemic intelligence. According to critics, including scientists within the federal government, GPHIN's role became steadily less prominent over the years until the Liberal government reallocated its resources in 2019. However, as the chapter by Lee and Piper explains, the pandemic demonstrated the need for renewed investment in an epidemic intelligence system. Moreover, they recommend that such a public health intelligence system be better integrated with the Canadian health system and other parts of the government, including the intelligence community.

Similarly, Davis and Corbeil argue that greater integration and information-sharing between the traditional security and intelligence community and the health intelligence community could produce earlier warning and, by extension, lead to better policy responses in future public health crises. Nevertheless, they remind us that there are real concerns with a possible expansion of the Canadian intelligence community's mandate to include health intelligence. These concerns include already existing resource shortages, the need to identify the right use of tools and technologies, and questions of proportionality and privacy. Therefore, they conclude that a wholesale adoption of health intelligence as a national security and intelligence priority might be premature, and they argue instead for better integration and information-sharing.

The chapter by Rayes and Sahloul explains how the pandemic has highlighted the public health, social, economic, and political challenges facing minority communities in the United States and Canada. They assess how these outcomes could have been mitigated with higher-quality data, and how data can be integral to preventing future national and global security threats. In this context, they recommend that the Canadian government engage in more thorough and transparent data collection on how public health emergencies affect minority communities.

Looking forward, the federal government should also reflect on the legal tools at its disposal. Two key debates that emerged during the pandemic were whether Canada's surveillance apparatus could be leveraged in a public health crisis and whether the federal government could mandate that individuals or telecommunication service providers share location data generated by wireless devices with health or security agencies. In her chapter, West argues that the answer in both cases is negative. Should lawmakers ultimately determine that it is appropriate to leverage the tools and techniques developed by CSIS and CSE to face future public health emergencies, West recommends, among other initiatives, that they consider amending the federal *Emergencies Act* to authorize the collection of information in a public welfare emergency or expanding CSE's assistance mandate to include provincial health authorities.

For their part, Nesbitt and Hansen explain how Canada's criminal justice system was put under significant stress by the pandemic, notably because of increases in certain types of criminal behaviour, such as cyber scams. In addition, Canada saw an increase in ideologically motivated extremism, particularly on the far right. As a result, they recommend the development of a strategy to better prioritize criminal investigations and prosecutions. This exercise should, in their view, include critical thinking on how to investigate and prosecute emerging threats, especially online criminality, financial crimes, fraud, and the spread of mis- and disinformation.

Lessons Learned

As the national security and intelligence community adapted to the pandemic, it learned useful lessons. Some of them, clearly, will be of limited value once the pandemic is over. Others, however, can be applicable, even if only partially, in the post-pandemic world to help the community improve its performance. At the very least, we therefore strongly recommend that the community commit to a serious lessons-learned exercise. This should provide an official record—some of which should be made public—of how the community adapted its operations, and where it succeeded and failed. To be most effective, this effort should be led by the

National Security and Intelligence Advisor and include participation from the heads of all relevant departments and agencies. The two main review and oversight bodies, the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency, should also consider examining the community's performance during the pandemic.

This lessons-learned exercise—similar to after-action reports prepared by the military—could include, in particular, how working from home can—and cannot, as the case may be—continue after the pandemic. As discussed in many chapters—notably by Carvin, Cox, and Robinson—there are some benefits to continuing this practice, albeit arguably in a limited form. Similarly, because so many of the intelligence community's employees have been working from home on at least a part-time basis, the pandemic has forced agencies to intensify their use of open-source information and analysis. Here, too, there are potential long-term benefits to incorporating these valuable lessons.

Finally, the pandemic forced difficult choices onto the community. Working at a reduced capacity, departments and agencies had to choose which activities they needed to stop or reduce. As discussed, for example, in the chapter on CAF operations by Saideman, von Hlatky, and Hopkins, the military was forced to determine which of its activities were vital priorities that could not be curtailed. The temptation here will often be to simply resume all or most of these activities as the pandemic subsides in 2021 and 2022. This would be a wasted opportunity. Vested interests and inertia often make it difficult for bureaucracies to jettison or significantly downsize programs. The gradual end of the pandemic presents a golden opportunity to engage in a comprehensive review of the community's priorities and to reallocate resources to tackle the next generation of security threats.

Acknowledgements

The editors would like to thank all of the contributors for agreeing to undertake this project during incredibly demanding times: your commitment to timely and relevant research is an inspiration. We are also grateful to the Privy Council Office's Intelligence Assessment Secretariat for

partnering with us on this project. The organization's willingness to engage in this study made this work stronger and, we hope, more relevant for those in the national security and intelligence community. We also want to thank the Social Sciences and Humanities Research Council for awarding us a Partnership Engage Grant, as well as Mobilizing Insights in National Defence and Security (MINDS), the Department of National Defence's engagement program, for their financial support for this project. Thank you also to the Centre for International Policy Studies (CIPS) at the University of Ottawa, the Faculty of Public Affairs at Carleton University, and the Canadian Association for Security and Intelligence Studies (CASIS) for hosting a series of webinars in early 2021 where contributors presented their work. Additionally, we want to thank our incredible team of research assistants: Jake Norris, who was with us from start to finish, Peter Shyba, and Anne-Marie Chevalier. We also wish to thank everyone at University of Calgary Press for their help in making this book a reality, from grant application to publication, in less than eighteen months, especially Brian Scrivener and Ryan Perks. Stephen Ullstrom also prepared the index.

Finally, a profound thank-you goes out to Stephanie Carvin, Michael Nesbitt, Jessica Davis, and Craig Forcese for your help in shaping this project and your steadfast support throughout this process.