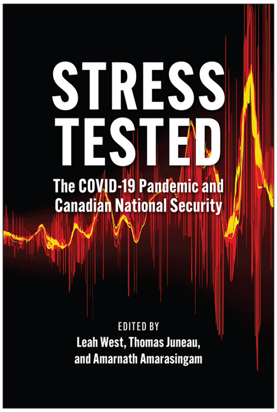
UNIVERSITY OF CALGARY
Press


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

7

Collection and Protection in the Time of Infection: The Communications Security Establishment during the COVID-19 Pandemic

Bill Robinson

Introduction

For the Communications Security Establishment (CSE), Canada's national cryptologic agency, the COVID-19 pandemic has presented great challenges, but it has also presented opportunities. A free-standing department housed in the portfolio of the Minister of National Defence, CSE has two primary missions: protecting the electronic communications, data holdings, and information-processing activities of the federal government and other designated institutions from theft or interference (known as information technology security [ITSEC], or more recently cyber security); and providing intelligence on the electronic communications, data holdings, and information-processing activities of foreign governments and other foreign entities of interest (known as signals intelligence [SIGINT]). Like all government institutions, CSE has faced the simultaneous challenges of maintaining essential operations and protecting its workforce from the pandemic. But COVID-19 also posed the urgent new task of ensuring the electronic security of public servants across the government who were suddenly directed to work from home. Protecting the country's health system and research institutions from pandemic-related cyber threats also became a top priority. Meanwhile, the demands for intelligence production levied on the SIGINT side of the agency remained as high as ever, while new pandemic-related intelligence concerns arose and pressure to exploit the intelligence-gathering opportunities presented by COVID-19 was probably also high.

This chapter looks at the challenges that the COVID-19 pandemic has posed for CSE, focusing first on the agency's cybersecurity role and then on its signals intelligence role. It then looks at the special problems of workforce protection posed for CSE by the fact that much of its work cannot be performed outside the office. The concluding section considers whether CSE's experience during the pandemic holds lessons for the agency's future operations.

When the COVID-19 pandemic arrived, CSE was already in the midst of adapting to major changes in its mission and operating environment. Among other measures, Bill C-59, adopted in mid-2019, included the *Communications Security Establishment Act*, a sweeping overhaul of the statute governing the agency's operations that added to its mission the conduct of offensive and defensive cyber operations. C-59 also replaced the oversight and review mechanisms for the agency, establishing entirely new organizations with broadened mandates (see Bill C-59, *An Act Respecting National Security Matters*, S.C., 2019, c. 13). The agency was also still adjusting to the 2018 creation of the Canadian Centre for Cyber Security, which amalgamated under CSE the IT security branch of the agency and most of the cybersecurity elements of Shared Services Canada[1] and Public Safety Canada (CSE 2018). The Cyber Centre, as it is often called, was still in the process of consolidating these disparate elements into a unified organization and moving its core operations to a new headquarters when the pandemic struck. CSE had to accommodate these changes and adjust to continuing technological flux across the agency's mission areas while absorbing ongoing staff and budget growth in both the cybersecurity and SIGINT programs. CSE has tripled in size since 2001, and it may still be growing (Robinson 2021a). The arrival of COVID-19 added an entirely new set of challenges with respect to operational priorities, operational tempo, and workforce safety.

Cybersecurity Operations

The most obvious effects of the pandemic have been on the cybersecurity side of CSE's operations. The federal government's March 2020 decision to quickly transition as much of the public service as possible to working from home created an enormous increase in demand for secure online access to government IT systems. As the technical authority on cybersecurity issues for the federal government and operator of its cyber defence systems, CSE has played a key role in supporting the rollout of pandemic-related online services for the Canadian public and the efforts of Shared Services Canada to provide secure and reliable services for online meetings of cabinet, virtual meetings of Parliament, and online access to government IT systems and databases by public servants at a scale far in excess of anything previously envisaged. The government provided an additional $114 million in October 2020 to support these efforts, of which $6.3 million went to CSE (Treasury Board of Canada 2020, 1-15). The agency also received a $47 million increase in budget authority in February 2021, but the portion of that sum that was related to pandemic efforts has not been disclosed (Treasury Board of Canada 2021, 2-15).

In addition to supporting the activities of the federal government, the Cyber Centre has provided cybersecurity advice and services to Canadian public and private health institutions and other pandemic-related private-sector activities such as vaccine research and development. The kinds of threats that such entities face include

- criminal efforts to steal and sell intellectual property (IP) or to use "ransomware" to encrypt the computer systems and data of vital institutions and demand payment for their decryption;
- state-sponsored efforts to steal IP or other confidential pandemic-related information; and
- efforts by states or other malicious actors to sabotage Canadian pandemic response efforts.

In addition to issuing its own public warnings and advisories directed at the health sector (e.g., CSE 2020b, 2020e, 2020h), the Cyber Centre issued at least one joint advisory with the Canadian Security Intelligence Service (CSIS 2020). The Cyber Centre also joined its counterparts in the United Kingdom and the United States to issue a public warning in July 2020 about the efforts of Russian intelligence services to steal "information and intellectual property relating to the development and testing of COVID-19 vaccines" (CSE 2020a). To help research organizations assess whether their systems had been compromised, the accompanying advisory included technical details of the tactics, techniques, and procedures used by the Russian intelligence services. More targeted outreach was also undertaken. During the first year of the pandemic,

> the Cyber Centre established new partnerships with over 100 health sector organizations, including provincial and territorial regional health authorities, patient care facilities, and organizations involved in the development, manufacture and delivery of COVID-19 vaccines. . . . Throughout 2020 the Cyber Centre held weekly video calls with over 100 representatives from the health sector to share practical advice and answer questions about cyber threats. In 2021, these calls are continuing on a bi-weekly basis (CSE 2021a).

The Cyber Centre also assisted in the development of a "cyber-survey tool to provide health sector organizations such as hospitals, doctors' offices and long-term care facilities, among others, with an easy-to-use tool to assess the cybersecurity of their organization" (Standing Committee on Health 2020, 21).

Since the passage of the *CSE Act*, the Minister of National Defence has had the option to designate entities outside the federal government (e.g., telecommunications companies, electricity providers, other levels of government) as infrastructures of importance to the Government of Canada. This designation opens the way for the Cyber Centre to provide additional services to these entities, such as monitoring the activity on their IT networks. However, such assistance can only be provided following a formal request from the recipient and, if required by the type of assistance sought, the issuance of a valid ministerial authorization. Cyber Centre head Scott Jones has testified that such support is offered only in special cases of particular importance where commercial cybersecurity services are unlikely to be sufficient (Standing Committee on Industry, Science and Technology 2020, 15). The government will not confirm whether any organizations associated with Canada's pandemic response have received this designation or are being provided such services.[2]

Publicly available information suggests that Canada's health institutions have weathered these threats quite well. According to the Cyber Centre, "a Canadian biopharmaceutical company was compromised by a foreign cyber threat actor almost certainly attempting to steal its intellectual property" in April 2020 (CSE 2020e). The first publicly identified intrusion, minor in its effects, hit a hospital network in Montreal in October 2020 (Tu and Freeze 2020). Two months later, CSE reported that "multiple Canadian hospitals have suffered ransomware attacks in recent months," referencing the Montreal case in particular (CSE 2020d). Overall, the Cyber Centre "issued over 20 cyber alerts to health sector partners and provided incident response support in more than 85 cases affecting the sector" in 2020–21 (CSE 2021a). To date, however, no major incidents have been identified.

Another role of the Cyber Centre is to provide cybersecurity advice and guidance to the broader Canadian public. Since the start of the pandemic, this has included advice on avoiding online hazards such as malicious websites, emails, and texts that seek to exploit COVID-19 concerns to deliver malware or collect personal data, including sites imitating Government of Canada sites offering COVID-19 information or pandemic income support and other services (CSE 2020c, 2020d). The Cyber Centre has also worked proactively with industry partners, including commercial and international Cyber Incident Response Teams, to shut down such activities, and it provides lists of malicious websites to the Canadian Internet Registration Authority's "Canadian Shield" domain name server, which automatically protects users of that service from connecting to them. Between March 2020 and July 2021, the Cyber Centre contributed to the removal of "more than 8,600 websites, social media accounts, and email servers impersonating the Government of Canada" (CSE 2021b). The Cyber Centre also produced a security assessment of the COVID Alert mobile app launched by the government in July 2020 to notify users of possible exposures to the virus (CSE 2021c).

Active cyber operations (ACO) and defensive cyber operations (DCO) have been another potential avenue for action by CSE. These could be used, for example, to interfere with the computer systems of malicious cyber actors targeting Canadians. The power to conduct such activities, more commonly called computer network attack or cyber attack operations, is a new element of CSE's mandate, granted only in 2019. Each operation requires specific ministerial approvals (CSE 2020f). CSE has begun receiving such approvals (NSIRA 2020, 25), but the agency will neither confirm nor deny that ACO/DCO measures have been employed for COVID-19-related matters.[3] Cyber operations have been characterized by the Cyber Centre as a last-resort measure, and thus their use, if any, has probably been limited. For now, the agency will state only that it "continues to leverage all aspects of our mandate to ensure that Canada is protected against cyber-threats and that the Government of Canada has access to information that can help inform decisions on Canada's approach to COVID-19" (Standing Committee on Government Operations and Estimates 2020, 10). CSE's Five Eyes partners have been more forthcoming on this question, with Australia (Australia 2020) and the United Kingdom (Fisher and Smyth 2020) both confirming the use of cyber attack capabilities against COVID-19-associated targets.

SIGINT Operations

The SIGINT side of CSE accounts for about 70 per cent of the agency's staff and budget resources (Robinson 2021a). Mandated to produce intelligence in response to Canadian government priorities (and also to conduct cyber operations), this part of the agency is by necessity even less forthcoming about the details of its work. However, it is likely that the advent of the pandemic has led to a rebalancing of the agency's intelligence-collection and intelligence-production priorities.

Collecting intelligence in support of the agency's cybersecurity activities—monitoring the plans, activities, and capabilities of foreign cyber threat actors—was already an important pre-pandemic role on the SIGINT side. Given the sweeping new vulnerabilities that were created across Canada in both the public and private sectors by the shift to working from home, it is likely that cybersecurity support was given even higher priority during the pandemic. Other COVID-19-related intelligence is also likely to have been a high priority. Probable topics of interest include pandemic-related developments and plans in other countries, particularly those suspected of withholding information from the international community, and intelligence about activities that might undermine Canada's pandemic response. In addition to threats to IT systems, the latter might include theft of intellectual property or disruption operations such as cyber-enabled influence campaigns that seek to undermine Canada's COVID-19 response or leverage concerns about the pandemic to advance other agendas (CSE 2021a). CSE may also have sought intelligence in support of Canadian COVID-related procurement activities abroad, such as information about the availability and quality of supplies of personal protective equipment and, conceivably, confidential details of foreign vaccine and treatment technologies.

The likely consumers of intelligence on topics such as these would include CSE's primary customers—the Privy Council Office and Prime Minister's Office; Global Affairs Canada; the Canadian Security Intelligence Service; the Royal Canadian Mounted Police; and the Department of National Defence/Canadian Armed Forces—but also Innovation, Science and Economic Development Canada; Public Services and Procurement Canada; and of course, Health Canada. Even before the pandemic, CSE had a memorandum of understanding in place with Health Canada governing the provision of SIGINT to both the department and the Public Health Agency of Canada. The agreement, signed in 2008, specifically noted that "A key focus of [Health Canada] is to maintain a pandemic preparedness plan" (CSE 2008). CSE has not revealed, however, whether it actually collected and provided Health Canada with any information useful for pandemic warning or preparedness in the period prior to the emergence of the COVID-19 pandemic, or whether such information, if provided, was employed in any way in subsequent decision-making.

In addition to pandemic-related questions, CSE's pre-pandemic intelligence priorities—encompassing permanent concerns such as North American security, counterterrorism, diplomatic and prosperity issues, and support to military operations—have remained important. Emphasis may have been reduced on some of these priorities as a short-term measure, but it is also likely that temporary collection opportunities have arisen across many topics as a result of the global shift to working from home and other disruptions caused by the pandemic. The agency will have wanted to seize those opportunities while they existed, not only to collect information in the moment but to establish footholds in target IT systems that CSE may be able to exploit after the return to more normal conditions.

The combination of these factors—new pandemic-related priorities and persisting priorities with new opportunities—means that pressure to maintain a high operations tempo on the SIGINT side will have been high.

The agency "reinvented" the way it packaged its intelligence reports in 2020–21 "to provide critical information about the pandemic more quickly, and in a more digestible format. We also adjusted our dissemination approach to be able to securely deliver timely intelligence to a wider group of government clients, including clients working remotely." However, the number of SIGINT clients served by CSE fell significantly—from 2,100 in 2019–20 to 1,450 in 2020–21—probably reflecting a lack of secure delivery options for lower-priority clients working from home (CSE 2021a).

Another motive for maintaining operations on the SIGINT side of the agency is to sustain the large inflows of data and reporting that CSE receives from partner agencies. Canadian reports account for less than 10 per cent of the SIGINT reports typically available to Canadian SIGINT customers, with most of the remainder coming from CSE's Five Eyes partners, primarily the National Security Agency (NSA) in the United States, but also the United Kingdom's Government Communications Headquarters, the Australian Signals Directorate, and New Zealand's Government Communications Security Bureau (Robinson 2020, 105). It is also vital to CSE and the wider Canadian intelligence community that CSE maintain its own provision of data and reporting to its foreign partners. The privileged access that Canada has to the output of its intelligence partners depends ultimately on the continuing contribution that Canada makes to the collective intelligence pool. As Canada's main collector of foreign intelligence, CSE is the primary Canadian contributor to that pool, providing intelligence end product reports and other reporting produced by CSE and the Canadian Forces Information Operations Group, the military organization that collects SIGINT for CSE and the Canadian Armed Forces;

bulk metadata ("minimized" to withhold information about Canadians); and communications intercepts collected by Canada on behalf of partner agencies. Intercepts acquired for partners are collected using selectors (email addresses, phone numbers, etc.) supplied by those partners and examined by CSE collection managers to ensure they are consistent with Canadian priorities and directions on intelligence collection and do not target Canadians or persons in Canada. If approved, they are then forwarded to Canadian collection systems (CSE 2012, 21). Canada's Five Eyes partners would surely sympathize if pandemic response measures caused some disruption to these activities, but they would also take note, and the continued operation of these approval, collection, and forwarding processes has undoubtedly been given very high priority by CSE.

Workforce Protection Issues

Like other parts of the intelligence community, CSE has faced special difficulties in balancing its need to maintain a high operational tempo with its need to protect its workforce from COVID-19. Public servants across much of the federal government have been able to work from home during much of the pandemic, but this option is not available to those whose work can only be done in high-security office spaces. A large part of CSE's work, especially on the SIGINT side of the agency, cannot be done from home or even in a normal office, but must be carried out within CSE's "secure compartmented information facility" (SCIF) spaces within its headquarters, the Edward Drake Building. This is a requirement not just of the Canadian government, but also of CSE's Five Eyes partners. As noted above, much of the SIGINT data and reporting that CSE is able to draw on to support its Canadian clients originates with those partners, and the sharing of that material with CSE is contingent on Canada's continued observance of the agreed security procedures for its handling.

CSE would not provide information on the extent to which SIGINT personnel may have been directed to stay at home at various points during the pandemic, on the grounds that this would be too revealing of the agency's capabilities.[4] However, some information is available about other parts of the Canadian intelligence community. The Canadian Forces Information Operations Group reduced peak-hours staffing at its main intercept station at Canadian Forces Station Leitrim in Ottawa by as much as 40 per cent from late March to May 2020, with occupancy returning to near-normal levels only in the fall (Robinson 2021b). Similarly, the Integrated Terrorism Assessment Centre (ITAC), located next door to CSE in the CSIS building, cut back the number of people working in its offices by as much as 80 per cent during the early days of the pandemic. Even by mid-summer 2020, the number of people working in ITAC spaces was only half the normal level, while by the fall, following renovations to improve the safety of the centre, around three-quarters of personnel were back.[5] CSIS seems to have followed a broadly similar trajectory with its own personnel at its Ottawa building (Robinson 2021b).

A comparison with other Five Eyes SIGINT agencies can also be instructive. Even in New Zealand, which was highly successful in suppressing the spread of COVID-19, the Government Communications Security Bureau initially "reduced staffing levels and limited staff numbers around [its] facilities by moving to shift working, with weekly rotations" (New Zealand 2020). Similarly, NSA and GCHQ, the American and British SIGINT agencies, both implemented sharp reductions in workforce attendance around the end of March 2020, followed by a gradual return to higher occupancy over the summer and fall. Interestingly, the major COVID-19 waves of the winter of 2020–21 and the spring of 2021 do not seem to have caused a similar retreat by these agencies, possibly indicating that modifications to occupancy practices and the workspaces themselves were by that time considered sufficient to protect their workforces (Robinson 2021b). It seems likely, therefore, that CSE applied at least some reductions in office occupancy during the pandemic's first wave in the spring of 2020. CSE may also have made some changes during the second and third waves (Robinson 2021b).

The problem of secure workspaces is much less acute on the cybersecurity side of CSE, where a portion of the Cyber Centre's work must be conducted in a SCIF, but much can also be performed at lower levels of classification, including, in many cases, the unclassified level. In fact, when the pandemic hit, the Cyber Centre was in the process of moving most of its personnel from the high-security Edward Drake Building on Ogilvie Road to new leased spaces in a commercial building at 1625 Vanier Parkway. Close to 800 of CSE's 3,000 employees will eventually be housed in this building. Many of these employees have been able to work from home, communicating with the office and each other over a CSE virtual private network suitable for material up to the Protected B level. Only when higher-security matters arise have they had to come into one of the buildings, where they can work on the "high side." This has also meant there is spare space in the Vanier Parkway building where other CSE employees, such as administrative support personnel, can work if they need office accommodations but not Drake-level security. CSE has acknowledged that it was "very fortunate" to have this space available when the pandemic arrived.[6]

The combination of work from home and the shift of Cyber Centre and other employees to the Vanier Parkway building will have made it much easier for CSE to provide physically distanced workspaces for those members of the workforce who do require the Edward Drake Building for most of their work. SIGINT analysts spend part of their time staying current with news reports and other open-source information related to their SIGINT targets, and although they would have to be careful to avoid revealing those targets, they could in principle read this sort of unclassified material at the Vanier Parkway offices, or possibly at home. Still, the great bulk of SIGINT work can only be performed in the Edward Drake Building. Here, too, CSE argues that it has been fortunate in that the Edward Drake Building is a new facility (occupied only in 2015) featuring a modern and efficient ventilation system.[7] At the time of its construction, the workspaces in the building were reportedly entirely open concept, with separate rooms for meetings but no private offices (Weston 2013) (Pod 1 of the complex, CSE's high-performance computing centre, may be an exception as it was constructed as part of a separate project). The open nature of the building has probably eased the problem of ensuring appropriate physical distancing of the SIGINT workforce. According to the agency, among other measures, it has

> staggered and reconfigured workstations to ensure two metres of physical distancing. We have significantly increased cleaning and sanitization of our facilities, focusing on high-touch surfaces. There are hand sanitization stations throughout our facilities. We have closed or reconfigured many of our

> common areas. Masks are mandatory any time employees are not seated at a safely distanced desk.[8]

Another way to enhance physical distancing within the Edward Drake Building is to utilize the building more intensively outside traditional office hours. A portion of the CSE workforce has always been on shift work to provide a minimal 24/7 operations capability, but this is quite small, leaving the building largely unoccupied during nights and weekends. When employees currently working primarily at home need to visit the office, the agency has sought to schedule those visits during these less crowded times.[9] CSE has also acknowledged "staggering [its] work schedules" (CSE 2021a), but it is not clear whether the agency made any effort to move a significant number of traditional day workers to other shifts. Shift work is never popular and would pose great problems for some employees, but it might be workable as a relatively limited and short-term expedient. The collective agreement CSE has with the Public Service Alliance of Canada enables the agency to schedule shift work when needed to meet its operational requirements (CSE 2015), and it is possible that it undertook some effort to transfer work outside of the normal Monday-to-Friday day-shift hours. Some agencies in the US intelligence community reportedly did this, moving "their employees and contractors into rotating shifts, where some worked from 6 a.m. to 2 p.m., and a new group came into the classified office space to work from 3 to 11 p.m." (Ogrysko 2020). The NSA may have been one of the agencies that did this at some points during the pandemic (Robinson 2021b).

Another workforce-protection measure has been the conversion of public events to an online format. For example, CSE's GeekWeek conference, an annual unclassified event designed to "foster collaboration between the Government of Canada, critical infrastructure partners and academic researchers to address vital problems facing the cyber security industry," was held entirely online in 2020 (CSE 2020g). University recruitment events have also been moved online, as have student internships. In a typical year, CSE hosts up to four hundred students on three-month internships, but during the pandemic all interns have worked exclusively from home.

CSE's workforce-protection measures appear to have been successful, as the agency reported that no cases of workplace transmission of the virus were recorded during 2020–21 (CSE 2021a). (No information is available about cases that may have occurred later in 2021, during the third and fourth waves of the pandemic.)

Work-life balance is another aspect of workforce management that CSE will have had to address. With the closure of schools and daycares for extended periods during the pandemic, employees with young children have had to juggle job requirements with the need to provide full-time child care, a task that commonly falls disproportionately on women. In 2017–18, women accounted for 37.3 per cent of the CSE workforce, with approximately half working in "a corporate function" such as policy, administration, and public communications (NSICOP 2020, 20). Such jobs are more likely than most at CSE to be at least partly transferable to home, which could ease the problem for those workers of ensuring that someone is available to supervise children or other dependents, but it also increases the probability that this task will fall more heavily to women. Meanwhile, for those members of the CSE workforce who must work at the office, flexible hours may ease the problem of meeting dependent-care requirements somewhat, but for others who may be required to work unusual shifts, such difficulties could be exacerbated. CSE will have had to adjust its expectations of its employees' productivity to account for the effect that increased dependent-care responsibilities have had on its workforce, particularly women. In March 2021, "CSE hosted a virtual panel discussion where six employees spoke frankly about the disproportionate impact of COVID-19 along gender lines" (CSE 2021a). The agency will also have had to consider the mental health needs of its workforce and remain alert to the consequences of pandemic-related stress. In response to such concerns, CSE reports that it "held training courses and speaker events on topics such as self-compassion, managing anxiety and parenting in the pandemic" (CSE 2021a).

Assessing Performance and Looking to the Future

Whatever the exact menu of measures applied by CSE to maintain its operations, at the end of 2020 the agency asserted that it had succeeded in remaining fully operational during the pandemic (CSE 2020i). The secrecy surrounding the agency's activities makes judging the success of those operations difficult. The COVID-19-related cybersecurity incidents made public to date have been minor in scope and consequences, with no evidence of any significant effect on Canada's federal or non-federal pandemic response. CSIS has confirmed that the intelligence community is "aware of the efforts of state adversaries to spread disinformation about pandemic responses in an attempt to discredit government efforts and diminish confidence in vaccine rollout efforts" (CSIS 2021), but these threats, while concerning, appear to have been marginal in their effects. Hostile intelligence-gathering activities against Canadian targets are more difficult to assess. The rapid move to working from home across the public and private sectors is likely to have opened new opportunities for hostile exploitation, but many of these intrusions may go undetected or otherwise remain unreported. The success of CSE's own intelligence-gathering efforts is even less likely to be revealed.

In some ways, the COVID-19 pandemic may have served as a preview of the issues the Cyber Centre will face in the future as work migrates outside the traditional office. Are there lessons from the current experience that can be applied to the design of more permanent, secure remote-work capabilities? The pandemic period may also have accelerated the agency's understanding of how best to operationalize the cybersecurity authorities it was granted in 2019 to work with entities outside the federal government. Was the Cyber Centre's advice and guidance used effectively by the organizations that needed it? Is the voluntary participation model laid out in the *CSE Act* sufficient for the most vital elements of Canada's critical infrastructure?

One lesson that CSE and other essential elements of government might draw from the COVID-19 pandemic is that they need to develop the infrastructure and procedures to securely perform work outside of existing high-security office spaces when emergencies require it. Such an option would improve the agency's resilience against a wide range of threats that might constrain the use of CSE facilities in the future, not just pandemics. However, it would likely require the relaxation of certain security requirements, which would need to be negotiated with the other members of the Five Eyes partnership. The time to do that is before the next emergency arises. The agency might also want to examine greater use of remote work even under normal circumstances, as Gioe, Hatfield, and Stout (2020) have suggested for the US intelligence community.

NOTES

[1] Shared Services Canada is the Canadian government agency responsible for providing information technology services to the federal government.

[2] Christopher Williams, Director General, Public Affairs at CSE, email message to author, 22 February 2021.

[3] Email from Christopher Williams.

[4] This information was provided during a 23 October 2020 online meeting between members of the Canadian intelligence community and authors for this book.

[5] 23 October 2020 meeting.

[6] 23 October 2020 meeting.

[7] 23 October 2020 meeting.

[8] Email from Christopher Williams.

[9] 23 October 2020 meeting.

REFERENCES

Australia. Department of Defence. 2020. “On the Offensive against COVID-19 Cyber Criminals.” 7 April 2020. https://www.minister.defence.gov.au/minister/lreynolds/media-releases/offensive-against-covid-19-cyber-criminals.

CSIS (Canadian Security Intelligence Service). 2020. “Joint CSE and CSIS Statement—May 14, 2020.” Government of Canada, last modified 28 May 2020. https://www.canada.ca/en/security-intelligence-service/news/2020/05/joint-cse-and-csis-statement.html.

———. 2021. “Remarks by Director David Vigneault to the Centre for International Governance Innovation.” Government of Canada, 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.

CSE (Communications Security Establishment). 2008. “Memorandum of Understanding between the Communications Security Establishment and Health Canada.” 12 February 2008. Released to the author in redacted form under Access to Information request A-2017-00017.

———. 2012. *OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*. 1 December 2012. Released to the author in redacted form under Access to Information request A-2017-00017.

———. 2015. "Collective Agreement between the Communications Security Establishment and the Public Service Alliance of Canada." 11 February 2015. http://negotech.labour.gc.ca/eng/agreements/12/1292005a.pdf.

———. 2018. "The Minister of National Defence Announces the Launch of the Canadian Centre for Cyber Security." Government of Canada, last modified 16 October 2018. https://cyber.gc.ca/en/news/minister-national-defence-announces-launch-canadian-centre-cyber-security-0.

———. 2020a. "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.

———. 2020b. "Cyber Security for Healthcare Organizations: Protecting Yourself against Common Cyber Attacks." Government of Canada, September 2020. https://cyber.gc.ca/sites/default/files/publications/itsap00131-e.pdf.

———. 2020c. *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity*. Government of Canada, last modified 10 June 2020. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity.

———. 2020d. *Cyber Threat Bulletin: The Continued Impact of COVID-19 on Cyber Threat Activity*. Government of Canada, last modified 21 December 2020. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-continued-impact-covid-19-cyber-threat-activity.

———. 2020e. *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threats to the Health Sector*. Government of Canada, last modified 25 June 2020. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threats-health-sector.

———. 2020f. "Foreign Cyber Operations." Government of Canada, last modified 27 October 2020. https://www.cse-cst.gc.ca/en/inside-interieur/cyberoperations-cyberoperations.

———. 2020g. "GeekWeek 7." Government of Canada, last modified 21 October 2020. https://cyber.gc.ca/en/events/geekweek-7.

———. 2020h. "Renewed Cyber Threats to Canadian Health Organizations," Alert AL20-026. Government of Canada, 30 October 2020. https://cyber.gc.ca/en/alerts/renewed-cyber-threats-canadian-health-organizations.

———. 2020i. "#YearInReview: In just a few short months . . ." Twitter post (@cse_cst), 31 December 2020, 12:59 p.m. https://twitter.com/cse_cst/status/1344704764223889408.

———. 2021a. *Communications Security Establishment Annual Report 2020–2021*. Government of Canada, last modified 28 June 2021. https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021.

———. 2021b. *Cyber Threats to Canada's Democratic Process: July 2021 Update*. Government of Canada, July 2021. https://cyber.gc.ca/sites/default/files/2021-07/2021-threat-to-democratic-process-3-web-e.pdf.

———. 2021c. *Security Assessment of the COVID Alert Exposure Notification Service*. ITSP.10.003, 14 January 2021. https://raw.githubusercontent.com/cds-snc/covid-alert-documentation/main/CCCS_SecurityAssessment.pdf.

Fisher, Lucy, and Chris Smyth. 2020. "GCHQ in Cyberwar on Anti-vaccine Propaganda." *Times* (London), 9 November 2020. https://www.thetimes.co.uk/article/gchq-in-cyberwar-on-anti-vaccine-propaganda-mcjgjhmb2.

Gioe, David V., Joseph M. Hatfield, and Mark Stout. 2020. "Can United States Intelligence Community Analysts Telework?" *Intelligence and National Security* 35 (6): 885–901. https://doi.org/10.1080/02684527.2020.1767389.

New Zealand. Government Communications Security Bureau. 2020. "Speech: Cyber Security in a Covid-19 World." Wellington, 3 August 2020. https://www.gcsb.govt.nz/news/cyber-security-in-a-covid-19-world/.

NSICOP (National Security and Intelligence Committee of Parliamentarians). 2020. *Annual Report 2019*. Ottawa, 12 March 2020. https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.

NSIRA (National Security and Intelligence Review Agency). 2020. "2019 Annual Report." 11 December 2020. https://www.nsira-ossnr.gc.ca/wp-content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf.

Ogrysko, Nicole. 2020. "Could the Pandemic Force the Intelligence Community to Reconsider Workplace Flexibilities?" *Federal News Network*, 21 May 2020. https://federalnewsnetwork.com/workforce/2020/05/could-the-pandemic-force-the-intelligence-community-to-reconsider-workplace-flexibilities/.

Robinson, Bill. 2020. "From 1967 to 2017: CSE's Transition from the Industrial Age to the Information Age." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, edited by David Lyon and David Murakami Wood, 89–111. Vancouver: University of British Columbia Press.

———. 2021a. "The Communications Security Establishment." In *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, edited by Stephanie Carvin, Craig Forcese, and Thomas Juneau, 72–89. Toronto: University of Toronto Press.

———. 2021b. "Spy agencies, COVID-19, and parking lots." *Lux Ex Umbra* (blog), 28 March 2021. https://luxexumbra.blogspot.com/2021/03/spy-agencies-covid-19-and-parking-lots.html.

Standing Committee on Government Operations and Estimates. 2020. Evidence. 1st Sess., 43rd Parliament, Meeting No. 14, 25 May 2020. https://www.ourcommons.ca/Content/Committee/431/OGGO/Evidence/EV10768227/OGGOEV14-E.PDF.

Standing Committee on Health. 2020. Evidence. 1st Sess., 43rd Parliament, Meeting No. 32, 7 July 2020. https://www.ourcommons.ca/Content/Committee/431/HESA/Evidence/EV10823064/HESAEV32-E.PDF.

Standing Committee on Industry, Science and Technology. 2020. Evidence. 1st Sess., 43rd Parliament, Meeting No. 16, 20 May 2020. https://www.ourcommons.ca/Content/Committee/431/INDU/Evidence/EV10761671/INDUEV16-E.PDF.

Treasury Board of Canada. 2020. “Supplementary Estimates (B), 2020-21.” https://www.canada.ca/content/dam/tbs-sct/documents/planned-government-spending/supplementary-estimates/supplementary-estimates-b-2020-21.pdf.

———. 2021. “Supplementary Estimates (C), 2020-21.” https://www.canada.ca/content/dam/tbs-sct/documents/planned-government-spending/supplementary-estimates/supplementary-estimates-c-2020-21.pdf.

Tu Thanh Ha, and Colin Freeze. 2020. “Quebec Health Network Targeted by Cyberattack.” *Globe and Mail*, 29 October 2020. https://www.theglobeandmail.com/canada/article-quebec-health-network-targeted-by-cyberattack/.

Weston, Greg. 2013. “Inside Canada’s Top-Secret Billion-Dollar Spy Palace.” *CBC News*, 8 October 2013. https://www.cbc.ca/news/politics/inside-canada-s-top-secret-billion-dollar-spy-palace-1.1930322.