Journal of Military and Strategic Studies

VOLUME 22, ISSUE 1

STUDENT AWARD OF EXCELLENCE 2022

HONOURABLE MENTION

The CSE Act And The Expansion Of Canadian Cyber Capabilities In The Twenty-First Century

William Moxley-Paquette

Introduction

The 21st century has witnessed new technological innovations in the digital realm that has shaped how connected society is with the international community. The introduction of the cyber domain in every country has facilitated this by allowing data to be sent between stations at a faster pace to serve a multitude of purposes in the public and private sectors. As the digital domain expanded, so too has the need to ensure that these systems are secured from hackers and other groups seeking to harm

ISSN : 1488-559X

the infrastructure. The rapid generation of data from the internet and social media means that "big data" must be protected from acts of sabotage and espionage.[1]

This "big data" can be described as "extremely large data sets that can be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions."[2] These datasets are used by both the public and private sector to fulfill a wide range of tasks and purposes. For hackers, this kind of data is valuable for their own objectives. By posing as a cyber threat or initiating a cyber attack at this data, these hackers can use this data to their advantage to "invade privacy, steal intellectual property, disrupt [critical] infrastructure and ultimately erode the identity of the state."[3] Within the realm of national security, big data can be used to assist national cryptology agencies to analyze identify patterns within the data and prepare for situations that may impact national security concerns.[4]

This collection of big data has made securitizing the cyber domain necessary because governments must utilize "extraordinary means" to protect the state and its citizens from having their information compromised and stolen.[5] Canada is no exception. Canada's cyber domain—the domain created and used inside Canada's borders—is protected and monitored by the federal agency, called the Communications Security Establishment (CSE). The CSE serves as Canada's national cryptology agency and was established in 1946 under the National Research Council as the Cold War was starting to begin. The agency was given two responsibilities: conducting signal intelligence (SIGINT) and managing information technology security to collect foreign intelligence and protect Canada's communications infrastructure.[6] However, many of the agencies began to go through rapid change in 2001 and have remained important in Canada's national security. In 2019, the CSE had their legal mandates expanded further

[1] Danda B. Rawat, Ronald Doku, and Moses Garuba, "Cybersecurity in big data era: From securing big data to data-driven security," *IEEE Transactions on Services Computing* 14 no. 6 (2019): pp. 2055, 2065.
[2] David Lyon and David Murakami Wood. "Introduction." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, Eds. by David Lyon and David Murakami Wood (Vancouver, BC: University of British Columbia Press, 2021), p. 4.
[3] Eloise F. Malone and Michael J. Malone, "The 'wicked problem' of cybersecurity policy: analysis of United States and Canadian policy response," *Canadian Foreign Policy Journal* 19, no. 2 (2013): p. 161.
[4] Andrew Clement, Jillian Harkness, and George Raine, "Metadata – Both shallow and deep: The fraught key to big mass state surveillance," in *Big Data Surveillance and Security Intelligence: The Canadian Case*, edited byDavid Lyon and David Murakami Wood (Vancouver, BC: University of British Columbia Press, 2021), pp. 256-257.
[5] Lyon and Wood, "Introduction," p. 4.
[6] Bill Robinson, "The Communication Security Establishment (CSE)," in *Top Secret Canada*, edited by Stephanie Carvin, Thomas Juneau, and Craig Forcese (London, ON: University of Toronto Press, 2020), p. 72.

with the addition of two new mandates: the mandate to seek ministerial authorization to conduct defensive cyber operations and the mandate to conduct active cyber operations after receiving ministerial authorization."[7]

Recent events have done nothing to slow down these developments. The current COVID-19 pandemic and the Russian invasion of Ukraine in early 2022 have made defending Canada's cyber domain more important than ever before.[8] This global environment has impacted everyone hard and made cyber infrastructure a salient policy issue in Ottawa.

With the recent expansion in the CSE's powers in 2019, Canada took a major step in safeguarding its cyber infrastructure while also bolstering the agency's importance in protecting Canada's cyber domain. However, there is concern over what these news powers actually mean. The CSE has a history of little to no transparency and inadequate oversight in its operations and has made it difficult for officials in Ottawa to conduct audits.[9] Furthermore, there is general concern over what the agency actually does, with the Snowden file revelations providing most of what we know about the CSE's secretive activities. There are less than 40 files detailing the CSE's activities.[10] This level of secrecy employed by CSE has been called by observers to unnecessarily "exceed what is necessary or justified."[11] This longstanding issue in the CSE's secretive activities brings into question how the intelligence agency will legally interpret their new mandates and what they will use them for. Regarding the CSE act's new mandates, this paper asks the following question: what significance do the *CSE Act's* new mandates entail for the CSE's role in enforcing Canadian cybersecurity?

---

[7] Ibid., p. 77.

[8] Bill Robinson, "Collection and Protection in the Time of Infection: The Communications Security Establishment during the COVID-19 Pandemic," in *Stress Tested: The COVID-19 Pandemic and Canadian National Security*, edited by Leah West, Thomas Juneau, and Amarnath Amarasingam (Calgary, AB: LCR Publishing Services, 2021), p. 127; Catherine Tunney, "Canadian intelligence agency calls for ramped-up cyber defences after Russia invades Ukraine," *CBC,* 24 February 2022. https://www.cbc.ca/news/politics/cyber-russia-cse-1.6362878 (Accessed 8 March 2022).

[9] Kevin Walby and Seantel Anaïs, "Communications security establishment Canada (CSEC), structures of secrecy, and ministerial authorization after September 11," *Canadian Journal of Law & Society* 27, no. 3 (2012): p. 363.

[10] Andrew Clement, "Limits to secrecy: What are the Communications Security Establishment's capabilities for intercepting Canadian internet communications?" in *Big Data Surveillance and Security Intelligence: The Canadian Case,* edited by David Lyon and David Murakami Wood (Vancouver, BC: University of British Columbia Press, 2021), pp. 126, 129.

[11] Ibid., p. 142.

The findings in this paper are twofold: The new mandates under the *CSE Act* represent the second time since 2001 that the CSE has had its powers expanded and legitimized through statutory law to conduct acts otherwise considered legally controversial, in response to growing saliency in cyber policy. Secondly, increasing concerns of attacks on Canada's cyber domain means that the agency's strict adherence to secrecy will not be balanced with greater transparency and oversight. In the lead-up to the conclusion, the paper will proceed as follows: first, a section will be devoted to elaborating on the issue of secrecy and the dilemmas that have emerged between Canada's intelligence community and society. Second, the salience of cybersecurity since 9/11 will be briefly reviewed up to the *CSE Act's* royal assent to show how prior events have been impactful on the present state of affairs in Ottawa and the importance of cybersecurity. The third section provides an examination of the *CSE Act's* new mandates and its potential implications for CSE's operations and statutory law. Finally, the CSE's activities will be examined in the post-2019 period to assess how salient cybersecurity has become and the expansions evident in the agency.

The Intelligence Community and the Prevalence of Secrecy

The intelligence community is a very esoteric group within the federal government that shares little of its activities with the public and many of its own fellow employees. Agencies in this community conduct intelligence, which involves conducting "a secret epistemic social process performed [through] a government bureaucracy to understand and act against an enemy's intentions, to avoid surprise, and to formulate rational decisions on national security issues." [12] However, this community's duty to protect society can easily become a double-edged sword when its involvement in society becomes complicated. Any democratic country's intelligence agency must ensure total secrecy surrounding its operations to thwart the country's external enemy's plans yet are faced with the issue of how transparent it should be with the public regarding its surveillance practices. [13] The law is the most important counterweight to stop this behaviour from being abused, yet crises where national

[12] Marco Munier, "The Canadian national intelligence culture: A minimalist and defensive national intelligence apparatus," *International Journal* 76, no. 3 (2021): p. 429. Other than the Communications Security Establishment, the Canadian Security Intelligence Service is the only other federal agency that focuses primarily on intelligence gathering.

[13] Christopher Prince, "On denoting and concealing in surveillance law," in *Big Data Surveillance and Security Intelligence: The Canadian Case*, edited by David Lyon and David Murakami Wood (Vancouver, BC: University of British Columbia Press, 2021), pp. 43-46.

security considerations trump the country's codified laws will encourage indifference to traditional longstanding values.[14]

In liberal democratic states, the rule of law is one of the most important guiding principles in the government's obligations. But the state's intelligence community remains in an ambiguous position with the law. This results in a principle-agent problem where the intelligence community provides a service that inevitably arouses suspicion from the public because many in society are unsure about what the intelligence community is conducting that may be contrary to the law and the country's democratic values.[15] In the wake of the terrorist attacks on 11 September 2001, pre-emptive security measures became widespread and accepted by many governments in the West as necessary to maintain "perpetual vigilance" and strike the threat before it causes any further tragedies.[16]

For Canada in particular, it is in Ottawa's interest to intervene and remain vigilant of faraway international crises to ensure they do not grow into issues that threaten international peace and stability.[17] The terrorist attacks on 9/11 were the culmination of the new emerging threat of international terrorism that was recognized to be a global problem in the mid-1990s: a serious threat that can "transcend political borders and affect whole regions, or even the globe."[18] After 9/11, many intelligence organizations had their authorities and capabilities expanded by new legislation that contradicted existing democratic laws and values—allowing these agencies to operate in crises that constitute a "state of exception" where pre-existing democratic values can be ignored to decisively resolve the crisis.[19] An expansion of surveillance networks to target individuals closely connected to criminal activity is one example of these practices that soon became widespread.[20]

As these forms of legislations across the West became enacted, many expressed concern over a paralysis in the West's checks and balances.[21] The severity of the

[14] Ibid., p. 43.
[15] David E. Pozen, "Deep Secrecy," *Stanford Law Review* 62, no. 2 (2010): p. 278.
[16] Richard V. Ericson, "The state of preemption: Managing terrorism risk through counter law," in *Risk and War on Terror*, edited by Louise Amoore and Marieke de Goede (Oxon, UK: Routledge, 2008), p. 57.
[17] Munier. "The Canadian national intelligence culture," 436-437.
[18] Ibid, p. 434.
[19] Ericson, "The state of pre-emption," p. 57.
[20] Ibid.
[21] Didier Bigo, Sergio Carrera, Elspeth Guild and R.B.J. Walker, *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project* (Brussels: Centre for European Policy Studies, 2007): p. 3.

situation, coupled with calls to prepare for the worst outcomes, has the potential to make officials indifferent towards their actions that may infringe on basic human rights.[22] In Canada's case, this came in the form of expanding the mandates of all its intelligence agencies to target Al-Qaeda supporters infiltrating Canada's Arab and Muslim communities—unintentionally causing Canada's Muslim communities to become distrustful of these agencies and their surveillance practices.[23] By the early 2000s, Canada's intelligence community was able to evade scrutiny in Ottawa despite lack of oversight in its ongoing procedures.[24]

The intelligence-evidence dilemma is an important factor for explaining why departments in the intelligence community are unwilling to disclose classified documents. This dilemma originates from the concern that revealing how information was gathered could result in an individual's life becoming endangered, reveal the agency's sources and how the agency collects its evidence.[25] Adversaries seek to exploit these vulnerabilities. In some cases, how the information of a criminal was collected may deem the evidence illegal and unlawful—blocking law-enforcement from detaining the suspect.[26]

For many in Canada's intelligence community, this dilemma has been a longstanding reason why investigations may take longer.[27] For example, while the prosecutions successfully found the eighteen Canadians that planned the 2006 Toronto terrorism plot guilty, law-enforcement initially faced a dilemma on how they could have the plotters charged without revealing too much about their evidence collection process.[28] For the CSE, this dilemma has emerged in the form of who it can and cannot collect information from. While Canadians and others in Canada cannot have their data collected by the CSE, it may unintentionally acquire their information during its "bulk

[22] Ibid., pp. 6-7.
[23] Martin Rudner, "Challenge and Response: Canada's Intelligence Community and the War on Terrorism," *Canadian Foreign Policy Journal* 11, no. 2 (2004): p. 22.
[24] Ibid., p. 33.
[25] Craig Forcese, "Threading the Needle: Structural Reform & Canada's Intelligence-to-Evidence Dilemma," *Manitoba Law Journal* 42, no. 4 (2019): p. 132.
[26] Ibid., p. 133. Many intelligence agencies in Canada have different mandates to fulfill their specific obligations. However, because some methods and practices may not be allowed for the collection of evidence and information, some of these agencies will not be able to use what they acquired. The best course of action would be to 'hint' their counterparts that are legally permitted to handle the material.
[27] Jay Pelletier and Craig Forcese, "Curing Complexity: Moving Forward from the Toronto 18 on Intelligence-to-Evidence," *Manitoba Law Journal* 44, no. 1 (2021): p. 160.
[28] Ibid.

interception" operations of foreign data.[29] However, given the current legislation under the *CSE Act*, the CSE may conduct data collection inside Canada's borders when granted ministerial authorization to do so—a legal requirement when there is substantial reason to believe Canadian data may unintentionally be swept up during the interception.[30]

While all secrets can vary in their complexity because some are known by a few while others are more known. According to David Pozen, this can take the form of "dark" secrets and "shallow" secrets, which can become vague or well-known depending on the following four characteristics: how many people know about the secret; who are the people who know the secret; how much is known to them; and finally, when do they learn about the secret.[31] In Canada's case, this is important to consider since the CSE predates the Canadian Charter of Rights and Freedoms by four decades.[32] The creation of new laws can cause new legal gaps to emerge when their "language and interpretation" do not account for these longstanding secretive practices.[33]

Secrecy can serve the purpose of protecting a country's vital information from its enemies, but prioritizing too much secrecy can impact public confidence in the government and impact the fundamentals of the rule of law.[34] Secrecy can also become fragmented and cause legal complexities to arise when the agency's authority and power are too ambiguous for legal experts to ascertain the its restrictions.[35] The CSE has been notorious for its secrecy practices and has often cited legislation to deflect questions to protect the organization's practices and techniques, even if revealing such information may not compromise their ongoing operations.[36]

The CSE itself has been described by former officials of the organization as being "extremely compartmentalized" for each employee to control how much CSE's own

---

[29] Craig Forcese, "Bill C-59 and the Judicialization of Intelligence Collection," in *Big Data Surveillance and Security Intelligence: The Canadian Case*, edited by David Lyon and David Murakami Wood (Vancouver, BC: University of British Columbia Press, 2021), p. 170.

[30] See the following for greater information regarding the agency's approaches when handling intercepted Canadian information: Canada. Communications Security Establishment, "Privacy," 26 October 2020. https://www.cse-cst.gc.ca/en/accountability/privacy (Accessed 29 March 2022).

[31] Pozen, "Deep Secrecy," p. 267.

[32] Prince, "On Denoting and Concealing in Surveillance Law," p. 46.

[33] Ibid., p. 47.

[34] Ibid., p. 43.

[35] Ibid., pp. 43-46.

[36] Clement, "Limits to Secrecy," p. 142.

agents know about the agency's activities.[37] As per the Security of Information Act, the agency's practices are a closely guarded secret, and so its employees are "duty-bound to secrecy" or else they will face legal consequences for being talkative.[38] Furthermore, the CSE does not need to worry about its transparency because it is exempted from abiding to the Access to Information Act.[39] As such, the CSE can be described as practicing *dark secrecy* in its day-to-day operations.

One's environment is also an important consideration when understanding why secrecy is enforced. The driving force for this behaviour is attributable to a country's "strategic culture" which is "the sum total of ideas, conditioned emotional responses, and patterns of habitual behaviour that members of a national strategic community have acquired through instruction or imitation."[40] A country's strategic "culture" establishes how the country observes dangers in the international environment and what threats should be prioritized in its intelligence collection and analysis processes.[41]

For the CSE, the Cold War undoubtedly had a strong impact on its culture. The CSE participated in the Cold War by acting as Ottawa's link to Canada's allies in the Five Eyes—an intelligence alliance that facilitates SIGINT cooperation between the United States, United Kingdom, Australia, New Zealand, and Canada—and annually wrote thousands of SIGINT reports focusing on the Soviet Union's activities and operations.[42] This international security environment created by the Cold War has made observers express concern over the CSE's modern-day intelligence gathering practices that potentially could be violating Canadian rights.[43]

Not only did the Cold War impact the agency in terms of its strict adherence to secrecy, but also its routine practices. After the Cold War concluded, the CSE worked with Five Eyes to collectively expand their SIGINT involvement into new policy matters that were growing in salience. In addition to paying greater attention to foreign interference and international terrorism after the Cold War, economic intelligence gained considerable traction because it became an important and practical tool for

[37] Walby and Anaïs, "Communications Security Establishment Canada (CSEC), Structures of Secrecy, and Ministerial Authorization after September 11," p. 376.
[38] Ibid., p. 367.
[39] Ibid.
[40] Isabelle Duyvesteyn, "Intelligence and Strategic Culture: Some Observations," *Intelligence and National Security* 26, no. 4 (2011): p. 522.
[41] Ibid., pp. 530-531.
[42] Robinson, "The Communication Security Establishment (CSE)," pp. 72-73.
[43] Ibid., p. 84.

promoting Canada's own economic competitiveness with its trading partners.[44] Although it is not openly stated, Ottawa likely viewed the agency's produced assessments positively. For example, journalists in the late 1990s revealed that the CSE conducted economic intelligence on behalf of Ottawa to provide Canadian policy-makers with an information advantage during high-profile multilateral and bilateral trade agreements between 1994 to 1997.[45]

Even when laws are passed to require transparency in these agencies, they can be bypassed. Canada has a wide scope of statutory law governing this that has legitimized CSE's exceptional obligations and practices.[46] Legislation developed to protect democratic principles can be bypassed when the intelligence community and national government are keen to preserve their *deep secrets* and will stall in revealing government secrets.[47] While the public may want to know what the government is keeping a secret, the public faces another challenge: identifying what the government is keeping classified.[48] Here, the CSE has historically made it difficult for officials in Ottawa (and even those conducting audits) to comment on much of CSE's sensitive information.[49] Former Commissioners tasked with reviewing the CSE expressed "frustration in their inability to comment on the actual surveillance practices […] and ambiguities in the laws governing [them]."[50] Because of the nature of the government's security interests, national security will trump calls for transparency when revealing classified information can harm the government's operations.[51]

As this section has shown, there are many reasons why the intelligence community (and especially the CSE) seek to ensure complete secrecy. Due to the nature of the threat, national security concerns can outshine and minimize the importance of democratic values. Here, the law is involved in a constant struggle against secrecy as these agencies seek to fulfill their mandates. This will be important to remember for the section on the *CSE Act*.

---

[44] Martin Rudner, "Canada's Communications Security Establishment from Cold War to Globalization," *Intelligence & National Security* 16, no. 1 (2001): pp. 118-119.
[45] Ibid., p. 119.
[46] Philippe Lagassé, "Defence Intelligence and the Crown Prerogative in Canada," *Canadian Public Administration* 64, no. 4 (2021): p. 540.
[47] Pozen, p. 313.
[48] Ibid.
[49] Walby and Anaïs, p. 376.
[50] Ibid.
[51] Pozen, p. 275.

The Post-9/11 Security Environment and Cybersecurity's Growing Saliency in Canada

The terrorist attacks on 11 September 2001 sent shock waves across the globe and exposed weaknesses in the international community in the face of possible terrorist attacks. This terrible day showed how easy it was for terrorist groups to infiltrate the West and cause a large amount of death and destruction in a short amount of time. No one in Ottawa was prepared for this terrorist attack. Prime Minister Jean Chrétien and his Cabinet Ministers were caught woefully unprepared by this, while their senior security advisors were left "confused, slow and uncoordinated" on how to properly respond.[52] While it later became evident that the terrorist attacks were directed at the United States (US), officials in Ottawa realized how dangerously unprepared Canada was for anticipating and identifying a national security threat entering its borders.[53] In a matter of months, Ottawa passed the 2001 Anti-Terrorism Act to expand the mandate and powers of its intelligence community. The CSE gained three mandates. To warn Ottawa of potential attacks and threats, the CSE was mandated to intercept communication of foreign individuals without facing serious access constraints enforced in the Canadian Criminal Code.[54] The other two mandates include "[protecting] electronic information and information infrastructures of importance to the Government of Canada," and "[providing] technical and operational assistance to federal law enforcement and security agencies."[55]

To broadly support Canada's intelligence community's new mission and authority, the Chrétien government allocated $7.7 billion in federal funding toward domestic security issues, including "emergency preparedness, intelligence and policing, air travel security, immigrant and refugee screening, and border security and infrastructure."[56] To clarify, these policy developments in Canadian domestic security concerns were not fundamental shifts in Canadian values but showed Ottawa's re-assessment of what security practices had to be modified and improved upon.[57] Surveillance practices immediately became stricter in Canada's airports with airline companies now logging their travellers' information.[58] Several intelligence agencies then

[52] Alan James Stephenson, "Canadian National Security Culture: Explaining Post 9/11 Canadian National Security Policy Outcomes," (PhD dissertation, Carleton University, 2016), p. 179.
[53] Ibid.
[54] Walby and Anaïs, pp. 364-365.
[55] Robinson, "The Communications Security Establishment (CSE)," p. 73.
[56] Stephenson, "Canadian National Security Culture," p. 181.
[57] Ibid., 184.
[58] David Lyon, "Airport Screening, Surveillance, and Social Sorting: Canadian Responses to 9/11 in Context," *Canadian Journal of Criminology and Criminal Justice* 48, no. 3 (2006): p. 398.

began to use these databases to more easily track individuals believed to pose a security threat and halt their mobility.[59]

Chrétien's policy approach would be expanded upon by his Liberal Party successor in 2003, Paul Martin. Prior to becoming prime minister, Martin served as the Minister of Finance under Chrétien's government and was already aware of the growing international security concerns that Ottawa needed to become more proactive in protecting itself against.[60] In 2004, the Martin government published Canada's first document focusing on cybersecurity. The document titled *Securing an Open Society: Canada's National Security Strategy*, highlighted growing volatility caused by international terrorism and other growing international security issues that could concerningly exploit Canada's vulnerable cyber infrastructure and use it for their own purposes (such as recruitment).[61] Cyber attacks were becoming increasingly frequent and severe, and required a government response: "the Government will substantially improve threat and vulnerability analyses for its systems, and strengthen its ability to defend its systems and respond to cyber-incidents."[62] To defend Canada's interests, the document designated the intelligence community as the country's front-line of defence in monitoring and defending Canada's cyber interests.[63] Among the several intelligence agencies mentioned, the CSE would play a critical role in providing Ottawa awareness of international issues that may impact national affairs, garnering a 25 percent increase in its annual budget.[64] Martin's government would only last another two years and his aspirations would have to be enacted by his successor, Stephen Harper, and the Conservatives.

When Stephen Harper became prime minister in 2006, the issue of home-grown terrorists did not dissipate in Canada. Instead, Canada came very close to experiencing its own deadly terrorist attacks. On 2 June 2006, more than 400 police officers and security agents stormed several houses across the Greater Toronto Area and arrested 15 individuals that were radicalized by Al-Qaeda's ideology and were planning to carry out several bombings across the City of Toronto.[65] For several months, officials in the

[59] Ibid., p. 404.
[60] Paul H. Chapin, "Into Afghanistan: The transformation of Canada's international security policy since 9/11," *American Review of Canadian Studies* 40, no. 2 (2010): pp. 193-194.
[61] Canada, Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa, ON: Privy Council Office, 2004), pp. 15-16.
[62] Ibid., p. 26.
[63] Ibid., pp. 15-16.
[64] Ibid.
[65] "Toronto 18: Key Events in the Case," *CBC*, 4 June 2008. https://www.cbc.ca/news/canada/toronto-18-key-events-in-the-case-1.715266 (Accessed 10 March 2022).

Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) monitored these terrorists and collected vital information about the planned attacks by intercepting these terrorists' electronic communication devices.[66] Just a few months into Harper's term in office and the possibility of a terrorist attack on Canadian soil was a high possibility. Vigilance remained paramount in thwarting these insidious plans.

As the years progressed and society became more dependent on the internet, malicious hacking remained a considerable threat. Harper expanded further on Martin's policy efforts and began to cement the importance of cybersecurity in Ottawa's national security objectives. In Ottawa's 2010 cyber strategy, the Harper government recognized that the Government of Canada and the Canadian private sector were quickly adopting and becoming increasingly dependent on the internet to carry out a wide variety of activities and tasks; making Canada's emerging cyber domain "one of [Canada's] greatest national assets."[67] According to the document, the strategy required government initiatives aimed at protecting Canada's cyber domain to closely follow its three pillars: secure the Government of Canada's cyber system, partner with provinces, territories, and the private sector to secure vital cyber systems outside of the federal government and help Canadians remain secure throughout their online activities.[68]

The document also highlighted the following adversaries that were serious security threats to the government and individual Canadians: state-sponsored cyber groups conducting cyber attacks, terrorist organizations exploiting the internet to expand their recruitment operations, organized crime exploiting the anonymity offered by the internet, and the sudden and rising volume and ferocity of cyber-attacks across the world.[69] The CSE, CSIS, the RCMP, and other federal agencies and departments were tasked to deter these groups and alert Ottawa of any suspicious activities, with Public Safety Canada (PSC) designated to lead the strategy's implementation.[70]

In the strategy's Action Plan, improvements were made under the planning and management of the PSC to ensure the strategy would meet the objectives highlighted under its three pillars by 2015. The Action Plan charted many of the projects that were initiated since the strategy's publication, with several of the completed assignments

[66] Ibid.
[67] *Canada, Public Safety Canada. Canada's Cyber Security Strategy: For a Stronger and more Prosperous Canada* (Ottawa, ON, CA: Public Safety Canada, 2010), p. 2.
[68] Ibid., p. 7.
[69] Ibid., pp. 5-6.
[70] Ibid., p. 10.

including greater cooperation with the US and improved intragovernmental cooperation and communication between the PSC's Canadian Cyber Incident Response Centre and the CSE (to name a few examples).[71] As these projects began to commence, the CSE was no longer embedded inside the Department of National Defence (DND) and became its own separate agency in late 2011, albeit still answering to, and requestion authorization for its cyber activities from, the Minister of DND.[72]

The CSE itself was also seeing its relationship with other federal agencies grow around this time. Since 9/11, the CSE established several Memorandum of Understandings (MOUs) between itself and other federal agencies and departments to improve cooperation in the distribution of their resources in operations and tasks with other federal agencies they had common interests with.[73] From 2006 to 2009, several of these MOUs were signed between CSE and DND and the Canadian Forces (CF) to improve the latter's operations that required expertise in cryptography, with several of these MOUs valid until the mid-2010s.[74] By 2012, several more MOUs would be signed this time with CSIS which the CSE continues to maintain an "extremely cozy" relationship revolving around their intragovernmental cooperation.[75] What this shows is that the CSE and its services were being sought after for security matters before the Harper government even published its cyber strategy the following year.

Unfortunately, new rounds of terror soon engulfed Canada. The rise of the Islamic State in Iraq and Syria inspired a wave of lone-wolf terror attacks across the West. Two took place in Canada in 2014. The first of these events occurred in Saint-Jean-sur-Richelieu, Quebec, when a radicalized individual ran over two members of the CF, killing one and injuring the other.[76] The second incident, the Ottawa Shooting, occurred afterward. In a planned attack on Parliament Hill by several radicalized Canadians, a member of the CF was shot and killed at the War Memorial while a subsequent shoot-

[71] Canada, Public Safety Canada, *Action-Plan 2010-2015 for Canada's cyber security* strategy (Ottawa, ON: Public Safety Canada, 2013), pp. 9-10.
[72] Robinson, "The Communication Security Establishment (CSE)," p. 73.
[73] Walby and Anaïs, p. 373.
[74] Ibid., p. 374.
[75] Jez Littlewood, "The Canadian Security Intelligence Service (CSIS)," in *Top Secret Canada.* , edited by Stephanie Carvin, Thomas Juneau, and Craig Forcese (London, ON: University of Toronto Press, 2020), p. 56.
[76] Ian Austen. "Hit-and-run that killed Canadian soldier is called terrorist attack." *The New York Times,* 21 October 2014. https://www.nytimes.com/2014/10/22/world/americas/canadian-soldier-run-down-in-what-officials-call-act-of-terror-dies.html (Accessed 11 March 2022).

out commenced inside several parliamentary buildings.[77] As such, the threat of international terrorism has not lessened and remains a serious national security threat, with the capital of Canada now threatened.

A year after these events took place, Ottawa passed the 2015 *Anti-Terrorism Act*. This new law expanded upon the powers of several federal intelligence agencies for collecting information, among other things.[78] This *Act*, however, did not expand CSE's capabilities in cybersecurity but instead broadened CSIS's powers and did not improve Ottawa's review mechanisms of the intelligence community's confidential activities. Rather, CSIS can conduct such operations that contravene Canadian law and the Charter if given authorization from federal courts for the sake of protecting Canadian security interests.[79] This legislation was reactive and broadened Ottawa's powers in a time of "fear" revolving around the 2014 attacks in Canada and the subsequent Paris Attacks in 2015.[80] This concern over the 2015 *Anti-Terrorism Act* catapulted Bill C-59 under the Trudeau government to improve oversight and, ironically, expand the powers of the CSE.[81]

While having grown in prominence under the Harper government, cybersecurity garnered greater salience by the start of Justin Trudeau's time in office. After commencing his term in office, several of Trudeau's Cabinet ministers were already tabling letters discussing the growing need to increase the protection of Canada's cyber domain from outside threats.[82] These came when Trudeau's government was adamant about rebuilding Canada's international involvement in peace operations and multilateral cooperative initiatives to address global security threats deemed harmful to

[77] Ashley Fantz, Josh Levs, and Catherine E. Shoichet, "'Terrorist' murdered soldier 'in cold blood,' Canada's prime minister says," *CNN*, 23 October 2014. https://www.cnn.com/2014/10/22/world/americas/canada-ottawa-shooting/index.html (Accessed 11 March 2014).

[78] Munier, p. 428.

[79] Kent Roach and Craig Forcese, "Legislating in Fearful and Politicized Times: The Limits of Bill C-51's Disruption Powers in Making Us Safer," in *After the Paris attacks: Responses in Canada, Europe, and around the globe,* edited by Edward M. Iacobucci and Stephen J. Toope (Toronto, ON: University of Toronto Press, 2015), p. 146.

[80] Ibid., p. 142.

[81] Michael Nesbitt, "Reviewing Bill C-59, An Act Respecting National Security Matters 2017: What's New, What's Out, and What's Different from Bill C-51, A National Security Act 2015?" *The School of Public Policy Publications* 13, 12 (2020): pp. pp. 1-2.

[82] Claire Wählen, "Trudeau Government Putting New Emphasis on Cybersecurity," *ipolitics*, 17 November 2015. https://www.ipolitics.ca/news/trudeau-government-putting-new-emphasis-on-cybersecurity (Accessed 14 March 2022).

Canada's interests of global peace and stability.[83] To do this, Trudeau expanded Canada's involvement through non-military means, with Canada's intelligence community deemed critical for furthering Canada's interests, protecting and alerting Canadians, and Ottawa of emerging international threats and crises.[84] This would be put into policy after subsequent publications in Ottawa.

First, in 2017, cybersecurity was specified in Ottawa's newest defence policy called *Strong, Secure, and Engaged* as an important pillar for building Canada's resiliency to international threats, and called on the CF to expand its troop-count in the trades specializing in space, cyber, and intelligence.[85] The CSE too was beginning to publish its own documents by this point and raised the alarm for cyber threats that could harm Canada's democratic values and institutions.[86] In one of these documents, the CSE warned Ottawa that some states were already conducting cyber attacks targeting Canada's cyber domain and were potentially preparing to disrupt the upcoming federal election in 2019.[87] Russia was one such country mentioned and was held responsible or directly linked to several other cyber attacks aimed at the national governments of Ghana, the US, and the Netherlands.[88] This is not new, as a recent article from the CBC showed both China and Russia sponsored many cyber attacks aimed at Canada and have been serious problems since the Harper era).[89]

In 2018, the Trudeau government published its cyber strategy. The accomplishments made under Harper's government are serving as the groundwork for Trudeau's government's progress.[90] The three pillars under Harper's cyber strategy have been achieved through the PSC's action plan, but new threats meant that new objectives must be generated. The Liberal government's strategy outlines three new goals: ensure Canada's cyber domain remains secure and resilient; improve Canada's cyber domain's adaptability and innovation; and ensure Ottawa provides leadership on

[83] Munier, p. 438.
[84] Ibid., pp. 438, 440
[85] Canada, Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa, ON: Department of National Defence, 2017), pp. 13-14.
[86] Canada, Communications Security Establishment, *Cyber Threats to Canada's Democratic Process* (Ottawa, ON: Communications Security Establishment, 2017), p. 4.
[87] Ibid.
[88] Ibid., pp. 17, 19.
[89] Catherine Tunney, "Flaws in cyber defence expose government information to state-sponsored theft: report," *CBC*, 15 February 2022. https://www.cbc.ca/news/politics/cyber-defence-nsicop-1.6350802 (Accessed 14 March 2022).
[90] Canada, Public Safety Canada, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age* (Ottawa, ON: Public Safety Canada, 2018), pp. 2-5.

cyber issues and collaborates with key actors in society.[91] Regarding the CSE's role in this, Ottawa established a sub-unit to the agency called the Canadian Centre for Cyber Security to provide specific technical advice and duties to monitor evolving cyber issues and alert the public and government.[92] However, the PSC's action plan reports that this sub-unit and the other objectives created specifically for the CSE will only be fully operational and completed by 2024.

Ever since the 2015 Anti-Terrorism Act was created, there has been general distrust to the Act's content. The Trudeau government promised to address these public concerns. As a result, the Trudeau government passed into law Bill C-59 in 2019, The National Security Act, which also led to the passing of the *CSE Act*.[93] Not only did the CSE gain new powers and authority, Ottawa addressed public concerns by establishing two new agencies and positions to provide oversight for the CSE and the general intelligence community: The National Security and Intelligence Review Agency (NSIRA) and the Intelligence Commissioner—fulfilling his government's promise to increase oversight.[94] These expansions in the CSE's mandate and new oversight institutions marked a major change in Canada's cyber policy and the wider federal intelligence community.

This section has shown that these security matters grew in salience after 9/11. From Chrétien's government to the present Trudeau government, cybersecurity concerns have been met with new government initiatives to thwart potential cyber-attacks and reduce vulnerabilities. International terrorism, state-sponsored hackers, and the increasing reliance on the internet have all pushed Canada's cyber domain to the forefront of Canadian policy. Since 2001, officials in Ottawa have increasingly recognized the importance of the intelligence community in preventing national disasters and attacks on Canadian soil and digits.[95] In this mess, the CSE held an important position. From 2001 and up to the *CSE Act's* passing, the CSE's annual budget grew from $100 million to nearly $800 million while its staff grew from over 900 to nearly 2,600.[96] The next section shall explore the *CSE Act* and its significance for Canadian security and the agency's practices.

[91] Ibid., p. 9.
[92] Canada, Public Safety Canada, *National cyber security action plan (2019-2024)* (Ottawa, ON: Public Safety Canada, 2019), p. 17.
[93] Nesbitt, "Reviewing Bill C-59, An Act Respecting National Security Matters 2017," p. 12.
[94] Ibid., p. 13.
[95] Munier, p. 428.
[96] Robinson, "The Communication Security Establishment (CSE)," p. 79.

The *CSE Act* and its Implications for Canadian Cybersecurity Practices

Having gained royal assent in 2019, the *CSE Act* is the most recent and consequential expansion in Canada's intelligence community. The last time the CSE had its mandates enshrined in statutory law was under the 2001 Anti-Terrorism Act. Now, the *CSE Act* has expanded the agency's mandates to five, covering *active* (or offensive) and defensive cyber operations.

The first of these two mandates focuses on "active cyber operations" and enables the agency to conduct such cyber operations "to disrupt foreign threats, including activities to protect our democratic institutions, to counter violent extremism and terrorist planning, or to counter cyber aggression by foreign states."[97] The second mandate includes "defensive cyber operations" and covers cyber operations aimed at "proactively [stopping] or [impeding] foreign cyber threats before they damage Canadian systems or information holdings."[98] Hence, the CSE's capabilities for protecting Canada's cyber domain are now greater than before, supported by legislation.

The Act does provide new legally permitted methods for targeting Canada's adversaries but the legislation does narrow the severity of the CSE's retaliatory or targeted operations. The mandates' legal restrictions are in in force in three scenarios: first, these operations are legally prohibited if they will intentionally or accidentally cause death or physically harm a person.[99] Second, these operations cannot be used to "obstruct, pervert or defeat" Canada's democratic ideals and institutions.[100] And last, as specified for the original three mandates, these operations "cannot be 'directed at' Canadians or persons in Canada."[101]

Despite these important restrictions, three notable concerns have arisen during and after the Act gained royal assent (especially for the third point). First, these two mandates are open-ended in their interpretations. Despite Ottawa's assurance that infringing on personal activities will require compelling evidence to be justified and authorized, the vast amount of activities the CSE will conduct under its new mandates can still infringe on any individual's privacy.[102] The new mandates are written in a very

[97] Ibid., p. 78.
[98] Ibid.
[99] Ibid.
[100] Ibid.
[101] Ibid., p. 82.
[102] Stephanie Williams, "The Powers of the CSE After C-59: Are Privacy Rights at Risk?" *National Journal of Constitutional Law* 40, no. 2 (2020): p. 143.

broad manner that impairs any legal experts' from confidently discerning the full legal limits surrounding the CSE's active and defensive cyber operations: "[The Act precludes] any person from clearly understanding the nature, type, scope, target, triggering conditions, or limitations on the potential activities contemplated by the Act in a way that ultimately raises rule of law issues."[103] Granted this broad power, a multitude of approaches can be undertaken that may expose an individual's personal information, such as through an act of intentional hacking.[104] The open-ended possibilities granted to the agency under the Act can result in the CSE's operations becoming rights-infringing and will likely (but unintentionally) cause "collateral harm to non-targeted parties and infrastructure."[105]

Second, these cyber operations do not require a judicial warrant. Instead, the Minister of DND authorizes these operations after receiving a request/approval from the Minister of Foreign Affairs that such operations are necessary to be initiated and carried out.[106] These authorizations are also easy to obtain since they do not have much oversight. Specifically, while the position of Intelligence Commissioner was created to provide legal advice and oversight, the Act does not require this official to perform these duties when the DND minister is authorizing active/defensive cyber operations.[107]

Ministerial authorization can be broadly used for circumstances where it is deemed necessary such as when national security interests are at stake. Regarding defensive and active cyber operations, the CSE does not need to conduct its activities in a "privacy-protective manner" which the Act requires under the three other mandates.[108] For example, if the CSE were to initiate an active cyber operation, Canadian citizens and individuals inside Canada could be caught in the middle and become "collateral damage."[109] As noted earlier, CSE's ministerial authorizations is a less rigorous than the check and balances enforced by the judicial-issued warrants which its intelligence agency colleagues in the federal government must satisfy before

[103] Christopher A. Parsons, et al., "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (an Act Respecting National Security Matters), First Reading," (Toronto, ON: The Citizen Lab, 2017), p. 32.
[104] Williams, "The Powers of the CSE After C-59," p. 142.
[105] Parsons, et al., "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (an Act Respecting National Security Matters), First Reading," p. 32.
[106] Williams, pp. 141-142.
[107] Nesbitt, p. 20.
[108] CCLA, "The New Communications Security Establishment Act in Bill C-59," *Canadian Civil Liberties Association,* 12 September 2017. https://ccla.org/privacy/national-security/the-new-communications-security-establishment-act-in-bill-c-59/ (Accessed 26 March 2022).
[109] Ibid.

initiating its own intrusive activities.[110] The Canadian Civil Liberties Association warns that these new powers will negatively impact the Canadian public's freedom of expression as a result of further communication interferences and activities that would compromise digital networks.[111]

Finally, and the most pressing of these three issues, the codification of CSE's new powers in statutory law legally enforces the agency's covert activities. When it elevated its mandates to statutory law in 2001, Ottawa effectively legitimatized CSE's secretive activities under Canadian law in the face of new and growing international security concerns.[112] This legal tactic effectively utilizes ministerial authorization as a "legal shield" for conducting its covert activities without CSE needing to worry about its standard operational practices and confidential information being compromised by growing public scrutiny.[113]

Statutory law expands the lawful authority of an agency in the federal government to conduct tasks that are specific to its field of expertise and fulfill its legal obligations.[114] When new statutory laws are established, legal authority is transferred to the executive branch which Parliament would have otherwise been responsible for.[115] Given what an agency may be mandated to complete, statutory law can provide enough broad authority to enable the agency to complete its tasks with fewer legal barriers: "all powers which are practically necessary for the accomplishment of the object [are] intended to be secured by the statutory regime."[116] In effect, this deployment of the law grants any agency greater legal authority that would otherwise have been constrained if it was established under the executive branch's "prerogatives"—an aspect of Canadian law that faces more legal scrutiny and constraints.[117]

Conversely, some laws are able to supersede the legal protections granted under other similarly crafted legislation to grant federal agencies more immunity from laws

[110] Nicholas Rosati, "Canadian National Security in Cyberspace: The Legal Implications of the Communications Security Establishment's Current and Future Role as Canada's Lead Technical Cybersecurity and Cyber Intelligence Agency," *Manitoba Law Journal* 42, no. 4 (2019): p. 195.
[111] CCLA, "The New Communications Security Establishment Act in Bill C-59."
[112] Walby and Anaïs, p. 377.
[113] Ibid.
[114] Alexander Bolt and Philippe Lagassé, "Beyond dicey: Executive authorities in Canada," *The Journal of Commonwealth Law* 3, no. 1 (2021): p. 16.
[115] Ibid.
[116] Ibid., p. 17.
[117] Lagassé, "Defence Intelligence and the Crown Prerogative in Canada," p. 552.

that would have held federal agencies accountable for their conduct.[118] For example, the lack of a judicial warrant for CSE to conduct surveillance is an anomaly in Canadian statutory law, which is generally more conservative towards the wider intelligence community.[119] By moving CSE's powers into statutory law, Ottawa has essentially removed legal barriers in order to respond to international threats.[120]

Problems can arise in statutory law and make legislation ambiguous and unspecific.[121] This is especially the problem in the *CSE Act*—remaining vague and legally controversial when, for example, considering Ottawa's narrow interpretation of "private communication" in the Criminal Code.[122] According to Craig Forcese, the Act's areas of ambiguity will likely not resolve general suspicion towards the agency's secretive operations.[123] As things stand for these issues, we are at the mercy of Ottawa's *goodwill* to not broadly interpret the legislation.

The conclusion from these concerns is on how the CSE may interpret its abilities behind closed doors. Are the previous concerns too dramatic? Probably not. As mentioned earlier in this paper, it can be inferred that the CSE has behaved more stringently in its secrecy than its contemporary in the US, the National Security Agency (NSA), and argues that revealing its practices will constitute a violation of existing security legislation, compromise the CSE's practices, and threaten Canada's national security interests.[124] A legal compromise that would secure some of the CSE's operational practices but be balanced by an adequate amount of transparency for some of its other practices would still not be welcomed by the agency because revealing any information or practices is viewed by the agency as a breach and impact their operational effectiveness—even on matters where scholars have pointed out that such measures of extreme secrecy are unnecessary.[125]

Much of what we can verify about the CSE's cyber capabilities and past operations are from top-secret documents revealed through the Snowden revelations. In 2015, the CBC published an article revealing the CSE's cyberwarfare tools used for

[118] Ibid.
[119] Walby and Anaïs, p. 372.
[120] Lagassé, p. 549.
[121] Bolt and Lagassé, "Beyond Dicey," p. 17.
[122] Craig Forcese, "Putting the Law to Work for CSE: Bill C-59 and Reforming the Foreign Intelligence Collection and Cybersecurity Process," *Ottawa Faculty of Law Working Paper* 2017-43 (2017), p. 8.
[123] Ibid.p. , 9.
[124] Clement, pp. 142-143. For example, officials in CSE claim that revealing any information would violate the *Secrets of Information Act*.
[125] Ibid., p. 143.

hacking electronics in distant countries within the Middle East and the Americas.[126] The CSE and the NSA cooperated expensively on developing and sharing cyber tools to hack foreign services and compromise foreign websites.[127] For example, the CSE was able to create its own malware software that could remain undetected while hacking its targets and remain hidden as it compromised its electronic devices and systems of communication.[128] Similar practices were done several years prior when several more classified documents mentioned the CSE's role in conducting economic intelligence on the Brazilian government's mining and energy ministry.[129] The CSE specifically targeted and collected the Ministry of Mines and Energy's stored phone calls and emails to collect sensitive and confidential information that would provide Canadian officials with important insight into Brazil's mining sector for future trade negotiations.[130] This last point about Brazil is also similar to the CSE's active economic intelligence practices in the 1990s that were discussed earlier, inferring to us that the agency's past practices of espionage have unlikely changed.

Some of CSE's own hacking tools closely resemble those used by the NSA. For example, the hacking software known as QUANTUM (used to redirect the targeted user to a malicious version of a website to infect the user's device) identified inside the top-secret documents to be one of CSE's cyber tools, is also the same hacking software used and developed by the NSA.[131] As reported by the CBC, QUANTUM was just one of several tools the agency could use to attack Canada's adversaries or targets. The classified document from 2011 included six other cyber tools that can be used for active cyber operations, with one of the tools allowing Canadians' cyber operations to disrupt and control a target's electronic devices.[132]

Another media agency called The Intercept was also able to publish separate classified documents and briefing papers that further revealed the CSE's close and

[126] Dave Seglins, "Communication Security Establishment's Cyberwarfare Toolbox Revealed," *CBC*, 23 March 2015. https://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978 (Accessed 17 March 2022).
[127] Ibid.
[128] Ibid.
[129] Ibid.
[130] CBC, "Canadian Spies Targeted Brazil's Mines Ministry: Report." *CBC*, 7 October 2013. https://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975 (Accessed 13 April 2022).
[131] Seglins.
[132] Ibid. See the presentation in the CBC article titled "Cyber activity spectrum" for further detail on each of the CSE's digital arsenal.

cooperative relationship with NSA and its "global hacking operations."[133] Furthermore, the CSE adopted "deception tactics" for its own cyber operations that closely resemble the tactics used by the Government Communications Headquarters (GCHQ), including disruptive tactics aimed at manipulating online information.[134] As such, several classified documents reveal that the CSE has already developed its offensive capabilities and many of its tools and tactics have been learned from its intelligence partners in Five Eyes.

Some of CSE's other capabilities revealed in the Snowden revelations also appear equally troubling. For example, the "Airport Wi-fi" story that surfaced in 2014 exposed some of the CSE's operations inside Canada's international airports—which involved accessing the information of anyone connected to the airport's internet and then storing and monitoring these individuals' online activity long after they left the airport.[135] The problem with instances like this is that they are treated by the CSE as one of their "normal global collection" practices of bulk data.[136] Problematically, this begs the question of what this means for Canadians since this internet-tracking experiment was done inside Canada and very likely intercepted Canadians' online activities and communications.[137]

These are a few examples of the classified documents that have revealed the extent of the CSE's capabilities by the mid-2010s. The fact that they all became public after the Snowden revelations also hints at how good the CSE is at maintaining the secrecy of its capabilities—the CSE's capabilities were only revealed because of a defecting NSA employee. Some of these, notably the cyberwarfare tools developed by CSE in its espionage activities in Brazil also show how effective the agency is behind the digital wall.

This brings us back to the concerns surrounding the CSE's active and defensive cyber operations mandates: what will the CSE be able/willing to do under its new powers? Given how CSE's revealed activities are very controversial and incredibly extensive, the CSE may interpret its powers broadly. This is especially so when national security matters make secrecy deemed necessary, despite their contradictions to the

[133] Ryan Gallagher, "Documents reveal Canada's secret hacking tactics." *The Intercept.* 23 March 2015. https://theintercept.com/2015/03/23/canada-cse-hacking-cyberwar-secret-arsenal/ (Accessed 23 March 2022).
[134] Ibid.
[135] Clement, pp. 129-130.
[136] Ibid., p. 131.
[137] Ibid.

interests of the public and democratic principles.[138] As discussed in the previous section about cybersecurity's growing salience in Canadian law, this is indeed a concern. While it is important that the CSE can conduct these operations for the sake of Canada's protection, how far it will go as it did under its three original mandates could cause a public backlash. Nevertheless, statutory law has certainly worked to the agency's benefit in ensuring "deep secrecy" in its activities and producing "counter law."[139]

Now, the CSE can expand its cyber activities under its new mandates. Most likely, these will continue to be *covert* cyber operations. These cyber operations are meant to aid a country's diplomatic, and military objectives and national security concerns and be conducted at a scale that makes the country's objectives attainable.[140] For example, Canada's own hacking capabilities via QUANTUM have allowed the CSE to covertly target users globally while camouflaging its tracks to make it appear other international actors were responsible for these acts.[141] The cyberwarfare tools it accumulated in the 2010s enable the CSE to conduct covert operations with general ease. But a balance is needed here: if the covert activity is too extensive, then who is conducting the cyber operations may be revealed as well as important state secrets—an embarrassment and serious compromise of the country's own security interests.[142]

Having the capabilities to conduct these cyber operations can be seen as an adequate approach to deter adversaries. But several scholars have argued that the Trudeau government's minimal mention of *deterrence* and goal to develop a *deterrence strategy* in *Strong, Secured and Engaged* may make Ottawa lag behind in punishing or denying adversaries from targeting Canada's cyber domain. Furthermore, Ottawa still has a long way to go for adopting norms focused on cyber aggression and demonstrating what is capabilities are to its potential adversaries.[143] But this framework of *deterrence* does not adequately capture how Canada's cybersecurity concerns should be approached. Despite these concerns, deterrence in the cyber domain is not simple to demonstrate. Identifying the originator of any kind of cyber attack is an exhaustive process that takes time and resources to accurately pinpoint the user responsible for the

[138] Prince, p. 43.
[139] Walby and Anaïs, pp. 377, 379.
[140] Michael Warner, "A Matter of Trust: Covert Action Reconsidered," *Studies in Intelligence* 63, no. 4 (2019): p. 33.
[141] Gallagher, "Documents reveal Canada's secret hacking tactics."; Seglins.
[142] Warner, "A Matter of Trust," p. 33.
[143] Ryder McKeown and Alex Wilner, "Deterrence in space and cyberspace," in *Canadian Defence Policy in Theory and Practice*. edited by Thomas Jeneau, Philippe Lagassé, and Srdjan Vucetic (Cham, Switzerland: Palgrave Macmillan, 2020), pp. 408-411.

damage.[144] The benefits (such as monetary gain) outweigh the potential costs. Rather, it is more appropriate to keep the country's defensive capabilities a higher priority than deterrence to thwart an attack because an attacker only needs to succeed once to harm a country's cyber infrastructure.[145] A state can also protect itself when it is able to conduct offensive cyber attacks while remaining anonymous.[146]

How far Ottawa will go in interpreting the *CSE Act* is still a mystery. Some scholars point out that the CSE will need to overcome large obstacles in its transition. According to Marco Munier, much of Canada's intelligence community's culture has followed a defensive, "minimalist" approach in its operations.[147] However, this may not be the case for the CSE. In a 2001 article by Marco Rudner, it was revealed that by the mid-1990s, the CSE's activities in economic intelligence expanded from defensive purposes, to actively observing and identifying how to leverage Canada's own economic advantages to maximize the benefits of the Canadian commercial market could obtain in bilateral and multilateral trade agreements while preventing any of its economic partners from exploiting the country's own economic situation.[148] It can then be suggested that the CSE maintained its *active* cyber role in economic espionage into the twenty-first century.

The Snowden files reinforce this observation and show that the agency was very energetic in expanding its cyber defensive capabilities. Even for its defensive cyber capabilities, the agency was not resting, but remaining active and continuously adapting to new threats. For example, two top-secret PowerPoint presentations from 2011 and 2015 reveal that the CSE sought to input "sensors" across all of Canada's internet services and infrastructure to detect malicious cyber threats entering Canada's cyber domain.[149] Recommendations on appropriate courses of action to improve on

[144] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense,Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2 (2015): p. 321.
[145] Ibid., p. 322.
[146] Ibid., p. 318.
[147] Munier, p. 444.
[148] It should be noted that this does not mean that it is a fact that the CSE fed its information to Canadian private firms and Crown corporations. It is likely that politicians used the gathered intelligence to assist them in what they wanted during negotiations and to advice Canadian businesses (without mentioning their sources). See, Rudner, "Canada's Communications Security Establishment From Cold War to Globalization," pp. 119-120.
[149] Clement, pp. 131-132.

identified technical barriers were also brought up in these presentations.[150] As such, even on the defensive side of cybersecurity, the CSE was not a minimalist.

In addition to these examples, the earlier-mentioned cases of CSE's espionage activities, hacking capabilities, and the airport Wi-Fi interception experiment make it clear that the CSE's role has extensively focused on improving its ability to deter attackers and target Canada's adversaries. Its experience in actually *hacking* foreign targets in the Middle East and Mexico[151] can ascertain for us how far its offensive capabilities have developed prior to the *CSE Act*. During a committee session in the House of Commons in 2018, representatives from CSE assured parliamentarians that the CSE already had the capabilities to conduct defensive and active cyber operations—enough that the CSE can effectively provide cyber support for the CF.[152] Hence, the CSE does not face significant barriers in adopting its new statutory mandates.

With these capabilities already developed and operational, the CSE will be able to conduct its operations sooner rather than later. We can safely say that such operations will not allow acts that harm human life and Canada's democratic institutions.[153] Nevertheless, what operations will be done is still less certain. One remaining problem in the *CSE Act* is that it does not define "cyber operation,"[154] which hinders our scope of what kind of tactics and methods can be used to target Canada's adversaries and their critical infrastructure.

When conducting its cyber operations, the CSE will have to remain complicit with the limitations imposed on the "use of force" and not use its cyber capabilities for coercive purposes, as per Article 2(4) of the United Nations Charter.[155] Ottawa will need to keep this in mind because these kinds of cyber operations are meant to exert a country's influence abroad and hinder its adversaries through methods that allow the attacking/defending country to "use force" that is not physical but still damaging.[156] In other words, Ottawa must ensure it can somehow measure the consequences of the

[150] Ibid.
[151] Seglins.
[152] Canada, Parliament, House of Commons, *Standing Committee on Public Safety and National Security* (1st sess., 42nd parliament, 2018. Committee report no. 097), p. 12. https://www.ourcommons.ca/Content/Committee/421/SECU/Evidence/EV9668804/SECUEV97-E.PDF
[153] Williams, p. 142.
[154] Leah West, "Cyber force: The International Legal Implications of the Communication Security Establishment's Expanded Mandate Under Bill C-59." *Canadian Journal of Law and Technology* 16, no.2 (2018): p. 387.
[155] Ibid., pp. 387-388.
[156] Warner, p. 37.

kind of force it intends to use. Regardless of this specific concern former DND Minister, Harjit Sajjan, stated that these types of operations will only be conducted against a foreign adversary that intends to harm Canada's security interests, which he will be required to authorize before being initiated.[157] The Supreme Court of Canada has also weighed in on this issue and declared that Ottawa and the CSE are to abide by principles of customary and conventional international law during its active cyber operations.[158] As such, we can hypothesize that the CSE will remain constrained by these values and be selective when deploying its cyber operations.

The *CSE Act* opens new doors for Canada's SIGINT-specializing agency. Its new cyber capabilities have been enshrined under statutory law even though its practices and operations may be seen as undemocratic. The CSE now enters a new chapter in its responsibility to safeguard Canada's cyber domain and is already prepared to fulfill its new statutory mandates.

After the *CSE Act*: The CSE at the Forefront of Canadian Security

Beginning in 2019, the international environment has been very chaotic, giving the CSE greater legitimacy for its new mandates and empowering its voice in Ottawa. Both the COVID-19 pandemic and Russia's invasion of Ukraine are making CSE's capabilities critical for providing a first-line of defence for Canada's cyber interests. As 2021 was coming to a close, Prime Minister Trudeau established a committee of his senior cabinet ministers to develop a new national cyber strategy at the same time the intelligence community "vocal" warnings about growing cyber threats and aggressive states.[159] By early 2021, the director of CSIS, David Vigneault, put bluntly in his agency's report that 2020 saw more acts of espionage and foreign interference not seen since the Cold War: "the key national security threats facing Canada, namely violent extremism, foreign interference, espionage and malicious cyber activity, accelerated, evolved and in many ways became much more serious for Canadians."[160] For the CSE in particular, the

[157] West, "Cyber force," p. 386.
[158] Ibid., p. 387.
[159] Alex Boutilier, "Trudeau Tasks Cabinet with new Cybersecurity Plan amid Growing Attacks, Spying," *Global News,* 16 December 2021. https://globalnews.ca/news/8456721/trudeau-cybersecurity-plan-cabinet/ (Accessed 3 April 2022).
[160] Canada, Canadian Security Intelligence Service, *CSIS Public Report 2020* (Ottawa, ON: Canadian Security Intelligence Service, 2021), p. 8.

CSE annual report for 2020-2021 noted that the agency had to respond to 2206 cyber security incidents targeting the Government of Canada.[161]

The COVID-19 pandemic has made the international community rely an incredible amount on the internet to fulfill daily tasks that they otherwise would have done in-person. When the pandemic started, everyone stayed home and became reliant on their computers and electronics to connect with the outside world. Consequentially, this made many vital sectors in society targets of malicious cyber attacks. Countries across the globe have had their health care sectors targeted by cyber criminals and rogue groups because of the sector's importance yet fragile cyber infrastructure.[162] Canada's health care sector too was hit like many others. As the pandemic unraveled in March 2020, the CSE warned that cyber groups were exploiting the general panic in Canada to destroy intellectual property (e.g., vaccine research) unless the country's health organizations paid a costly ransom.[163] In the early summer of that same year, cyber criminals were targeting businesses across the Americas to gain remote access to sensitive business documents while other criminal cells began to increase the number of phishing and fraud campaigns.[164]

The situation got worse as the pandemic continued. CSE's sub-unit, the Cyber Centre, reported that cyberattacks in 2021 increased significantly from 2020 and were going to become more aggressive towards the country's critical infrastructure.[165] Many of these groups are linked to authoritarian states. For example, the ransomware group called Sodinokibi is based in Russia and is responsible for conducting the largest ransomware attack in history, compromising America's Kaseya VSA supply chain.[166] In response to these serious cyber vulnerabilities in early 2021, the CSE Chief claimed that

[161] Canada, Communications Security Establishment, *Communications Security Establishment Annual Report 2020-2021* (Ottawa, ON: Communications Security Establishment, 2021).
[162] Bernardi Pranggono and Abdullahi Arabo, "COVID-19 Pandemic Cybersecurity Issues," *Internet Technology Letters* 4, no. 2 (2021): p. 1.
[163] Catherine Tunney, "Canada's Health Sector at Risk of Cyberattacks as COVID-19 Fear Spreads: CSE," *CBC*, 19 March 2020. https://www.cbc.ca/news/politics/health-covid-cyberattack-pandemic-1.5502968 (Accessed 18 March 2022).
[164] INTERPOL, *INTERPOL Report Shows Alarming Rate of Cyberattacks During COIVD*-19 (Lyon, France: INTERPOL), p. 6, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
[165] Canada, Communications Security Establishment, *Cyber Threat Bulletin: The Ransomware Threat in 2021* (Ottawa, ON: Communications Security Establishment, 2021), p. 5.
[166] Ibid.

greater action was necessary by Ottawa to provide the necessary resources to the CSE to make Canada's cyber domain harder to attack and exploit by these malicious groups.[167]

As these developments occurred, the CSE adapted well to its new mandates. When the pandemic started, the CSE was still in the process of institutionalizing its new mandates when it was suddenly tasked with thwarting attacks targeting Canada's health care system while trying to protect its own employees from the virus's rapid spread.[168] Its financial assets were also being bolstered by Ottawa. In response to the emerging situation in cybersecurity, the agency received $6.3 million from Ottawa, with another $47 million added to its annual budget in February 2021.[169] Furthermore, the CSE significantly rebalanced its focus between SIGINT and cybersecurity—transferring many of its assets and employees dedicated to SIGINT over to cybersecurity operations.[170] It appears to have paid off: in December 2021, the CSE publicly confirmed that it was conducting cyber operations aimed at cyber criminals targeting Canada's critical infrastructure and reportedly inflicted significant damage to these groups.[171] This news suggests that the CSE has been able to adapt despite the challenges it faced in early 2020. This also shows that the previous experiments and capabilities it has developed throughout the 2010s have likely aided in its quick responsiveness.

Very recently, Russia has re-appeared on Canada's radar of national security threats and the CSE has been very active. As tensions began mounting in late January of this year, the CSE warned that Russian-backed cyber groups were starting to increase their number of attacks.[172] In one incident, the CSE warned of increasing Russian-backed cyber attacks on Canada's critical infrastructure on the same day Global Affairs

[167] Mike Lapointe, "'We must make Canadian Cyberspace a Harder Target,' says CSE Chief," *The Hill Times*, 31 May 2021. https://www.hilltimes.com/2021/05/31/we-must-make-canadian-cyberspace-a-harder-target-says-cse-chief/298987 (Accessed 18 March 2022).
[168] Bill Robinson, "Collection and Protection in the Time of Infection," p. 127.
[169] Ibid., p. 129.
[170] Ibid., pp. 132-133. While how much of its resources and manpower is unknown, SIGINT operations accounted for 70 percent of CSE's budget and its employees. This means that the shift would have been significant, given the magnitude of the ransomware attacks.
[171] Alex Boutilier, "Canadian Spy Agency Targeted Foreign Hackers to 'Impose a Cost' for Cybercrime," *Global News*, 6 December 2021. https://globalnews.ca/news/8429008/canadian-spy-agency-targets-cybercrime/ (Accessed 18 March 2022).
[172] Christopher Nardi, "Threat of Russian-Backed Cyber Attacks Growing Amid Ukraine Tensions, Canada's Cybersecurity Agency Warns," *National Post*, 21 January 2022. https://nationalpost.com/news/politics/threat-of-russian-backed-cyber-attacks-growing-amid-ukraine-tensions-canadian-cybersecurity-agency-warns (Accessed 19 March 2022).

Canada became a target of these attacks.[173] Both the CSE and CSIS continued to call on Ottawa and the Trudeau government to invest more resources and give more attention to securing Canada's cyber infrastructure and cyber domain from Russian hackers, who continue to target Canadian infrastructure whenever Canada appeared vulnerable: "Russians have sort of this habit of going after critical infrastructure at times when nobody's looking. [For example,] a Friday night."[174] The continuous influx of crises and vulnerabilities impacting Canada means that constant vigilance and seriousness need to be performed by Ottawa and its intelligence-oriented agencies.

In the aftermath of Russia's invasion of Ukraine in late February, Ottawa dispatched a small contingent of CSE personnel to work with the Canadian Forces' team tasked in Ukraine with conducting cyber operations and intelligence gathering.[175] Presently, it is public knowledge that the CSE is conducting counter-intelligence operations to discredit the Kremlin's online disinformation activities.[176]

In response to the conflict, the Minister of DND has called for new measures in Ottawa to table "aggressive options" that would help expand the CF's budget and protect Canada's security interests from potential future Russian aggression.[177] And it appears this call from the defence minister has greatly benefited the CSE. A landmark in the post-Cold War period, the CSE's annual budget can double in the next five years. The federal budget that was tabled in the House of Commons pledges to give the CSE $875.2 million over the next fives years, with a large portion of the funding to be specifically allocated towards assisting the agency's ability to carry out its two new mandates, protect critical infrastructure, and make government electronic systems more

[173] Christopher Nardi, "Canada's Foreign Affairs Department Targeted in 'Significant' Cyber Attack." *National Post*, 24 January 2022. https://nationalpost.com/news/politics/canadas-foreign-affairs-department-targetted-in-significant-cyber-attack (Accessed 19 March 2022).
[174] Tunney, "Canadian Intelligence Agency Calls for Ramped-Up Cyber Defences A after Russia Invades Ukraine."
[175] Amanda Connolly, "Canada Providing Cyber 'Support' to Ukraine Against Russian Invasion. Here's What We Know," *Global News*, 24 February 2022. https://globalnews.ca/news/8643680/russia-invasion-ukraine-cyber-warfare/ (Accessed 19 March 2022).
[176] Alex Boutilier, "Canadian Intelligence Flags Russian Disinformation Campaigns amid Ukraine War," *Global News*, 1 April 2022. https://globalnews.ca/news/8727605/canadian-intelligence-flags-russian-disinformation-campaigns/ (Accessed 3 April 2022).
[177] CBC, "Defence Minister says She's Considering 'Aggressive Options' to Increase Canada's Military Spending," *CBC*, 16 March 2022. https://www.cbc.ca/news/politics/anand-defence-spending-1.6387361 (Accessed 19 March 2022).

resilient to cyber-attacks.[178] As this crisis currently stands, the situation on the ground is still developing.

Concluding Thoughts

The last two decades have been some of the most eventful and important periods in CSE's post-Cold War history. Based on this paper's findings, there are two conclusions to be drawn: first, the new mandates introduced under the *CSE Act* liberally broaden the CSE's powers and responsibilities via statutory law to do to protect Canada from ever-increasing security concerns in the cyber realm, despite how controversial they may be. Secondly, this *Act* signals that the agency's secretive nature will continue to remain unchanged at the cost of transparency and oversight via statutory legitimacy. This essentially means that the CSE now has an immense amount of power that is unheard of elsewhere in Ottawa. This is compounded by the fact that cybersecurity issues in Canada are not shared widely outside the CSE amongst Canada's intelligence community.[179]

Additionally, the international crises that emerged since 2020 could cause the CSE's operations to expand even further along with its importance in protecting Canadian society. After all, the situation in the international community is dire right now: the former opponent of the CSE—the Soviet Union—has its own successor state that is very hostile to the West, the Russian Federation. This leads us to a similar situation to the Cold War era, where the law was relegated for the sake of preserving Canada's national security interests through secrecy.[180] What we are witnessing now is the *securitization* through Ottawa's new policy initiatives in intelligence and defence, as mentioned in the last section. This point of *securitization* in a country's policy process is where an existing existential threat legitimatizes the government's decision to bolster its own security measures that are deemed appropriate to the identified threat.[181] The Russian Federation and the growing number of malicious cyber attacks support Ottawa's threat perception (as have the events prior to the *CSE Act's* ascension to law).

[178] Catherine Tunney, "Electronic Espionage Agency Getting Major Funding Boost to Ward off Cyber Attacks," *CBC*, 7 April 2022. https://www.cbc.ca/news/politics/budget-cyber-funding-1.6411613 (Accessed 9 April 2022).
[179] Malone and Malone, "The 'Wicked Problem' of Cybersecurity Policy," p. 169.
[180] Prince, p. 43.
[181] Rita Floyd, "Can Securitization Theory be Used in Normative Analysis? Towards a Just Securitization Theory," *Security Dialogue* 42, no. 4-5 (2011): p. 428.

While the CSE's expansion is good for Canada's security, it can easily become a double-edged sword for Canadians. Transparency and accountability remain unresolved issues for the CSE and many of its counterparts in Canada's intelligence community.[182] Despite the NSIRA being established at the same time the *CSE Act* passed in 2019, much of what can be reviewed by the NSIRA in the CSE's operations only provides the public with abstract and vague analyses of the CSE's activities.[183] Similarly, the intelligence commissioner's powers do not extend into active and defensive cyber operations.[184] As the international environment becomes more destabilized, this issue may not be resolved.

This lack of transparency will contribute to one undesirable effect: an enduring lack of public knowledge and awareness about the CSE. In this regard, the Canadian public remains largely unaware of the CSE's existence. In 2017, a study found that only 3 percent of Canadians were able to correctly name the CSE and what its responsibilities are.[185] This was the same year that the *CSE Act* was first introduced, under the National Security Act. In 2020, a year after the *CSE Act* was passed, the Phoenix PSI groups conducted a new poll on behalf of the CSE and found the number surprisingly dropped—only 2 percent of Canadians could name the agency while only 1 percent could name both the agency and the Cyber Centre.[186] This is concerning, especially given that the *CSE Act* gained royal assent the year prior. Despite the fact the public knows little about the agency, those who are familiar with the agency are beginning to lose trust in the agency, with the percentage of those trusting the agency falling from 73 percent in 2017 to 63 percent in 2020.[187] Despite the advancements in the CSE's legal arsenal, the public remains woefully unaware of the agency. As such, there will remain a gap in the amount of scrutiny the agency needs to receive from Canadians. Equally important, the CSE will have to be careful that is does not commit something that may entice tin-foil-hat-enthusiasts to cause unnecessary social disturbances amongst the public who lack a full context about the situation.

---

[182] Thomas Juneau and Dominic Rochon, "Improving Transparency in Canada's National Security and Intelligence Community," *Policy Options*, 13 January 2021. https://policyoptions.irpp.org/magazines/january-2021/improving-transparency-in-canadas-national-security-and-intelligence-community/ (Accessed 19 March 2022).

[183] Clement, p. 128.

[184] Nesbitt, p. 20.

[185] Jim Bronskill, "Most Canadians Don't Really Know Much About Canada's Cyberspy Agency," *Global News*, 8 November 2017. https://globalnews.ca/news/3849709/canada-cyberspy-agency-canadians/ (Accessed 1 April 2022).

[186] *Canada, Communications Security Establishment, Attitudes Towards the Communications Security Establishment - Tracking Study: Final Report* (Ottawa, ON: *Communications Security Establishment*, 2020), p. 1.

[187] Ibid., p. 2.

Despite these concerns, the 2019 *CSE Act* is the culmination of growing security risks that needed a more robust SIGINT agency to address. These powers were timely introduced to address the crises that emerged in 2020. However, this still does not diminish the prior-mentioned concerns, and Canadians need to be prepared for the new reality. Whatever concerns there are over what the CSE will do, the agency's activities will remain shrouded in secrecy and continue to pose dilemmas for Canada's democratic ideals.

Bibliography

Austen, Ian. "Hit-and-Run That Killed Canadian Soldier Is Called Terrorist Attack." *The New York Times,* 21 October 2014. https://www.nytimes.com/2014/10/22/world/americas/canadian-soldier-run-down-in-what-officials-call-act-of-terror-dies.html (Accessed 11 March 2022).

Bigo, Didier, Sergio Carrera, Elspeth Guild and R.B.J. Walker. *The Changing Landscape Of European Liberty And Security: Mid-Term Report On The Results Ff The CHALLENGE project*. Brussels, Belgium: Centre for European Policy Studies, 2007.

Bolt, Alexander, and Philippe Lagassé. "Beyond Dicey: Executive Authorities In Canada." *The Journal of Commonwealth Law* 3, no. 1 (2021): pp. 1-53.

Boutilier, Alex. "Canadian Intelligence Flags Russian Disinformation Campaigns Amid Ukraine War." *Global News,* 1 April 2022. https://globalnews.ca/news/8727605/canadian-intelligence-flags-russian-disinformation-campaigns/ (Accessed 3 April 2022).

Boutilier, Alex. "Trudeau Tasks Cabinet With New Cybersecurity Plan Amid Growing Attacks, Spying." *Global News,* 16 December 2021. https://globalnews.ca/news/8456721/trudeau-cybersecurity-plan-cabinet/ (Accessed 3 April 2022).

Boutilier, Alex. "Canadian Spy Agency Targeted Foreign Hackers To 'Impose A Cost' For Cybercrime." *Global News,* 6 December 2021. https://globalnews.ca/news/8429008/canadian-spy-agency-targets-cybercrime/ (Accessed 18 March 2022).

Bronskill, Jim. "Most Canadians Don't Really Know Much About Canada's Cyberspy Agency." *Global News,* 8 November 2017. https://globalnews.ca/news/3849709/canada-cyberspy-agency-canadians/ (Accessed 1 April 2022).

Canada. Canadian Security Intelligence Service. *CSIS Public Report 2020*. Ottawa, ON: Canadian Security Intelligence Service, 2021.

Canada. Communications Security Establishment. *Communications Security Establishment Annual Report 2020-2021*. Ottawa, ON: Communications Security Establishment, 2021.

Canada. Communications Security Establishment. *Cyber Threat Bulletin: The Ransomware Threat In 2021.* Ottawa, ON: Communications Security Establishment, 2021.

Canada. Communications Security Establishment. "Privacy." 26 October 2020. https://www.cse-cst.gc.ca/en/accountability/privacy (Accessed 29 March 2022).

Canada. Communications Security Establishment. *Attitudes Towards The Communications Security Establishment - Tracking Study: Final Report*. Ottawa, ON: *Communications Security Establishment*, 2020.

Canada. Communications Security Establishment. *Cyber Threats To Canada's Democratic Process.* Ottawa, ON: Communications Security Establishment, 2017.

Canada. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa, ON: Department of National Defence, 2017.

Canada. Parliament. House Of Commons. *Standing Committee On Public Safety And National Security.* 1st sess., 42nd parliament, 2018. Committee report no. 097. https://www.ourcommons.ca/Content/Committee/421/SECU/Evidence/EV9668804/SECUEV97-E.PDF

Canada. Privy Council Office. *Securing An Open Society: Canada's National Security Policy.* Ottawa, ON: Privy Council Office, 2004.

Canada. Public Safety Canada. *National Cyber Security Action Plan (2019-2024)*. Ottawa, ON: Public Safety Canada, 2019.

Canada. Public Safety Canada. *National Cyber Security Strategy: Canada's Vision For Security And Prosperity In The Digital Age*. Ottawa, ON: Public Safety Canada, 2018.

Canada. Public Safety Canada. *Action-Plan 2010-2015 For Canada's Cyber Security Strategy.* Ottawa, ON: Public Safety Canada, 2013.

CBC. "Defence Minister Says She's Considering 'Aggressive Options' To Increase Canada's Military Spending." *CBC,* 16 March 2022. https://www.cbc.ca/news/politics/anand-defence-spending-1.6387361 (Accessed 19 March 2022).

CBC. "Canadian Spies Targeted Brazil's Mines Ministry: Report." *CBC,* 7 October 2013. https://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975 (Accessed 13 April 2022).

CCLA. "The New Communications Security Establishment Act in Bill C-59." *Canadian Civil Liberties Association*, 12 September 2017. https://ccla.org/privacy/nationalsecurity/the-new-communications-security-establishment-act-in-bill-c-59/ (Accessed 26 March 2022).

Chapin, Paul H. "Into Afghanistan: The Transformation Of Canada's International Security Policy Since 9/11." *American Review of Canadian Studies* 40, no. 2 (2010): pp. 189-199.

Clement, Andrew. "Limits To Secrecy: What Are The Communications Security Establishment's Capabilities For Intercepting Canadian Internet Communications?." In Big Data Surveillance and Security Intelligence: The Canadian Case. Edited by David Lyon and David Murakami Wood, pp. 126-146. Vancouver, BC: University of British Columbia Press, 2021.

Clement, Andrew, Jillian Harkness, and George Raine. "Metadata – Both Shallow And Deep: The Fraught Key To Big Mass State Surveillance." In *Big Data Surveillance and Security Intelligence: The Canadian Case*. Edited by David Lyon and David Murakami Wood, pp.253-268.Vancouver, BC: University of British Columbia Press, 2021.

Connolly, Amanda. "Canada Providing Cyber 'Support' To Ukraine Against Russian Invasion. Here's What We Know." *Global News*, 24 February 2022. https://globalnews.ca/news/8643680/russia-invasion-ukraine-cyber-warfare/ (Accessed 19 March 2022).

Duyvesteyn, Isabelle. "Intelligence And Strategic Culture: Some Observations." *Intelligence and National Security* 26, no. 4 (2011): pp. 521-530.

Ericson, Richard V. "The State Of Preemption: Managing Terrorism Risk Through Counter Law." In *Risk And War On Terror.* Edited by Louise Amoore and Marieke de Goede, pp.57-76. Oxon, UK: Routledge, 2008.

Fantz, Ashley, Josh Levs, Catherine E. Shoichet. "'Terrorist' Murdered Soldier 'In Cold Blood,' Canada's Prime Minister Says." *CNN*, 23 October 2014. https://www.cnn.com/2014/10/22/world/americas/canada-ottawa-shooting/index.html (Accessed 11 March 2014).

Floyd, Rita. "Can Securitization Theory Be Used In Normative Analysis? Towards A Just Securitization Theory." *Security Dialogue* 42, no. 4-5 (2011): pp. 427-439.

Forcese, Craig. "Bill C-59 And The Judicialization Of Intelligence Collection." In *Big Data Surveillance And Security Intelligence: The Canadian Case*. Edited by David Lyon and David Murakami Wood, pp.166-179. Vancouver, BC: University of British Columbia Press, 2021.

Forcese, Craig. "Threading The Needle: Structural Reform & Canada's Intelligence-To-Evidence Dilemma." *Manitoba Law Journal* 42, no. 4 (2019): pp. 131-188.

Forcese, Craig. "Putting The Law To Work For CSE: Bill C-59 And Reforming The Foreign Intelligence Collection And Cybersecurity Process." *Ottawa Faculty Of Law Working Paper* 2017-43 (2017).

Gallagher, Ryan. "Documents Reveal Canada's Secret Hacking Tactics." *The Intercept.* 23 March 2015. https://theintercept.com/2015/03/23/canada-cse-hacking-cyberwar-secret-arsenal/ (Accessed 23 March 2022).

Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, And Deception In Cyberspace." *Security Studies* 24, no. 2 (2015): pp. 316-348.

INTERPOL. *INTERPOL Report Shows Alarming Rate Of Cyberattacks During COIVD*-19, Lyon, France: INTERPOL. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Juneau, Thomas and Dominic Rochon. "Improving Transparency In Canada's National Security And Intelligence Community." *Policy Options,* 13 January 2021. https://policyoptions.irpp.org/magazines/january-2021/improving-transparency-in-canadas-national-security-and-intelligence-community/ (Accessed 19 March 2022).

Lagassé, Philippe. "Defence Intelligence And The Crown Prerogative In Canada." *Canadian Public Administration* 64, no. 4 (2021): pp. 539-560.

Lapointe, Mike. "'We Must Make Canadian Cyberspace A Harder Target,' Says CSE Chief." *The Hill Times,* 31 May 2021. https://www.hilltimes.com/2021/05/31/we-must-make-canadian-cyberspace-a-harder-target-says-cse-chief/298987 (Accessed 18 March 2022).

Littlewood, Jez. "The Canadian Security Intelligence Service (CSIS)." In *Top Secret Canada.* Edited by Stephanie Carvin, Thomas Juneau, and Craig Forcese, pp. 45-71. London, ON: University of Toronto Press, 2020.

Lyon, David and David Murakami Wood. “Introduction.” In *Big Data Surveillance And Security Intelligence: The Canadian Case*. Edited by David Lyon and David Murakami Wood, pp.1-18. Vancouver, BC: University of British Columbia Press, 2021.

Lyon, David. "Airport Screening, Surveillance, And Social Sorting: Canadian Responses To 9/11 In Context," *Canadian Journal Of Criminology And Criminal Justice* 48, no. 3 (2006): pp. 397-412.

Malone, Eloise F., and Michael J. Malone. "The “Wicked Problem” Of Cybersecurity Policy: Analysis Of United States And Canadian Policy Response." *Canadian Foreign Policy Journal* 19, no. 2 (2013): pp. 158-177.

McKeown, Ryder and Alex Wilner. “Deterrence In Space And Cyberspace.” In *Canadian Defence Policy In Theory And Practice*. Edited by Thomas Jeneau, Philippe Lagassé, and Srdjan Vucetic, pp. 399-416. Cham, Switzerland: Palgrave Macmillan, 2020.

Munier, Marco. "The Canadian National Intelligence Culture: A Minimalist And Defensive National Intelligence Apparatus." *International Journal* 76, no. 3 (2021): pp. 427-445.

Nardi, Christopher. “Canada’s Foreign Affairs Department Targeted In ‘Significant’ Cyber Attack.” *National Post,* 24 January 2022. https://nationalpost.com/news/politics/canadas-foreign-affairs-department-targetted-in-significant-cyber-attack (Accessed 19 March 2022).

Nardi, Christopher. “Threat Of Russian-Backed Cyber Attacks Growing Amid Ukraine Tensions, Canada’s Cybersecurity Agency Warns.” *National Post,* 21 January 2022. https://nationalpost.com/news/politics/threat-of-russian-backed-cyber-attacks-growing-amid-ukraine-tensions-canadian-cybersecurity-agency-warns (Accessed 19 March 2022).

Nesbitt, Michael. "Reviewing Bill C-59, An Act Respecting National Security Matters 2017: What’s New, What’s Out, And What’s Different From Bill C-51, A National Security Act 2015?." *The School Of Public Policy Publications* 13, no. 12 (2020).

Parsons, Christopher A., Lex Gill, Tamir Israel, Bill Robinson, and Ronald J. Deibert. "Analysis Of The Communications Security Establishment Act And Related Provisions In Bill C-59 (An Act Respecting National Security Matters), First Reading." Toronto, ON: The Citizen Lab, 2017.

Pelletier, Jay and Craig Forcese, "Curing Complexity: Moving Forward From The Toronto 18 On Intelligence-To-Evidence." *Manitoba Law Journal* 44, no. 1 (2021): pp. 158-183.

Pozen, David E. "Deep Secrecy," *Stanford Law Review* 62, no. 2 (2010): pp. 257-340.

Pranggono, Bernardi, and Abdullahi Arabo. "COVID-19 Pandemic Cybersecurity Issues." *Internet Technology Letters* 4, no. 2 (2021): e247.

Rawat, Danda B., Ronald Doku, and Moses Garuba. "Cybersecurity In Big Data Era: From Securing Big Data To Data-Driven Security." *IEEE Transactions On Services Computing* 14, no. 6 (2019): pp. 2055-2072.

Roach, Kent and Craig Forcese. "Legislating In Fearful And Politicized Times: The Limits Of Bill C-51's Disruption Powers In Making Us Safer." In *After The Paris Attacks: Responses In Canada, Europe, And Around The Globe.* Edited by Edward M. Iacobucci and Stephen J. Toope, pp.141-158. Toronto, ON: University of Toronto Press, 2015.

Robinson, Bill. "Collection And Protection In The Time Of Infection: The Communications Security Establishment During The COVID-19 Pandemic." In Stress Tested: The COVID-19 Pandemic And Canadian National Security. Edited by Leah West, Thomas Juneau, Amarnath Amarasingam, pp. 127-144. Calgary, AB: LCR Publishing Services, 2021.

Robinson, Bill. "The Communication Security Establishment (CSE)." In *Top Secret Canada.* Edited by Stephanie Carvin, Thomas Juneau, and Craig Forcese, pp. 72-89. London, ON: University of Toronto Press, 2020.

Rosati, Nicholas. "Canadian National Security In Cyberspace: The Legal Implications Of The Communications Security Establishment's Current And Future Role As Canada's Lead Technical Cybersecurity And Cyber Intelligence Agency." *Manitoba Law Journal* 42, no. 4 (2019): pp. 189-206.

Rudner, Martin. "Challenge And Response: Canada's Intelligence Community And The War On Terrorism." *Canadian Foreign Policy Journal* 11, no. 2 (2004): pp. 17-39.

Rudner, Martin. "Canada's Communications Security Establishment From Cold War To Globalization." *Intelligence & National Security* 16, no. 1 (2001): pp.97-128.

Seglins, Dave. "Communication Security Establishment's Cyberwarfare Toolbox Revealed." *CBC,* 23 March 2015.

https://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978 (Accessed 17 March 2022).

Stephenson, Alan James. "Canadian National Security Culture: Explaining Post 9/11 Canadian National Security Policy Outcomes." PhD dissertation, Carleton University, 2016.

Tunney, Catherine. "Electronic Espionage Agency Getting Major Funding Boost To Ward Off Cyber Attacks." *CBC*, 7 April 2022. https://www.cbc.ca/news/politics/budget-cyber-funding-1.6411613 (Accessed 9 April 2022).

Tunney, Catherine. "Canadian Intelligence Agency Calls For Ramped-Up Cyber Defences After Russia Invades Ukraine." *CBC*, 24 February 2022. https://www.cbc.ca/news/politics/cyber-russia-cse-1.6362878 (Accessed 8 March 2022).

Tunney, Catherine. "Flaws In Cyber Defence Expose Government Information To State-Sponsored Theft: Report." *CBC*, 15 February 2022. https://www.cbc.ca/news/politics/cyber-defence-nsicop-1.6350802 (Accessed 14 March 2022).

Tunney, Catherine. "Canada's Health Sector At Risk Of Cyberattacks As COVID-19 Fear Spreads: CSE." *CBC*, 19 March 2020. https://www.cbc.ca/news/politics/health-covid-cyberattack-pandemic-1.5502968 (Accessed 18 March 2022).

Prince, Christopher. "On Denoting And Concealing In Surveillance Law." In *Big Data Surveillance and Security Intelligence: The Canadian Case*. Edited by David Lyon and David Murakami Wood, pp. 43-56. Vancouver, BC: University of British Columbia Press, 2021.

Wählen, Claire. "Trudeau Government Putting New Emphasis On Cybersecurity." *ipolitics*, 17 November 2015. https://www.ipolitics.ca/news/trudeau-government-putting-new-emphasis-on-cybersecurity (Accessed 14 March 2022).

Walby, Kevin, and Seantel Anaïs. "Communications Security Establishment Canada (CSEC), Structures Of Secrecy, And Ministerial Authorization After September 11." *Canadian Journal of Law & Society*, 27, no. 3 (2012): pp. 365-380.

Warner, Michael. "A Matter Of Trust: Covert Action Reconsidered." *Studies In Intelligence* 63, no. 4 (2019): pp. 33-41.

West, Leah. "Cyber Force: The International Legal Implications Of The Communication Security Establishment's Expanded Mandate Under Bill C-59." *Canadian Journal Of Law and Technology,* 16, no.2 (2018): pp. 381-415.

Williams, Stephanie. "The Powers Of The CSE After C-59: Are Privacy Rights At Risk?." *National Journal Of Constitutional Law* 40, no. 2 (2020): pp. 131-151.