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

NICHOLAS ROSATI *

CRITICAL COMMENTARY

ABSTRACT

National security policy in cyberspace presents a unique security challenge. Operations under the current mandate of the Communications Security Establishment (CSE) may incidentally capture Canadian information and thereby affect Canadian privacy interests. This raises serious concerns that this regime does not comply with sections 8 and 2(b) of the *Canadian Charter of Rights and Freedoms*. However, legislative reform under Bill C-59 implements external accountability measures in a manner that satisfies *Charter* requirements. Finally, Bill C-59 makes significant changes to CSE's mandate, namely the addition of an "active" cyber mandate. These changes raise concerns that the expansion of CSE's offensive capabilities, without careful oversight, may enable CSE to conduct

* Nicholas Rosati is a JD student at the Peter A. Allard School of Law at the University of British Columbia. In law school, he competed in the Jessup International Law Moot Court Competition. Upon graduation, he will clerk at the Supreme Court of British Columbia before articling at a full-service firm in Vancouver. He thanks his reviewers for their helpful feedback.

cyber operations that do not comply with Canada's international legal obligations and are not authorized by Parliament.

***Keywords*:** Bill C-59, *An Act respecting national security matters*, surveillance state, privacy, national security, Communications Security Establishment, cyberspace, cyber security, cyber operations, *Charter* rights, section 8, section 2(b), international law, offensive cyber capabilities.

I. INTRODUCTION AND OVERVIEW

This paper provides an overview and analysis of the contemporary Canadian approach to national security in cyberspace. Cyberspace presents a unique security challenge, which must be addressed while also meeting constitutional and international legal requirements. Operations under the current mandate of the Communications Security Establishment (CSE) may incidentally capture Canadian information and thereby affect Canadian privacy interests. However, such operations are not currently subject to independent judicial-like accountability. This raises serious concerns that this regime does not comply with sections 8 and 2(b) of the *Canadian Charter of Rights and Freedoms* (*Charter*).[1] However, this analysis also reveals that legislative reform under Bill C-59, which at time of writing is before the Canadian Senate, will likely implement external accountability measures in a manner that satisfactorily fulfills *Charter* requirements.[2] Finally, Bill C-59 makes significant changes to CSE's mandate, namely the addition of an "active" cyber mandate. These changes raise concerns that the expansion of CSE's offensive capabilities, without careful oversight, may enable CSE to conduct cyber operations that do not comply with Canada's international legal obligations and are not authorized by Parliament.

---

1 *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), c 11 [*Charter*].

2 Bill C-59, *An Act respecting national security matters*, 1st Sess, 42nd Parl, 2018 (as passed by the House of Commons 19 June 2018) [Bill C-59]; For clarity, the body of this paper refers to "sections" in Bill C-59 when referring to the provisions of specific acts the bill will create, however because the bill has yet to be enacted into law, they are formally considered "clauses" (as is reflected in this paper's footnote citations). Post-submission update: Bill C-59 received royal assent on June 21, 2019.

II. The Complex Nature Of National Security In Cyberspace

Cyberspace is a non-physical network that does not occupy any physical space and connects networks of computers to one another.[3] Vast quantities of data concerning private information are transferred and stored in cyberspace and therefore privacy interests are engaged by its operation and regulation. However, the fact that cyberspace exists due to a connection between physical devices means that that physical territory cannot be ignored in its regulation.[4] Cyberspace can also be used as a weapon for both for defensive and offensive purposes, such as cyberwarfare, which takes the form of cyber-attacks. In a cyber-attack, attackers utilize malware to penetrate computers, networks or websites to cause political, military, economic or other types of damage.[5] In 2011, foreign hackers, allegedly from China, launched an unprecedented attack on the Canadian government, targeting Defence Research and Development Canada, a civilian agency of the Department of National Defence.[6] These hackers thereby accessed highly classified information and forced the Finance Department and Treasury Board, two critical government institutions, to temporarily cut-off their internet access.[7] Connected attacks also targeted major Bay Street law firms, financial institutions and public-relations agencies involved in a foreign takeover attempt of Potash Corporation of Saskatchewan, in an effort to acquire inside information.[8] A state's contemporary infrastructure assets, such as those involving its military, transportation networks, electrical grids, natural resources and financial services are particularly vulnerable given

---

3 *ACLU v Reno*, 929 F Supp 824, 830-844 (ED Pa 1996), aff'd, 521 US 844 (1997) at 849-850.

4 Matthew E Castel, "International and Canadian Law Rules Applicable to Cyber Attacks by State and Non- State Actors" (2012) 10:1 CJLT 89 at 90.

5 *Ibid* at 91.

6 Greg Weston "Foreign hackers attack Canadian Government", *CBC News* (16 February 2011), online: <www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618> [perma.cc/Y4D3-QHLB].

7 *Ibid*.

8 Jeff Gray "Hackers linked to China sought Potash deal details: consultant", *The Globe and Mail* (30 November 2011), online: <www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/> [perma.cc/94Y3-V4CL].

their incorporation of and reliance on integrated computer technologies.[9] Events such as these cyber-attacks demonstrate the need for an effective national security policy capable of dealing with cyberthreats.

Complicating matters, competing interests make the implementation of national security measures in cyberspace more challenging. In addition to the agenda of national security and intelligence institutions, the interests of businesses and consumers, the privacy and expressive rights of individuals and a multitude of other interests must be taken into account.[10] Legislation promulgated in the wake of the September 11, 2001 terrorist attacks has strengthened the abilities of states to monitor internet activity with little independent oversight.[11] Some commentators argue that technology can amplify the effect of legislative changes favouring surveillance policies.[12] They argue that sophisticated surveillance technologies that harness the globally interconnected nature of communications reveal serious issues about compliance with the rule of law, which requires state action to be subject to oversight and accountability.[13]

III. THE CANADIAN NATIONAL SECURITY APPARATUS IN CYBERSPACE

A. Cybersecurity Policy in Canada

In June 2017, the federal government released an updated defence policy white paper entitled *Strong, Secure, Engaged: Canada's Defence Policy*, that presented the Government of Canada's long-term vision and approach to future defence policy.[14] A significant aspect of this update was the

---

9 Castel, *supra* note 4 at 95.

10 Eloise F Malone & Michael J Malone, "The 'wicked problem' of cybersecurity policy: analysis of United States and Canadian policy response" (2013) 19:2 Can Foreign Policy J 158 at 171.

11 Arthur J Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" (2003) 29 Queen's LJ 364 at 381, 385-386.

12 *Ibid* at 394.

13 Lisa M Austin, "Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State" in Michael Geist, ed, *Law, Privacy, and Surveillance in Canada in the Post-Snowden Era*, (Ottawa: University of Ottawa Press, 2015) 103 at 104.

14 Canada, Department of National Defence & Canadian Armed Forces, *Strong, Secure, Engaged: Canada's Defence Policy*, (Ottawa: National Defence, 2017), online (pdf):

Government's explicit acknowledgement that cybersecurity is an increasingly integral part of an effective modern national security regime. In the white paper, the Trudeau government declared that it "will assume a more assertive posture in the cyber domain" not only by strengthening its defensive capabilities, but also by developing an active cyber operations capacity.[15] The white paper noted that rapid technological development in the cyber domain presents a challenge that requires domestic and international legal frameworks to adapt.[16] It warned that technological advancement has revealed new cyberspace-related security issues. Terrorist groups, state-sponsored espionage and disruptive operations are all making use of the vulnerability arising out of the nature of cyberspace.[17] Jurisdictional challenges, arising out of the possibility that attacks on Canada can be carried out remotely from outside Canada, further complicate a national security response. In a military context, state and non-state actors may exploit vulnerabilities in existing technologically dependent military systems.[18] The white paper cautioned that Canada must develop advanced cyber capabilities to address such threats.[19] This is particularly significant because it represents the first time that the Canadian government has formally called for the development of an offensive cyberwarfare capability to respond to external threats.

A year later, the government released the 2018 *National Cyber Security Strategy*, which serves as an update to its first cybersecurity strategy released in 2010.[20] It defines cybersecurity as "the protection of digital information and the infrastructure on which it resides."[21] Like the 2017 white paper, the 2018 strategy calls for a stronger federal government response to cyberthreats.[22] Of particular significance is the (albeit brief) mention of

---

<dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf> [perma.cc/RJC9-SUZX] at 11.

15 *Ibid* at 15.

16 *Ibid* at 55.

17 *Ibid* at 56.

18 *Ibid*.

19 *Ibid* at 57.

20 Public Safety Canada, *National Cyber Security Strategy*, (Ottawa: Public Safety Canada, 2018), online (pdf): <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf> [perma.cc/23W4-5MER] at 2.

21 *Ibid* at 7.

22 *Ibid* at 11.

funding to support the newly created Canadian Centre for Cyber Security.[23] The Canadian Centre for Cyber Security, initially announced in February 2018, is housed within CSE and gained initial operational capability in Fall 2018. It is expected to be fully operational by Spring 2020.[24] The decision to open the centre within CSE represents an explicit choice of the government to consolidate cybersecurity operations under the authority and control of CSE.[25] However, beyond this, the report is limited to vague commitments to greater federal leadership, investment, collaboration and support of the private sector. The *National Cyber Security Strategy* provides little specificity regarding the nature of cybersecurity operations. The remainder of this paper considers the constitutional and international legal implications of CSE's current and future roles as Canada's lead technical cybersecurity and cyber intelligence agency.

B. The Current CSE Mandate

CSE is Canada's signals intelligence service. Signals intelligence involves the interception and analysis of communications and other electronic signals.[26] CSE exercises its authority under the *National Defence Act*, RSC 1985 c N-5 [*NDA*]. CSE's mandate authorizes it to do three things: "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence" (Mandate A); to advise, guide and provide "services to help ensure the protection of electronic information and of information infrastructures" (Mandate B); and to assist "federal law enforcement and security agencies in the performance of their lawful duties" (Mandate C).[27] Mandates A and B are constrained by a requirement that activities are not "directed at Canadians or any person in Canada; and…shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information."[28] Only under Mandate C may CSE target Canadians in its spying activities.

---

23 "Canadian Centre for Cyber Security" (last modified 16 November 2018) *Canada Communications Security Establishment*, online: <www.cse-cst.gc.ca/en/backgrounder-fiche-information> [perma.cc/8C3Z-8ECP].

24 *Ibid*.

25 *Ibid*.

26 "Foreign signals intelligence" (last modified 25 July 2019), online: *Canada Communications Security Establishment* <www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement> [perma.cc/K9FQ-BULV].

27 *National Defence Act*, RSC 1985, c N-5, s 273.64(1) [*NDA*].

28 *Ibid*, s 273.64(2).

However, this mandate is restricted to activities that CSE has explicit legal authorization to do.[29] Thus Mandate C allows CSE to extend technical assistance to the Canadian Security Intelligence Service (CSIS), Canada's principal national intelligence service, in the domestic context.[30] There is an implicit legal requirement in the domestic context (explained below) that a warrant must be sought for any actions that would otherwise violate section 8 of the *Charter*, which provides the right against unreasonable search or seizure.[31] While Mandates A, B and C appear discrete in theory, CSE cyber operations can result in legally problematic overlap in practice.

The potential for CSE Mandate A activities, which can only be carried out on foreign targets, to have domestic impacts or impacts on Canadians abroad is contemplated by the *NDA*, which specifies that the Minister of National Defence may authorize CSE "to intercept private communications."[32] This recognizes that situations may arise where information about Canadians is incidentally intercepted.[33] The law restricts such authorization to situations where the Minister is satisfied that: the interception is directed at foreign targets; the information cannot reasonably be obtained by other means; the value derivable from the information justifies the interception; and that privacy measures are in place to protect Canadian communications if they are unintentionally collected.[34] In practice, because one cannot be certain that a given activity will not accidentally implicate Canadian communications, ministerial authorizations are sought pre-emptively on a routine basis.[35]

This ministerial authorization regime raises profound accountability issues. CSE's ministerial regime differs from a traditional judicial warrant regime, which police agencies and CSIS are required to comply with, in two critical regards. Unlike the warrant process that police agencies and CSIS engage in, which authorizes surveillance in narrow circumstances (i.e. where

---

29 *Ibid*, s 273.64(3); Craig Forcese, "One Warrant to Rule Them All: Reconsidering the Judicialisation
of Extraterritorial Intelligence Collection" in Randy K Lippert et al, eds, *National Security, Surveillance and Terror*, 1st ed (Cham, Switzerland: Palgrave McMillan, 2016) 27 at 30 [Forcese 2016].

30 Forcese 2016, *supra* note 29 at 30.

31 *Ibid*.

32 *NDA*, *supra* note 27, s 273.65(1).

33 Forcese 2016, *supra* note 29 at 32.

34 *NDA*, *supra* note 27, s 273.65(2).

35 Forcese 2016, *supra* note 29 at 33.

the target, location and nature of the surveillance practices are specified), the ministerial process authorizes broad surveillance practices that are not constrained to specific individuals or subject matters).[36] Second, the ministerial process lacks judicial oversight. Unlike warrant processes, which require the approval of independent judges, ministerial authorizations are only subject to the approval of the Minister of Defence, a member of the executive.[37] Moreover the CSE mandate, codified in 2001, does not reflect the extent to which technological advancement has blurred the line between foreign and domestic targets. For instance, an email or instant message intercepted overseas could belong to a Canadian or originate from within Canada.[38] The collection of metadata is a prominent example of such blurring that raises privacy concerns. CSE describes metadata as "the context, but not the content of a communication," including information such as location data, an internet protocol address or the time of a communication.[39] The agency acknowledges: "some metadata associated with Canadian communications is likely to be present in the subsets of metadata collected by CSE."[40] CSE collects such information without ministerial or judicial authorization.[41] This practice raises significant concerns regarding the legality of CSE's intelligence gathering activities in cyberspace.

IV. THE CSE MANDATE AND THE *CHARTER*

A. *Charter* Concerns arising out of the CSE Mandate

Academic commentators have warned that the scope of "national security" has expanded from the targeting of foreign states and agents to also include the targeting of ordinary citizens.[42] The primary legal concern that arises out of CSE's current cyber operations that this analysis will examine is its potentially unconstitutional impact on privacy rights. In

---

36 *Ibid.*

37 *Ibid.*

38 *Ibid.*

39 "Metadata and our Mandate" (last modified 25 July 2019), online: *Canada Communications Security Establishment* <www.cse-cst.gc.ca/en/inside-interieur/metadata-metadonnees> [perma.cc/82LB-KLC8].

40 *Ibid.*

41 Forcese 2016, *supra* note 29 at 34.

42 Austin, *supra* note 13 at 2.

Canada, there is no explicit constitutional right to privacy.[43] However as this paper will explain below, it is widely recognized that section 8 of the *Charter,* which provides a right against unreasonable search and seizure, can be utilized to protect individuals' privacy interests.[44] In addition to protections afforded under section 8, expert commentators posit that freedom of expression protections under section 2(b) of the *Charter* may also afford privacy protections.[45]

Section 8 of the *Charter* provides a right against unreasonable search or seizure, which shares a nexus to privacy protections.[46] The Supreme Court of Canada's (SCC) unanimous decision in *R v Spencer*, 2014 SCC 43 [*Spencer*] illustrates this point. In *Spencer*, the police identified the internet protocol address of a computer that had been used to access and store child pornography through an Internet file-sharing program.[47] This information, which led to Mr. Spencer's identification, arrest, and consequent conviction, was obtained from his Internet Service Provider without prior judicial authorization.[48] The question of whether Mr. Spencer's rights under section 8 of the *Charter* were engaged turned on whether he enjoyed a reasonable expectation of privacy in the information that his internet service provider disclosed to the police.[49] Cromwell J, writing for the Court, explained that "anonymity is…particularly important in the context of Internet usage…[and can be] claimed by an individual who wants to present ideas publicly but does not want to be identified as their author."[50] Legal expert David Tortell aptly observes that *Spencer*, a section 8 case, thus expanded constitutional protection for free speech without any reference to

---

43 "Your privacy rights" (last modified 29 July 2019), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/your-privacy-rights/> [perma.cc/76HY-6KF3] [OPC]; Cockfield, *supra* note 11 at 370.

44 OPC, *supra* note 43; "Rights and Freedoms in Canada", online: *Department of Justice Canada* <www.justice.gc.ca/eng/rp-pr/cp-pm/just/06.html> [perma.cc/ELP3-297A].

45 While some privacy advocates have also suggested that sections 7 and 15 of the *Charter* may raise privacy implications, these are narrow and less analytically persuasive. For example, see David M Tortell, "Surfing the Surveillance Wave: Online Privacy, Freedom of Expression and the Threat of National Security" (2017) 22:2 Rev Const Stud 211 at 219-220 [Tortell 2017]. The following analysis is restricted to privacy guarantees under sections 8 and 2(b) of the *Charter*.

46 *Charter*, *supra* note 1, s 8.

47 *R v Spencer*, 2014 SCC 43 at para 1 [*Spencer*].

48 *Ibid* at para 1.

49 *Ibid* at para 16.

50 *Ibid* at para 45.

section 2(b) of the *Charter*.[51] This represents a shift in the jurisprudence on the relationship between speech and privacy. Traditionally, privacy and expressive rights are conceptualized as existing in tension.[52] In the context of defamation, the expressive rights of one party are viewed as existing at odds with the reputational privacy interests of another party.[53] However *Spencer* suggests that privacy and expressive rights can be conceptualized as existing in a complementary relationship, wherein expressive rights are augmented by the protection of privacy.[54]

It is constitutionally dubious whether CSE's current widespread collection of metadata, which can result in the incidental interception of Canadian communications (as described in the preceding section), is compliant with the privacy requirements that section 8 of the *Charter* entails. It is generally acknowledged that section 8 requires authorities to obtain a warrant from an independent judicial officer to engage in practices that intrude upon individuals' reasonable expectations of privacy.[55] While metadata provide only the context of communications, they can reveal significant personal information, including a person's habits, beliefs and conduct, for which there exists a reasonable expectation of privacy.[56] The *Spencer* decision, which affirmed that a police request for subscriber information corresponding to anonymous Internet activity "engages a high level of informational privacy," supports this conclusion.[57] Consequently, current CSE practices that involve the collection of constitutionally protected data should be subject to an independent judicialized process to ensure constitutional compliance.[58]

---

51 David M Tortell, "Two Tales of Two Rights: *R v. Spencer* and the Bridging of Privacy and Free Speech" (2016) 36:2 NJCL 253 at 255-256 [Tortell 2016].

52 *Ibid* at 255.

53 *Ibid* at 255.

54 *Ibid* at 256.

55 Craig Forcese, "Putting the Law to Work for CSE" (December 2017) Brief to the Commons Standing Committee on Public Safety and National Security at 3, online (pdf): <www.ourcommons.ca/Content/Committee/421/SECU/Brief/BR9326418/br-external/ForceseCraig-e.pdf> [perma.cc/6GWQ-G94U] [Forcese 2017].

56 *Ibid*.

57 *Spencer*, *supra* note 47 at para 50; Forcese 2017, *supra* note 55 at 4.

58 Forcese 2017, *supra* note 55 at 4; This issue is at the core of a legal action that the British Columbia Civil Liberties Association launched against CSE in 2013. In 2016, lawyers for the Attorney General of Canada utilized a legal procedure to move this matter from open court to a closed proceeding due to its national security implications. For more

The right to freedom of expression provided under section 2(b) of the *Charter* may also extend privacy protections. Commentators argue that the rising use of surveillance technology, which has accompanied the growth of cyberspace, may encroach on freedom of expression.[59] Professor Arthur Cockfield, a former legal and policy consultant to the Department of Justice and the Office of the Privacy Commissioner, Tortell, and others persuasively argue that if people believe their activities may be monitored, they modify their behaviour, and in doing so edit or limit their expression.[60] The SCC jurisprudence on privacy and the *Charter* supports this conclusion. McLachlin CJ, writing for the majority in *R v Sharpe*, 2001 SCC 2 explained that "[p]rivacy may also enhance freedom of expression claims under [section] 2(b) of the *Charter*, for example in the case of hate literature…because the freedoms of conscience, thought and belief are particularly engaged in the private setting."[61] Likewise, the unanimous decision in *Spencer* exemplifies this link between privacy and freedom of expression in a cyber context. While that case proceeded on a claim under section 8 of the *Charter*, the Court explicitly linked the protection of speech (which is usually protected under *Charter* section 2(b) protections for freedom of expression) with privacy. Specifically, Cromwell J's reference to the particular importance of cyber anonymity in empowering individuals to present ideas publicly without being identified as their author illustrates a clear conceptual link in the Court's understanding of the relationship between privacy and freedom of expression.[62]

Finally, legal scholars invoke principles of statutory interpretation to read privacy protections into section 2(b). It is a widely accepted principle of interpretation that courts should interpret the sphere of protected expression under section 2(b) of the *Charter* in a broad and inclusive

---

information, see Michelle Zilio & Colin Freeze, "Ottawa accused of breaking intelligence agency transparency vow", *The Globe and Mail* (2 June 2016), online: <www.theglobeandmail.com/news/national/ottawa-accused-of-breaking-intelligence-agency-transparency-vow/article30256336/> [perma.cc/J45M-R8J6]; "Spying in Canada: Civil Liberties Watchdog Sues Surveillance Agency Over Illegal Spying On Canadians" Press Release, *British Columbia Civil Liberties Association*, online (pdf): <bccla.org/wp-content/uploads/2013/10/Final-Press-Release-Spying-10_21_131.pdf> [perma.cc/U4NW-RQWT].

59 Cockfield, *supra* note 11 at 394.

60 *Ibid*; Tortell 2016, *supra* note 51 at 215.

61 *R v Sharpe*, 2001 SCC 2 at para 26.

62 *Spencer*, *supra* note 47 at para 45; Tortell 2017, *supra* note 45 at 221.

manner.[63] Such a broadly interpreted sphere of protected expression should encompass the need to protect the privacy necessary to enable individuals' free expression. Second, legal scholars invoke the constitutional "living tree" doctrine, which requires that the constitution be interpreted progressively in a manner that accommodates modern realities.[64] Such scholars argue that the doctrine requires section 2(b) to be understood to provide constitutional protection that addresses the practical reality that individuals' privacy must enjoy protection to defend expressive rights in cyberspace.[65] Therefore, on the same basis as described with respect to section 8 of the *Charter* above, protections under section 2(b) provide another basis on which the constitutionality of CSE's current practices that incidentally gather Canadian information can be challenged.

B. Bill C-59 as a Response to *Charter* Concerns

Under the *NDA,* CSE's current home statute, CSE obtains "ministerial authorizations" where it conducts cyber operations that may incidentally collect Canadian private communications.[66] As discussed in Section 3.b above, this statutory regime raises profound accountability issues. Ministerial authorizations are broad in nature and lack independent judicial oversight. This process is subject to much less accountability than a traditional judicial warrant process, which requires law enforcement agencies to seek judicial approval for specific surveillance activities that are narrow in scope. In contrast to ministerial authorizations, judicial approval is constrained to specific targets, locations and methods of surveillance. The lack of similarly strict accountability requirements for CSE's current surveillance practices raises serious concern whether such practices are *Charter*-compliant. Moreover, inter-agency cooperation practices mean that CSE may share incidentally-collected information with other partner security agencies, such as CSIS.[67] Resultantly CSE may share information with police and intelligence agencies that such agencies could otherwise only lawfully collect under the authority of a warrant.[68] However, Professor Craig

---

63 *Irwin Toy Ltd v Quebec (Attorney General)*, 1989 1 SCR 927 at 969-970, 58 DLR (4th) 577.

64 *Reference re Same-Sex Marriage*, 2004 SCC 79 at para 22.

65 Tortell 2017, *supra* note 45 at 223.

66 *NDA, supra* note 27, s 273.65; Forcese 2017, *supra* note 55 at 2-3.

67 Forcese 2017, *supra* note 55 at 4.

68 *Ibid* at 5.

Forcese, an expert in national security law, warns that imposing a judicial warrant process is not necessarily an appropriate fix, given that CSE's collection activities differ significantly from surveillance conducted by police or CSIS:

> [While] the latter invade privacy under warrants that meet strict specificity standards...[CSE] does not target Canadians and persons in Canada under its foreign intelligence and cyber security mandates – and therefore never *intentionally* targets the privacy of any constitutionally-protected individual.[69]

An appropriate authorization regime must therefore account for the "foreseeable but incidental" nature of the collection of constitutionally protected information.[70] Thus stricter specificity requirements, like those in a judicial warrant process, cannot form the basis of an appropriate accountability mechanism for CSE's operations.[71] However, the fact that *Charter* interests are at stake suggests that an appropriate regime must find a way to provide adequate independent judicial-like oversight.

Bill C-59 is an omnibus national security bill which implements several changes that respond to these *Charter* concerns. Professor Forcese characterizes Bill C-59 as "unquestionably the biggest overhaul of national security law and the institutional setting in which it operates" since the creation of CSIS in 1984.[72] Two elements of the bill have major implications for CSE's cyber operations. First, Part 3 of the bill will enact a "Communications Security Establishment Act," which has significant implications for CSE's cybersecurity mandate that will be addressed in Section 5 of this paper.[73] The second major change under Part 2 of the bill addresses these *Charter* concerns arising out of a lack of independent oversight and accountability. Bill C-59 creates the office of the Intelligence Commissioner (IC) to remedy these concerns.[74]

The IC is, among else, responsible for reviewing the Minister's "Foreign Intelligence Authorizations" and "Cybersecurity Authorizations."[75] This statutory overhaul and new oversight mechanism is the Federal Government's attempt to create a *Charter*-defensible regime that ensures

---

69 *Ibid* at 6 [emphasis in original].

70 *Ibid.*

71 *Ibid.*

72 *Ibid.*

73 *Ibid*, Part 3, *Communications Security Establishment Act*.

74 Bill C-59, *supra* note 2, Part 2, *Intelligence Commissioner Act*.

75 *Ibid*, ss 13, 14.

that CSE's incidental collection of protected information is *Charter* compliant.[76] The IC regime represents an attempt to emulate the independent judicial oversight that *Charter* compliance entails, but also to ensure that the institution tasked with oversight has the institutional competence (knowledge and capacity) to make determinations in a complex national cybersecurity context. Bill C-59 stipulates a requirement that the IC must be a retired judge of a superior court.[77] This is intended to secure the independent judicial-like accountability that is required for constitutional compliance where *Charter* interests are at stake. The creation of the IC is also superior to assigning these oversight duties to a Federal Court judge because it creates an office with greater institutional expertise and field sensitivity to oversee complex technological aspects of CSE operations.[78] However, retired judges are not necessarily subject to the exact impartiality standards imposed on sitting judges.[79] Nonetheless, this regime of independent IC oversight represents a significant improvement over the current regime of ministerial authorization.

Furthermore, a revision of the bill (as passed by the House of Commons on June 19, 2018) responds to concerns raised in a December 2017 brief to the Commons Standing Committee on Public Safety and National Security. In an earlier draft of the bill, IC oversight was only triggered for activities in contravention of "an Act of Parliament."[80] Critics argued this trigger was under inclusive, and would thus not be triggered for *all* activities that may implicate constitutionally protected information.[81] In the bill's updated articulation, ministerial authorization (which prompts the vetting process by the IC) must be sought for any activities that contravene "any other Act of Parliament – or involve the acquisition…of information from the global information infrastructure that interferes with the reasonable expectation

---

76 Forcese 2017, *supra* note 55 at 7.

77 Bill C-59, *supra* note 2, cl 4.

78 Forcese 2017, *supra* note 55 at 7.

79 For example, retired Justice John Gomery (who headed the Commission of Inquiry into the Sponsorship Program and Advertising Activities) was held to a lower standard of impartiality in his role as Commissioner than the standard expected of sitting judges. See *Chrétien v Canada (Ex-Commissioner, Commission of Inquiry into the Sponsorship Program and Advertising Activities)*, 2009 FC 802 at paras 72-73.

80 Bill C-59, *supra* note 2, Part 2, *Intelligence Commissioner Act*, cl 23(1).

81 Forcese 2017, *supra* note 55 at 8.

of privacy of a Canadian or a person in Canada."[82] This modification arguably addresses outstanding *Charter* concerns because it lowers the trigger for independent judicial-like oversight to the same threshold for interests under section 8 of the *Charter*.[83]

V. International Legal Implications Under CSE's Expanded Mandate

While Bill C-59 marks a major improvement in terms of CSE's *Charter* compliance regarding privacy issues, it also raises new questions surrounding CSE's revised mandate. The bill expands CSE's active (i.e. offensive) cyber operations mandate with two changes that have significant international legal implications. First, the bill expands what is currently Mandate C to include the provision of "technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence."[84] In addition, the bill creates a new CSE mandate to engage in "active cyber operations…to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[85] Under the new statutory regime, the Minister will be required to authorize active cyber operations under section 30(1), which specifies the circumstances in which such action can be authorized.[86] The language of section 30(1) states that such offensive operations can be authorized "despite any other Act of Parliament or of any foreign state."[87] Leah West, an Anti-Terrorism Law Research Fellow and counsel for the Department of Justice's National Security Litigation and Advisory Group, notes that this language does not authorize CSE to violate Canada's international legal obligations (even though Parliament could use legislation to approve actions in contravention

---

82 Professor Forcese proposed this solution in Forcese 2017, *supra* note 55 at 9 [emphasis added].

83 There does not appear to be a principled reason to lower the threshold for interests under other sections of the *Charter*; Forcese 2017, *supra* note 55 at 9.

84 Bill C-59, *supra* note 2, cl 20.

85 *Ibid*, cl 19.

86 *Ibid*, cl 30(1).

87 *Ibid*.

of international law).[88] Had Parliament intended to authorize CSE to breach Canada's international legal obligations, they could have used broader language such as "notwithstanding any other law" or "without regard to any other law" which are phrases employed in the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23.[89] When combined with the principle of interpretation that legislation is presumed to conform with international law, the wording in section 30(1) suggests that Parliament intends for CSE to comply with Canada's international legal obligations in its active cyber operations.[90]

The question thus becomes whether a cyber-attack (i.e. an active cyber operation) by CSE is an act prohibited by international law. Article 2(4) of the *Charter of the United Nations* demands that "[a]ll Members…refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[91] This prohibition is widely recognized as a principle of customary international law.[92] Commentators have suggested that this may create an international legal prohibition on state-sponsored cyber-attacks, however the extent of the use of force required to engage this prohibition is debated.[93] What is clear is that a cyber operation that results in death, injury, physical damage, or destruction would constitute a use of force.[94] Whether a specific non-lethal cyber-attack qualifies as a use of force is not settled in international law. An extensive review of this issue by 19 international law experts suggests that an "effects-based" approach that considers eight factors: severity; immediacy; directness; invasiveness; measurability of effects; military character; state involvement; and presumptive legality should be taken.[95] While a full international legal analysis is beyond the scope of this paper, this contextual approach suggests that decision-makers authorizing CSE's active cyber operations must remain sensitive to potentially complex

---

88 Leah West, "Cyber Force: The International Legal Implications of the Communication Security Establishment's Expanded Mandate under Bill C-59" (2018) 16 CJLT 381 at 392.

89 *Ibid*; *Canadian Security Intelligence Service Act*, RSC 1985, c C-23.

90 West, *supra* note 88 at 393; *R v Hape*, 2007 SCC 26 at para 53.

91 *Charter of the United Nations,* 26 June 1945, Can TS 1945 No 7, art 2(4).

92 West, *supra* note 86 at 394.

93 Castel, *supra* note 4 at 96; West, *supra* note 86 at 398.

94 West, *supra* note 86 at 398.

95 *Ibid* at 399-402.

international legal implications that will likely result from CSE activities under its new offensive mandate. This will require that decision-makers seek expert advice on international law, particularly international humanitarian law, and that they pay special attention to potential international implications in overseeing CSE's cyber operations. Without due consideration by decision-makers at both strategic and operational levels, it is clear that CSE's expanded mandate under Bill C-59 could facilitate cyber operations that do not comply with Canada's international legal obligations and are not authorized by Parliament.

VI. Conclusion

Ultimately, cyberspace presents a unique security challenge that requires a tailored national security apparatus capable of responding to threats in a cyber context that complies with both constitutional and international legal requirements. Under Canada's national cybersecurity framework, CSE provides technical leadership on cybersecurity and intelligence operations. Operations under the current CSE mandate may incidentally capture Canadian information in a manner that is inconsistent with the *Charter*. Ministerial oversight alone does not provide the independent judicial-like accountability that the *Charter* requires. However, this paper has argued that reform under Bill C-59, which expands external oversight and accountability under the office of the IC, provides satisfactory constitutional compliance where *Charter* interests are at stake. This reform also ensures that oversight rests with a body, the IC, which has the technical expertise and field sensitivity to appropriately oversee the technologically complex aspects of CSE operations. Finally, planned expansions to CSE's mandate under Bill C-59 that provide the agency with an active cyber operations mandate could have significant international legal implications. This raises a concern that, without careful oversight from decision-makers with access to appropriate legal advice, such a mandate expansion could result in CSE conducting cyber operations that are unauthorized by Parliament and counter to Canada's international legal obligations.