Canadian Journal of Law and Technology

Volume 16 | Number 2 Article 6

1-1-2016

Cyber Force: The International Legal Implications of the Communication Security Establishment's Expanded Mandate under Bill C-59

Leah West
SJD Candidate, University of Toronto

CYBER FORCE: The International Legal Implications of the Communication Security Establishment's Expanded Mandate under Bill C-59

Leah West*

INTRODUCTION

Canada is about to join the ranks of Russia, China, Iran, and North Korea; countries with a declared policy and authorized program of state-sponsored cyber attacks.[1]

In the summer of 2017, the Liberal Government introduced Bill C-59 *An Act Respecting National Security Matters*.[2] The bill, if passed, represents the most significant overhaul to Canadian national security institutions since the establishment of the Canadian Security Intelligence Service (CSIS) as a separate organization from the Royal Canadian Mounted Police (RCMP) in 1984. One component of this sweeping reform is the introduction of *The Communications Security Establishment Act* (*CSE Act* or the *Act*). Through the passage of this Act, Canada's signals intelligence agency, the Communications Security Establishment (CSE or the Establishment) will, for the first time, be constituted under its own legislation. The *CSE Act* institutes greater oversight and review requirements for this super secret agency, while also dramatically expanding the Establishment's current tripartite mandate to include defensive cyber operations, active cyber operations, and the provision of technical and operational assistance to the Canadian Armed Forces (CAF).

It is these latter roles that raise a series of concerns from a public international law perspective, namely: the principle of non-intervention and the prohibition on the use of force under the *United Nation's Charter*, the role of civilians and compliance with the international humanitarian law (IHL) rules that govern the conduct of hostilities. What's more, the use of active operations and engagement in cyber warfare may invoke a response from targeted states in

---

* Leah West was previously counsel with the National Security Litigation and Advisory Group at the Department of Justice and is currently an SJD candidate at the University of Toronto. Her views are her own and do not reflect those of the Department of Justice.

1 Dean Beeby, "State-sponsored cyberattacks on Canada successful about once a week," *CBC News* (30 October 2017), online: < www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711 > ; Jim Garamore, "Cyber Tops List of Threats to U.S., Director of National Intelligence Says" (13 February 2018), online: U.S. Department of Defense < www.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/ > .

2 1st Sess, 42nd Parl, 2017 (first reading 20 June 2017) [C-59].

the form of countermeasures, attacks in self-defence, and the lawful targeting of the Establishment and its employees.

To date, the Government of Canada has failed to address the serious international relations implications and the possible repercussions that could result from the employment of CSE's new mandate. Instead, proponents of the Bill have spent their time in the House of Commons and Parliamentary committees assuring Canadians that their privacy rights will be protected and answering questions about the collection of "publicly available information."[3] This article, therefore, seeks to fill the void by identifying and analyzing the international legal implications surrounding state-sponsored cyber attacks.

The question of whether and how international law regarding the use of force and the law of armed conflict applies to cyber operations is the subject of comprehensive analysis by a group of 19 international law experts in *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*.[4] It has also been the subject of significant scholarship by the *Tallinn Manual*'s editor Michael Schmitt, as well as Marco Roscini, Heather Harrison Dinniss, and Johann-Christoph Woltag.

This article draws on the works of these authors to highlight how international legal principles ought to inform CSE and the Government of Canada's choice to engage in active cyber operations, both in times of peace and during armed conflict. It also wrestles with the uneasy application of international law in the cyber domain and how the choices made by CSE in the conduct of its operations may affect the fate of not just those under attack, but also the Canadian civilians doing the attacking. To be clear, the purpose of this article is not to opine on the wisdom of the Act or the expansion of CSE's mandate from a policy perspective. Instead, the intent is to suggest and map out the questions that should be asked and answered by CSE, their legal advisors, and the Minister of National Defence before leveraging these new powers.

This article breaks down into five parts. Part I will briefly outline the history of CSE and its role in national security and defence, as well as the new powers proposed in Bill C-59. This section will also define the terms cyber attack and cyber operations.

We must assess the lawfulness of an international cyber operation under two different legal regimes. For this reason, Part II will begin by exploring the international law governing the use of force (*jus ad bellum*). This section will set out guidelines for when a cyber operation might qualify as a use of force or rise

---

3 See especially House of Commons, *Standing Committee on Public Safety and National Security*, 42nd Parl, 1st Sess, No 97 (13 February 2018) (Shelly Bruce and Scott Millar) [SECU 97].

4 Michael Schmitt, ed, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017) [*Tallinn Manual*]. The Tallinn Manual is not law in the sense that it is not binding on any state. That said, it is persuasive and would almost certainly qualify "as teachings of the most highly qualified publicists of the various nations" under article 38.1(d) of the *Statute of the International Court of Justice*.

to the level of an armed attack, and when a state has the right to respond to a cyber attack in self-defence. It will also touch on the availability of countermeasures in response to a cyber use of force. Part III will move on to international humanitarian law (*jus in bello*) and examine the laws of armed conflict that govern participation in hostilities. It will address both the circumstance by which CSE employees would be classified as either combatants or civilians directly participating in hostilities, and the resulting implications. Part IV highlights the core legal principles that ought to guide CSE operations during an armed conflict, specifically: precaution, distinction, and proportionality, as well as the lawfulness of certain tactics. Finally, in Part V, this article will conclude by weaving these issues together into a set of legal considerations that should be addressed by CSE before commencing a cyber operation against or within a foreign state.

PART I: THE RISE OF THE CANADIAN CYBER WARRIOR

The History and Mandate of CSE

For most of its history, Canada's signals intelligence agency existed in the shadows. Formed during World War II as a military signals corps, the mission of the agency evolved in the post-war era, becoming the Communications Branch of the National Research Council in 1946.[5] In 1975, CSE was rebranded with its current name but remained an obscure and unknown entity with a mission of providing signals intelligence for the Government of Canada and protecting Canadian communications.[6] It was not until the passage of the *Anti-Terrorism Act* in the wake of the attacks on September 11, 2001 that Parliament clarified the powers of CSE through an amendment to the *National Defence Act* (*NDA*).[7] At that time, CSE was a civilian arm of the Department of National Defence. However, this changed in 2011 when, by way of an order in council, the Establishment became a stand-alone agency under the portfolio of the Minister of National Defence.[8]

Part 5.1 of the *NDA* sets out the current mandate of CSE. Section 273.64(1) of the *NDA* defines the three distinct responsibilities of the Establishment, colloquially referred to as the "a" "b," and "c" mandates:

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

---

5 Communications Security Establishment, "History" (24 April 2018), online: <www.cse-cst.gc.ca/en/history-histoire>.

6 *Ibid*.

7 *National Defense Act*, R.S.C. 1985, c. N-S [*NDA*], as amended by *Anti-terrorism Act*, S.C. 2001, c. 41.

8 SECU 97, *supra* note 3 at 17 (Scott Millar).

(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[9]

Until recently, the Establishment rarely discussed its work publicly. That started to change in 2013 following the release of documents stolen by Edward Snowden from the National Security Agency (NSA). Both CSE and the NSA are "five-eyes partners," which refers to the information sharing agreement between the signals intelligence agencies of the United States, Canada, the United Kingdom, Australia, and New Zealand. [10] The leaked documents revealed that CSE had gathered data from the wireless devices of thousands of innocent civilians at a major Canadian airport and used that data to track their movements days after they left the terminal.[11]

Subsequently, the British Columbia Civil Liberties Association filed a lawsuit against the Establishment. The suit alleges that the Ministerial authorization scheme (not provided for in the *NDA*) used to sanction the collection of foreign intelligence where the personal information of Canadians may be incidentally collected violates the right to privacy protected by s. 8 of the *Canadian Charter of Rights and Freedoms*.[12] While the decision in that case is still pending, public and political pressure to enhance CSE's oversight and improve transparency continues to mount.[13]

The evolution of communications technology and the associated security risks have also grown exponentially in the 17 years since the codification of CSE's mandate. Not surprisingly, CSE's role in national security, cyber defence, and intelligence gathering has grown with it, consequently doubling the size and significantly expanding the budget of the agency in recent years.[14] To tackle these

---

9 *NDA*, *supra* note 7, s. 273.64(1).

10 Scarlet Kim et al, "Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements" *Lawfare* (23 April 2018), online: Lawfare blog <lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing>; "CSEC commissioner calls for safeguards on Five Eyes data sharing," *Canadian Press* (14 July 2017), online: <www.cbc.ca/news/politics/csec-commissioner-calls-for-safeguards-on-five-eyes-data-sharing-1.2706911>.

11 Greg Weston, Glenn Greenwald & Ryan Gallagher, "CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents," *CBC News* (30 January 2014), online: <www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>;

12 "Backgrounder on Spying: Civil Liberties Watchdog Sues Surveillance Agency Over Illegal Spying On Canadians" (1 June 2016), online: <bccla.org/wp-content/uploads/2016/06/2016_06_02_Backgrounder-BCCLA-Sues-CSE-1.pdf>.

13 See generally "Trudeau calls for 'proper' CSE oversight," *CBC News* (28 January 2015), online: <www.cbc.ca/news/trudeau-calls-for-proper-cse-oversight-1.2935111>.

14 Colin Freeze, "How CSEC became an electronic spying giant," *The Globe and Mail* (25

threats, the 2018 Federal Budget promised CSE an additional $155 million over the next five years (on top of its nearly $600 million annual budget) to create a Canadian Centre for Cyber Security.[15]

Bill C-59: An Act Respecting National Security Matters

In November 2017, Minister of Public Safety, Ralph Goodale, introduced Bill C-59 with the aim of "enhancing accountability and transparency. . .and updating our national security laws to ensure that our agencies can keep pace with evolving threats."[16]

As noted above, the *CSE Act* as proposed in Bill C-59 expands the Establishment's mandate. Section 16 of the *Act* provides that "[t]he Establishment is the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance." The five aspects of this mandate include: "foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations and technical and operational assistance."[17] From an international law perspective, the proposed active cyber operations and the technical and operational assistance powers are cause for concern.

Elaborating on the scope of the Establishment's assistance mandate, section 21 of the *CSE Act* merely expands what is currently "mandate C" under the *NDA* to include the Canadian Armed Forces:

> [t]he technical and operational assistance aspect of the Establishment's mandate is to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence.[18]

Conversely, active cyber operations are an entirely new line of operations for CSE. Section 20 of the *CSE Act* states:

> the Establishment's mandate is to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of

---

March 2017), online: Globe and Mail < www.theglobeandmail.com/news/politics/how-csec-became-an-electronic-spying-giant/article15699694/ > .

15 Stuart Thomson, "Federal budget invests $500 million over five years to battle cybercrime," *The National Post* (27 February 2017), online: < nationalpost.com/news/politics/federal-budget-invests-500-million-over-five-years-to-battle-cyber-crime > ; Alex Boutilier, "Review agency for Canada's spies says it needs more funding" *The Toronto Star* (14 March 2017), online: < www.thestar.com/news/canada/2017/03/14/review-agency-for-canadas-spies-says-it-needs-more-funding.html > .

16 *House of Commons Debates*, 42nd Parl, 1st Sess, No 234 (20 November 2017) at 15289 (Hon Ralph Goodale).

17 C-59, *supra* note 2 at cl. 76, s. 16.

18 *Ibid* at s. 21.

> a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.[19]

Notably, when describing this new role, the Minister of National Defence, Harjit Sajjan testified that: "CSE's active and defensive cyber-operations would be carefully targeted, by law, to the activities of foreign individuals, states, organizations, or terrorist groups *that have implications for Canada's* international affairs, defence, and security."[20] This is not the limitation found in the *Act*. Even if the Minister's statement could be interpreted in a way to constrain the reach of this provision, a plain and ordinary reading of the proposed legislation would permit the use of active cyber operations to disrupt, influence, and interfere with the international affairs, defence, and security of a foreign state.

Under the *Act*, the Minister of National Defence must authorize all active cyber operations. Section 31(1), which defines the parameters for such an authorization, stipulates that they may issue despite "any other Act of Parliament or of any foreign state."[21] While Parliament can use legislation to authorize the violation of Canada's international legal obligations (even though doing so would not absolve Canada of state responsibility), this is not what s. 31(1) of the *CSE Act* does.[22] The language in this provision only authorizes violations of Canadian legislation or the legislation of a foreign state. The reference to foreign "acts" does not extend to cover violations of international customary law, international treaties, or bilateral treaties which Canada has signed and ratified. Had the drafters intended to relieve CSE of its international legal obligations they could have easily done so by using the phrase "notwithstanding any other law" or "without regard to any other law." These phrases are found in the *Canadian Security Intelligence Service Act*; the latter having been specifically added in 2015 to resolve questions of jurisdiction and the relevant provisions' international application.[23]

---

[19] *Ibid* at s. 20 (s. 2 of the *CSE Act* explains that the "global information infrastructure includes electromagnetic emissions, any equipment producing such emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, that equipment, those systems or those networks").

[20] House of Commons, *Standing Committee on Public Safety and National Security*, 42nd Parl, 1st Sess, No 101 (22 March 2018) at 1 (Hon Harjit Sajjan) [SECU 101] (my emphasis).

[21] C-59, *supra* note 2, cl. 76, s. 31(1).

[22] Craig Forcese, "Does CSE risk a Re X moment with the current drafting in C-59?" *National Security Law* (2 February 2018), online: <craigforcese.squarespace.com/national-security-law-blog/2018/2/2/does-cse-risk-a-re-x-moment-with-the-current-drafting-in-c-5.html>.

[23] R.S.C., 1985, c. C-23, s. 21 (this provision was amended through Bill C-44 *An Act to amend the Canadian Security Intelligence Service Act and other Acts,* 41st Parl, 2nd Sess, 2015, cl. 8 (as passed by the House of Commons 2 August 2005)); Parliament of Canada, "Legislative Summary of Bill C-44: An Act to amend the Canadian Security Intelligence

Therefore, as the Supreme Court of Canada instructed in *R. v. Hape,* we must presume that Parliament intends for CSE and the Minister to comply with Canada's international obligations when engaging in active cyber operations.[24] Unfortunately, as Part II of this article explains, the conduct of active cyber operations will rarely, if ever, fully comply with international law, as the mere access of a foreign server by CSE without the permission of the host state is, strictly speaking, a violation of that state's sovereignty.

Defining Cyber Operations

Although the *CSE Act* describes the purpose and scope of the Establishment's active and defensive cyber operations, it does not define the term "cyber operation." Thus, this article will apply the definitions set out by the International Group of Experts in the *Tallinn Manual*. First, the term "cyber" is used to connote a relationship with information technology, and 'cyber activity' refers to "any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure. Such activities include, but are not limited to cyber operations."[25] "Cyber operations" explicitly involve "the employment of cyber capabilities to achieve objectives in or through cyberspace."[26] Finally, "cyber attack" is defined in Rule 92 of the *Tallinn Manual* as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[27]

PART II: CYBER OPERATIONS AS A USE OF FORCE

Article 2(4) of the *United Nations Charter* is the core of modern international law's prohibition on the use of force in interstate relations. The article stipulates that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any

---

Service Act and other Acts," by Holly Porteous, Dominique Valiquet & Julie Béchard (Ottawa: Library of Parliament, 2014).

[24] *R. v. Hape*, 2007 SCC 26, 2007 CarswellOnt 3563, 2007 CarswellOnt 3564, [2007] 2 S.C.R. 292, [2007] S.C.J. No. 26 at para. 53: "*the legislature is presumed to act in compliance with Canada's obligations as a signatory of international treaties and as a member of the international community*. In deciding between possible interpretations, courts will avoid a construction that would place Canada in breach of those obligations. The second aspect is that the legislature is presumed to comply with the values and principles of customary and conventional international law. Those values and principles form part of the context in which statutes are enacted, and courts will therefore prefer a construction that reflects them. The presumption is rebuttable, however. Parliamentary sovereignty requires courts to give effect to a statute that demonstrates *an unequivocal legislative intent to default on an international obligation*."

[25] *Tallinn Manual*, *supra* note 4 at 564.

[26] *Ibid.*

[27] *Ibid* at 415.

state, or in any other manner inconsistent with the Purposes of the United Nations."[28]

The International Court of Justice (ICJ) recognizes this prohibition as a principle of customary international law,[29] and while it is widely regarded as a *jus cogens* norm,[30] debate persists as to the reach of article 2(4) and its customary law equivalent. A strict approach to the prohibition suggests that any use of force in the territory of another state without consent is inconsistent with that state's sovereign control over its affairs within its borders,[31] and is therefore "inconsistent with the Purposes of the United Nations."[32] A narrower view of the prohibition is sometimes advanced to justify humanitarian intervention which would otherwise qualify as a use of force so long as it does not impair the "territorial integrity or political independence of any state."[33] Regardless of the approach taken, if the coercion "visited by one state on another does not reach the threat or use of force, it is not governed by article 2(4) and, absent some other restraint in international law, is lawful."[34]

---

[28] *Charter of the United Nations*, 26 June 1945, Can TS 1945 No. 7.

[29] *Case concerning military and paramilitary activities in and against Nicaragua* (*Nicaragua v. United States of America*), [1986] ICJ Rep 14 at 99 [*Nicaragua Case*].

[30] A *jus cogens* norm "is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character" *Vienna Convention on the Law of Treaties*, 23 May 1969, 1155 UNTS 331 art. 53 (entered into force 27 January 1980). Alternatively, see James Green, "Questioning the Peremptory Status of the Prohibition of the Use of Force," (2011) 32 Mich J Intl L 215.

[31] UN General Assembly's influential *Declaration on Principles of International Law concerning Friendly Relations and Co-operation*, GA RCS 2625 (xxv), UNGAOR, 25th sess., Supp. No. 28, UN Doc. A/5217 (1970) 121 [*Friendly Relations Declaration*] denounces "armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law." This resolution is not a binding legal obligation. However, the *Friendly Relations Declaration* "elaborates the major principles of international law in the UN Charter, particularly on use of force, dispute settlement, nonintervention in domestic affairs, self-determination, duties of cooperation and observance of obligations, and 'sovereign equality.'" Oscar Schachter, "United Nations Law" (1994) 88 AJIL 1. This approach is also consistent with the ICJ's ruling in *Case concerning Armed Activities on the Territory of the Congo* (*Democratic Republic of the Congo v. Uganda*) [2005] ICJ Rep. 168 at 227. [*Case Concerning Armed Activities*].

[32] Tom Ruys, "The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force excluded from UN Charter Article 2(4)?" (2014) 108 AJIL 159 at 163.

[33] See discussion, e.g., in Celeste Poltak, "Humanitarian Intervention: A Contemporary Interpretation of the Charter of the United Nations" (2002) 60 UT Fac L Rev 1; Christine Gray, *International Law and the Use of Force* (Oxford University Press: Oxford, 2008) vol. 3 at 593. For more recent discussions of this theory in relation to US air strikes in Syria see, e.g., Anders Henriksen, "The Legality of Using Force to Deter Chemical Weapons," *Just Security* (17 April 2018), online: <www.justsecurity.org/55005/legality-international-law-force-deter-chemical-warfare/>.

Defining what is and is not a use of force is the subject of significant discourse amongst international law scholars. Disagreements arise regarding the degree of violence required before state conduct graduates from a lesser form of coercion to force. Establishing a threshold for the use of force in the cyber context is even less settled yet, there is little debate that the concept applies. The ICJ's advisory opinion in the *Legality of the Use by a State of Nuclear Weapons in Armed Conflicts* instructed that the prohibition on the threat or use of force applies regardless of the weapon employed.[35]

It is this author's opinion that the question of whether or not a proposed CSE action qualifies as a use of force is a crucial consideration for Canadian officials involved in authorizing and engaging in active cyber operations abroad. As will be discussed below, violating the prohibition on the use of force gives an offended state the right to respond with countermeasures or act pursuant to a plea of necessity. What's more, should the Establishment's use of force rise to the level of an armed attack it could trigger the offended state's inherent right of self-defence, thereby permitting a counter attack or preemptive strike against Canada.

Lesser Forms of Coercion

Some actions undertaken by states may impinge the sovereignty of other states but fall short of a use of force. Nonetheless, falling short of force does not make a cyber operation lawful. The Permanent Court of International Justice notoriously stated in the *SS Lotus* matter:

> . . .the first and foremost restriction imposed by international law upon a State is that — failing the existence of a permissive rule to the contrary — it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.[36]

The exercise of state power or "enforcement jurisdiction," and the customary international law principle of non-intervention are core elements of state sovereignty.[37] Without the consent of the host state, CSE actions to degrade,

---

[34] Craig Forcese & Leah West Sherriff, "Killing Citizens: Core Legal Dilemmas in the Targeted Killing Abroad of Canadian Foreign Fighters" (2017) 54 Can YB Intl Law 134 at 152.

[35] *Legality of the Use by a State of Nuclear Weapons in Armed Conflicts*, Advisory Opinion, [1996] ICJ Rep 226 at 244 [*Nuclear Weapons Case*].

[36] *SS Lotus case (France v. Turkey)* (1927) PCIJ (ser A) No 10 at 18, 19 [*SS Lotus*].

[37] *Nicaragua Case*, *supra* note 29 at 106. Enforcement jurisdiction, explains Professor Currie "concerns the power to take action . . . usually by way of executive or administrative action, and includes all measures of constraint aimed at securing compliance with such rules. It includes, for example, powers of arrest, the service of process, the conduct of investigations, the seizure of evidence, prosecution, and other

disrupt and influence the capabilities, intentions, or activities of individuals, organizations, and states in the territory of another state would be a violation of both principles. Should the Establishment's operations be aimed at the international affairs, defence, or security of another state, they would be absolutely unlawful because they violate that State's right to respect for its territorial integrity.[38] This is further supported in the *Nicaragua Case*, in which the ICJ concluded that, at a minimum, the principle of non-intervention

> . . . forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy.[39]

Certain offensive cyber operations would violate the principle of non-intervention but not qualify as a use of force.[40] Covert actions and psychological operations intended to undermine confidence in a foreign government, and Russia's influence activities apparently designed to impact the outcome of the 2016 United States Presidential Election are but a few examples. These types of operations may nonetheless be prohibited by s. 33(1) of the *CSE Act*, which forbids the Establishment from engaging in activities that willfully attempt to obstruct, pervert, or defeat the course of justice or democracy.[41]

Cyber-espionage or hacking, activities permitted under CSE's foreign intelligence or operational assistance mandate, are also a violation of state sovereignty. However, espionage is not *per se* prohibited under international law. Thus, if conducted purely to gather information, operations of this type are unlikely to qualify as a use of force.[42]

Classically, state actions designed to be economically coercive are also not considered a use of force. The drafters of the *UN Charter* explicitly considered and rejected a prohibition on economic coercion under article 2(4).[43] This

---

coercive judicial procedures." He further explains: "it is a starting presumption in international law that, within its borders, a state is sovereign and free to exercise plenary enforcement jurisdiction." John Currie, *Public International Law* (Toronto: Irwin Law, 2001) at 292-293.

38 Menno T Kamminga, "Extraterritoriality" in *Max Planck Encyclopedia of Public International Law*, online: < opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040?rskey = 74KqX2&result = 1&prd = EPIL > .

39 *Nicaragua Case*, *supra* note 29 at 61-62.

40 *Tallinn Manual*, *supra* note 4 at 351.

41 C-59, *supra* note 2.

42 *Tallinn Manual*, *supra* note 4 at 168.

43 Documents of the United Nations Conference on International Organization San Francisco, 1945; see also Oliver D—rr, "Use of Force, Prohibition of" in *Max Planck Encyclopedia of Public International Law* at para 12, online: < opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e427?prd = EPIL > .

proposition was again raised and refused in the proceedings leading to the UN General Assembly's *Declaration on Friendly Relations*,[44] and subsequently reinforced in the General Assembly's *Declaration on the Non-Use of Force*.[45] Despite this longstanding exception, some scholars suggest that economically coercive cyber operations against a state's banking and trading systems should be treated differently because the operations themselves violate the territorial integrity of the state rather than merely creating external pressures on a state's economy.[46] Others argue that cyber operations could serve as the functional equivalent of a blockade (traditionally considered an act of war because of the violence required to enforce it) by denying access to information and communications which are vital to a state's economy and national security.[47]

The debate surrounding the prospect of an economic use force reflects the possible serious yet, in all likelihood, brief impact cyber operations may have on a state's economy.[48] Despite the gravity of the harm that could result from economically-coercive cyber operations, this author shares Marco Roscini's view that a teleological interpretation of article 2(4) supports a narrower reading of this provision which limits its scope to violent or armed coercion.[49] As Roscini points out, "the overall purpose of the [UN] Charter is 'to save succeeding generations from the scourge of war' not to ban all forms of coercion."[50] The International Group of Experts also agreed on this point. Rule 69 of the *Tallinn Manual* posits that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of

---

[44] UN GAROR Special Commission on Friendly Relations, UNGAOR UN Doc A/AC.125/SR.110 to 114 (1970).

[45] Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, GA Res. 42/22, UNGAOR (1987).

[46] Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Cambridge: Intersentia, 2014) at 144; Todd A Morth, "Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the UN Charter" (1998) 30 Case W Res J Intl L 567 at 592-597; Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict" (2006) 47:1 Harvard Intl LJ 1 179 at 188.

[47] Alison Lawlor Russell, *Cyber Blockade* (Washington, DC: Georgetown University Press, 2014) at 19, 35; Jason Barkham, "Information Warfare and International Law on the Use of Force" (2001) 34 NYUJ Intl L & Pol 57 at 92.

[48] A denial of service attack is used to force systems to shut down. This impact is achievable in various ways including overloading a system with messages or infecting a system with malicious software. However, as Rabkin and Yoo point out, while system shutdown can be costly and inconvenient, systems crash all the time, and, in most cases, the victim is capable of restoring the network within a few hours or days. What's more, after resolving the problem the system would typically be hardened to defend against the same threat. Jeremy Rabkin & John Yoo, *Striking Power: How Cyber, Robots and Space Weapons Change the Rules for War* (New York: Encounter Books, 2017) at 167.

[49] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Cambridge: Cambridge University Press, 2014) at 45.

[50] *Ibid.*

force."[51] As the international community has never classified a non-cyber operation that merely seek to influence the economy of a state without causing physical damage to infrastructure as a use of force, there is no basis to conclude that a similar action taken in cyberspace would qualify.[52]

Use of Force

While the above examples provide some general guidelines of what is not a use of force, decision makers at CSE must nevertheless evaluate every potential use of cyber force individually and in the context in which it arises.[53] As a starting point, cyber operations that injure or kill persons or result in physical damage or destruction would undoubtedly constitute a use of force.[54]

We also know from the *Nicaragua Case* that armed actions without direct destructive effects may also qualify as a use of force.[55] In that case, the ICJ found that the arming and provision of military training to the Contras by the United States was a violation of article 2(4).[56] Even earlier, in the *Corfu Channel Case*, the ICJ dismissed the United Kingdom's argument that their minesweeping operations in Albanian Territorial waters were not a violation of article 2(4) because they did not seek to undermine Albania's territorial integrity or political independence.[57] The ICJ found that the sending of warships by the Untied Kingdom into the Corfu Channel against the express wishes of the territorial state amounted to a "policy of force" and that such abuse does not have a place in international law.[58]

If destruction or death is not required for an action to qualify as a use of force, then the question becomes: *when does a comparable cyber operation violate article 2(4)*?

---

51 *Tallinn Manual*, *supra* note 4 at 330.

52 Ian Brownlie, *International Law and the Use of Force* (Oxford University Press: Oxford, 1963) at 362; Georg Kerschischnig, *Cyberthreats and International Law*, (Eleven: The Hague, 2012) at 106.

53 Michael N Schmitt, "Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework" (1994) 37 Colum J Transnat'l L 885 at 914.

54 *Tallinn Manual*, *supra* note 4 at 333; Roscini, *supra* note 49 at 53.

55 *Nicaragua Case*, *supra* note 29 at 118-119.

56 *Ibid.* Additionally, the European Union's Independent International Fact-Finding Mission on the Conflict in Georgia recorded a view in a footnote that some military incidents could fall below this threshold, such as "the targeted killing of single individuals, forcible abductions of individual persons, or the interception of a single aircraft," *Report of the Independent International Fact-Finding Mission on the Conflict in Georgia* (2009), online: <www.legal-tools.org/uploads/tx_ltpdb/Independent_International_Fact-Finding_Mission_on_the_Conflict_in_Georgia_Volume_II_2.pdf>.

57 *Corfu Channel Case (Merits) (UK v. Albania)*, [1949] ICJ Rep. 4 at 13, 35 [*Corfu Channel*].

58 *Ibid.*

To answer the question of when a non-lethal cyber operation will qualify as a use of force the International Group of Experts, expanding on the earlier work of Michael Schmitt, proposes an effects-based analysis based on eight criteria.[59] Whether this approach will be adopted by the international community remains unsettled. State practice following major cyber operations has been inconsistent,[60] and outside the confines of traditional armed conflicts very few cyber operations have been conclusively attributable to a state, resulting in a muted international response.[61] At the very least it appears that the United States will adopt an effects-based approach, as evidenced by the often cited statement of Harold Koh, former legal advisor to the Secretary of State: "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force."[62]

Knowing the answer to the question above will be vital when weighing the possible consequences and international implications arising from a use of force by CSE. To accurately weigh those consequences, the eight criteria outlined below should be evaluated by the Minister of Foreign Affairs and Minister of National Defence before authorizing an active cyber operation by CSE. The more criteria an active CSE operation fulfils, the more likely the international community will assess it as a use of force."[63]

1. Severity

The first step is to assess the severity of the intended outcome of CSE's operation. This factor will be the most determinative when assessing whether an act by CSE violates article 2(4). Of the eight conditions set out in the *Tallinn Manual*, an act's severity is the only criteria "that alone suffices to qualify a cyber operation as a use of force."[64]

---

[59] *Tallinn Manual*, *supra* note 4 at 333. (Two competing analytical approaches include the target-based and instrument-based approach. Scholars like Roscini and Barkham favour the latter which compares cyber operations to conventional military weapons to determine whether they ought to be captured by the prohibition under article 2(4). They argue that looking only at effects and not means blurs the lines between armed force and other forms of coercion, and causes undue expansion of the prohibition. Rossini, *supra* note 50 at 49; Jason Barkham, "Information Warfare and International Law on the Use of Force" 34 NYUJ Intl L & Pol 1 57 at 86. The former approach defines cyber attacks based on the intent and objective of the action. See, e.g., Oona Hathaway et al, "The Law of Cyber Attack" 100 Cal L Rev 4 at 817.

[60] Woltag, *supra* note 46 at 147.

[61] Heather Harrison Dinnis, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012) at 54.

[62] Harold Koh, "International Law in Cyberspace" (2012) 54 Harv Intl LJ online at 4.

[63] Woltag, *supra* note 46 at 145.

[64] " Michael N Schmitt, "The Use of Cyber Force and International Law" in Marc Weller, ed, *The Oxford Handbook of the Use of Force in International Law* (Oxford: Oxford University Press, 2015) 1110 at 1114.

To date, the Stuxnet Attack on Iran's nuclear enrichment program at Natanz is the most sophisticated state-sponsored cyber operation explicitly designed to cause physical damage to critical infrastructure.[65] The Stuxnet worm was programmed to tamper with the frequencies of Iran's nuclear enrichment centrifuges to cause their malfunction and potential destruction.[66] While Iranian officials denied that the attack caused any interruptions to their nuclear program, a steady drop in Iran's uranium production appeared to coincide with the first trace of the worm in 2009.[67] A second example of a cyber use of force with severe consequences is the attack by the Central Intelligence Agency (CIA) against a Soviet pipeline in 1982. The American attack manipulated the pressure-control valves that regulated the pipeline, resulting in a massive explosion.[68]

In both instances, the operations were not attributed to the United States government until long after they took place.[69] Although Iran continues to deny the impact of Stuxnet on its nuclear program, in 2011 Iranian state officials declared the existence of an "electronic war" and stated that Iran was prepared to take pre-emptive measures against the centers who would and had launched attacks.[70]

Although s. 33(1)(a) of the *CSE Act* prohibits operations that cause death or bodily harm, nothing in the *Act* prohibits an active operation from causing physical damage or the destruction of property.[71] As such, when authorizing an active cyber operation, the Minister of National Defence must be cognizant of the projected destruction and the corresponding impact the operation will have on the target state's critical infrastructure and national interests.

2. *Immediacy*

> A critical difference between a use of force and other forms of coercive action is the immediacy of its impact.[72] For this reason, the Minister

---

65 Kerschischnig, *supra* note 52 at 69-70.

66 *Ibid*; William Broad & David Sanger, "Worm Was Perfect for Sabotaging Centrifuges," *The New York Times* (18 November 2010).

67 William Young, "Iran Denies Malware Connection to Nuclear Delay" *The New York Times* (5 October 2010).

68 Thomas Rid, *Cyber War Will Not Take Place* (Hurst & Co: London, 2013) at 41; Anatoly Medetsky, "KGB Veteran Denies CIA Caused '82 Blast," *The Moscow Times* (18 March 2004).

69 David E Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran" *The New York Times* (1 June 2012), online: <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>; David Hoffman, "Reagan Approved Plan to Sabotage Soviets," *Washington Post* (27 February 2004), online: <www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/?utm_term=.41dd4f614c7a>.

70 Dinniss *supra* note 61 at 57; David Danger "Iran to take pre-emptive action against cyber terrorism," *Mehr News* (26 February 2011), online: <en.mehrnews.com/news/44830/Iran-to-take-pre-emptive-action-against-cyber-terrorism-general>.

71 C-59, *supra* note 2, cl 76.

> ought to consider how quickly the effects of CSE's operation will manifest in the foreign jurisdiction.

Under the *CSE Act*, active cyber operations may "degrade, disrupt, influence, respond to or interfere" with a foreign state's defence and security capabilities.[73] If the consequences of CSE's actions arise quickly, the target state will have little opportunity to engage with Canadian officials to find a peaceful resolution to the dispute that motivated CSE's operation and forestall its adverse effects.[74] In such circumstances, the Establishment's action are more likely to be perceived as a use of force.

3. Directness

The Minister ought to consider how closely linked CSE's initial actions are to the resulting second and third order effects of the operation. "The greater the attenuation," notes the International Group of Experts, "the less likely States will be to declare the actor in violation of the prohibition on the use of force."[75]

A cyber operation by Israel on Syria's air defence system in 2007 is an example of a use of force with immediate but indirect consequences. The operation took the system offline without causing any physical damage to its infrastructure. However, while Syria's air defences were in the dark, Israel conducted an airstrike on an alleged nuclear facility near Deir-ez-Zor.; a clear use of force.[76] Should CSE support the actions of the Canadian forces or an allied partner in an operation where physical destruction is similarly proximate, CSE's actions may be perceived as a violation of article 2(4).

4. Invasiveness

The degree to which CSE's operations intrude inside the target State or its systems is also an essential consideration. While acts of cyber espionage are not in and of themselves a violation of article 2(4), covert cyber operations that penetrate state systems to gain access to nuclear codes, for example, are more likely to be perceived as a use of force.[77]

5. Measurability of Effects

Unlike conventional armed force, measuring the intended or actual effect of an operation in the cyber domain can be challenging. This is especially true if CSE cannot predict the spread of malware once released or if the corruption of software leads to unintended consequences. Nevertheless, the easier it is for states

---

[72] *Tallinn Manual*, *supra* note 4 at 334.

[73] C-59 *supra* note 2, cl. 76, s. 20.

[74] *Tallinn Manual*, *supra* note 4 at 334.

[75] *Ibid* at 334.

[76] Kerschischnig, *supra* note 65 at 72-73; Rid, *supra* note 68 at 42.

[77] *Tallinn Manual*, *supra* note 4 at 171.

to quantify or calculate the impact on an active cyber operation, the easier it will be for that state to assert CSE's actions amount to a use of force.[78]

6. Military Character

Any nexus between CSE's operation and military action by the Canadian Armed Forces will heighten the likelihood that the Establishment's conduct will be characterized as a use of force. Additionally, if the target of the operation is the armed forces of another state, the operation is also more likely be characterized as a use of force.[79]

7. State Involvement

The closer the relationship between a state and the cyber operation, the greater the chance the international community will characterize an action as a use of force.[80] The fact that the Minister of Foreign Affairs must request all active cyber operations before the Minister of National Defence must authorize them will serve as a clear demonstration that the Government of Canada directed CSE's actions. Thus, CSE's operations are more likely to be viewed as a violation of the prohibition on the use of force than if the actions were undertaken by a decentralized agency.[81]

8. Presumptive Legality

As noted above, that which is not expressly prohibited by international law is presumptively lawful.[82] Active cyber operations carried out by CSE to spread propaganda or influence, to collect intelligence, or to exert economic pressure are not *per se* illegal and are less likely to be considered a use of force.[83] Nonetheless, it will often be difficult for a target state to distinguish activities like cyber espionage from other offensive cyber operations.[84] In most cases, both require penetration of a system and the introduction of malware to carry out the operation.[85] Thus, the technical realities of cyber operations contribute to the risk that the international community will perceive operations conducted by CSE which are not otherwise unlawful as a use of force.[86]

---

78 *Ibid* at 335.

79 *Ibid*.

80 *Ibid* at 336.

81 C-59, *supra* note 2 cl. 76, s. 31.

82 *SS Lotus*, *supra* note 36 at 19.

83 *Tallinn Manual*, *supra* note 4 at 336.

84 *Ibid* at 172.

85 *Ibid*.

86 *Ibid* at 173.

Countermeasures

As noted above, an active cyber operation undertaken by CSE, will very likely violate state sovereignty regardless of whether the actions amount to a use of force. The UN *Declaration on Friendly Relations* is categorical on this point: "[n]o State or group of States has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other State."[87] This prohibition is not limited to armed or violent intervention; all "forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law."[88] Yet, article 20 of the *CSE Act* precisely contemplates interference with the capabilities, intentions, and activities of a foreign state. Consequently, any CSE operation directed within the territory of a state in accordance with this provision and without that state's consent will leave Canada susceptible to countermeasures.

The Draft Articles on State Responsibility stipulate that an injured state may take countermeasures to induce a state to comply with its international obligations, but only for so long as the state fails to abide by its obligations.[89] This means that an offended state may withhold performance of the obligations it owes to Canada.[90] This portion of the draft articles reflects customary international law.[91]

Importantly, the ICJ found in the *Gabcíkovo-Nagymaros Case* that countermeasures may only be directed at a state once the state has committed the wrongful act.[92] The offended state must also call on Canada to stop its cyber activities or make reparations for CSE's actions before taking countermeasures.[93] While they would have to be proportionate to the harm suffered, there is no requirement that the countermeasures leveraged against Canada suspend the performance of the same or even a closely related international legal obligation.[94]

---

87 *Friendly Relations Declaration*, *supra* note 31.

88 *Ibid.*

89 International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, GA Res 56183, UNGAOR, 56th Sess, sup No 10, UN Doc A/56/10 (2001):

> 1. An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act to induce that State to comply with its obligations under Part Two.
> 2. Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State.
> 3. Countermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question.)

90 *Ibid* at 311 (commentary to the draft articles).

91 Roscini, *supra* note 49 at 105.

92 *Case Concerning the Gabcíkovo-Nagymaros Project (Hungary v. Slovakia)*, [1997] ICJ Rep 7 at 55-56.

93 *Ibid* at 56.

Active Operations and the Inherent Right to Self-Defence

There are three recognized exceptions to the article 2(4) prohibition against the threat or use of force. First, the use of force by one state in the territory of another is permissible with the consent of the effected state.[95] Second, pursuant to Chapter VII of the United Nations *Charter,* the UN Security Council may authorize the use of force.[96] Third, and most importantly in the context of CSE's active cyber operations, is a state's inherent right to self-defence under article 51 the *UN Charter*. Article 51 stipulates that

> [n]othing in the present Charter shall impair the *inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security*. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

As the reference to "inherent right" suggests, the concept of self-defence is part of customary international law.[97] Both the authors of the *Tallinn Manual* and a UN group of experts agree that the use force in self-defence in response to a cyber operation would be compliant with international law if the cyber attack reached the level of an "armed attack," and if the response was both proportionate and necessary.[98]

Importantly, the term "use of force" is not synonymous with an "armed attack." All armed attacks will also be a use of force however, "not just any violation of article 2(4) necessarily gives entitlement to a right of self-defence. Minor uses of force, such as a border incident, entails its author's international responsibility. It does not, however, allow its victim to riposte by military action" absent a Security Council resolution.[99] Further to this statement, in the *Nicaragua* judgement the ICJ went on to distinguish between "the most grave

---

94 *Ibid*; *Draft Articles*, *supra* note 89 at 129.

95 Geoffrey S Corn et al, *The Law of Armed Conflict: An Operational Approach* (New York: Wolters Kluwer, 2012) at 17.

96 *Ibid* at 18 (the UN Security Council has never authorized a cyber attack under Chapter VII).

97 See *Nicaragua Case*, *supra* note 29. For a discussion of Article 51 and the persistence of a parallel customary source of the right to self-defence, see Leo Van den hole, "Anticipatory Self-Defence Under International Law" (2003) 19 Am U Intl L Rev 69.

98 *Nicaragua Case*, *supra* note 29 at 94. See also *Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, [2003] ICJ Rep 161 at 198 [*Oil Platforms Case*].

99 Olivier Corten, *The Law Against War* (Oxford: Hart Pub, 2010) at 403.

forms of the use of force (those constituting an armed attack) from other less grave forms."[100] The Court also highlighted the importance of the "scale and effects" of the clash when differentiating between an armed attack and a "mere frontier incident."[101] "Scale," writes Tom Ruys, "refers to the amount of armed force employed or its durations, while 'effect' refers to the damage caused."[102]

Like the challenge that arises when trying to identify whether a cyber operation qualifies as a use of force, there is uncertainty regarding when the threshold from a lesser use of force to an armed attack is crossed in the cyber domain. What is certain is that the use of weapons or "arms" by the aggressor is not a pre-condition to the right to self-defence — rather, the critical factor in the cyber domain is the scale and effects of the operation.[103] Therefore, to be considered an armed attack, a cyber operation must result in "considerable loss of life and extensive destruction of property."[104] These consequences must also be the foreseeable, if not intended, effects of the cyber operation.[105]

It is arguable whether any cyber operation has yet risen to the level of an armed attack. The International Group of Experts disagreed as to whether the Stuxnet attack crossed the threshold from what was clearly a use of force to an armed attack.[106] Other examples of cyber operations that would be serious enough to constitute an armed attack include: (1) an extensive power grid outage with significant secondary and tertiary effects; (2) an attack on waterworks or dams that results in significant flooding; (3) a denial of service on air traffic control systems, and; (4) an attack on a nuclear reactor leading to the release of radioactive materials into the environment.[107] While the latter examples would violate the *CSE Act*'s prohibition against active cyber operations that result in bodily harm or death, it is conceivable that example 1 and 2 could be carried out without contravening this provision.

There is also disagreement amongst scholars as to whether a series of cyber operations could cumulatively support a response in self-defence. This "pin-

---

[100] *Nicaragua Case*, *supra* note 29 at 101.

[101] *Ibid* at 103-104.

[102] Tom Ruys, *Armed Attack and Article 51 of the UN Charter* (Cambridge: Cambridge University Press, 2010) at 139.

[103] "A state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right to self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects": *Tallinn Manual*, *supra* note 4 at 339.

[104] See discussion in Karl Zemanek, "Armed Attack" in *Max Planck Encyclopedia of Public International Law* at paras 9-10, online: < opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241 >; *Tallinn Manual*, *supra* note 4 at 341; Dinniss, *supra* note 61 at 81. See also discussion in International Law Association, *Draft Report on Aggression and the Use of Force,* Johannesburg Conference (2016) at 4.

[105] *Tallinn Manual*, *supra* note 4 at 343.

[106] *Ibid* at 342.

[107] Yoram Dinstein, "Computer Network Attacks and Self-Defense" (2002) 76 Intl L Studies 99 at 105.

prick" approach has been adopted by some states to justify acts in self-defence for counter-terrorism purposes.[108] As an example, in 2015 the government of the United Kingdom asserted that "[t]he scale and effects of [Daesh's] campaign are judged to reach the level of an armed attack against the UK."[109] The basis for this conclusion was "six terrorist plots having being foiled in the UK in the preceding 12 months."[110] Based on this legal reasoning, the government justified the execution of a drone strike against a British citizen operating in Syria.[111]

The United Kingdom's self-defence justification raises the question of whether Canada could similarly leverage CSE's active cyber operations mandate in self-defence following a series of cyber operations by either state or non-state actors.

A cyber operation against Canada and attributable to a state that rises to the level of armed attack can be met with a use of force in self-defence if that response is both proportionate and necessary to stop further imminent attacks.[112] This interpretation of the law is consistent with Canada's "Cyber Security Strategy" which states that "the severity of the cyber attack determines that appropriate level of response and/or mitigation measures."[113] Additionally, the Minister of National Defence testified that "when it comes to active cyber-operations. . . we as a government have to take some type of action to protect Canadians."[114]

If a state attacks Canada, it is foreseeable that the Canadian Armed Forces would be called upon to defend Canadian interests with the assistance of CSE under its technical and operational assistance mandate, rather than relying on

---

[108] Gray, *supra* note 33 at 150; Kerschischnig, *supra* note 65 at 120; Dinstein, *supra* note 107 at 109.

[109] UK, Joint Committee on Human Rights, "The Government's policy on the use of drones for targeted killing," 2nd Report of Session 2015-16, HL Paper 141; HC 574 (2016) at 41, online: < www.publications.parliament.uk/pa/jt201516/jtselect/jtrights/574/574.pdf > [Joint Committee Report].

[110] *Ibid* at 44. The UK Parliament report relies on SC Res 2249, UNSCR, 2015 and its invocation of terrorist attacks by Daesh in many locations outside Syria and Iraq through 2015 to conclude that the armed attack threshold was met.

[111] For further details see *Letter dated 7 September 2015 from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council*, SC Res 688, UNSCOR, 2015. See also Joint Committee Report, *supra* note 109.

[112] "Necessity" means that the force used in self-defence must be necessary to respond to the armed attack. "Proportionality" means the use of force in self-defence must be no greater than is required to halt and repel the armed attack." "Addendum — Eighth report on State responsibility by Mr. Roberto Ago, Special Rapporteur — the internationally wrongful act of the State, source of international responsibility (part 1)" (1980) 2 Yearbook of the International Law Commission 14 at 69. For a discussion on imminence see, e.g., Forcese & Sherriff, *supra* note 34 at 164.

[113] Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Public Safety Canada, 2010) at 3.

[114] SECU 97, *supra* note 3 at 1.

CSE's active mandate. This author suggests this response is more likely for two reasons. First, Canada's response to a cyber attack would not necessarily be a reciprocal cyber-attack. There is no requirement for a "like for like" response in self-defence. Canada may respond to a cyber attack using conventional weapons so long as it is necessary to halt or repel additional attacks against Canada.

Second, under s. 35(4) of the *CSE Act*, an active cyber operation may not be authorized by the Minister of National Defence unless there are "reasonable grounds to believe . . . that the objective of the cyber operation could not reasonably be achieved by other means." What the word "reasonably" conveys in the context of this provision is unclear. Under both international and domestic human rights law, the concept of reasonableness is tied to the level of impact a state action will have on a protected right or the state's efforts to ensure protected rights; it is a question of balancing state versus individual interests.[115] Under international humanitarian law the question of reasonableness corresponds to the concept of proportionality and the amount of force or destruction leveraged against a target.[116] Neither of these conceptions of reasonableness are helpful when interpreting s. 35(4) of the *CSE Act*.

Under *jus ad bellum* however, the term "reasonable" is tied to an operation's likelihood of success and the idea that one should not wage war if there is no reasonable prospect of success.[117] If this is the principle the drafters intended to import into the phrase "could not be reasonably achieved by other means," the Minister of National Defence must be convinced that an active cyber operation is the most likely means of repelling an armed attack by a foreign state; a limit that could prove overly-constraining in the face of an impending attack.

It is perhaps more conceivable that CSE would employ its active mandate in self-defence against multiple operations by *non-state* actors that cumulatively rise

---

[115] Domestically see *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act*, *1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11, s. 8; *R. v. Collins*, 1987 CarswellBC 699, 1987 CarswellBC 94, [1987] 1 S.C.R. 265, [1987] S.C.J. No. 15 at para 23; *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.*, 1984 CarswellAlta 121, 1984 CarswellAlta 415, [1984] 2 S.C.R. 145 *sub nom. Hunter v. Southam Inc.*, [1984] S.C.J. No. 36 at 160-162. Internationally see, *Optional Protocol of the International Covenant of Economic, Social and Cultural Rights: resolution adopted by the General Assembly*, GA Res 63/117, UNGAOR, 2009, art. 8(4).

[116] Office of the Judge Advocate General, *Use of Force in CF Operations,* Joint Doctrine Manual B-GJ-005-501/FP-000 2001-06-01 (2001): "The Canadian government, military commanders and all members of the CF [Canadian Forces] are subject to national and international laws. Both national and international law requires that any use of force by the CF must be controlled and limited to the extent that is proportional or reasonable and necessary to achieve legitimate military objectives." The Canadian Manual defines "proportionality" as follows: "The use of no more force than is reasonable and necessary for the proposed military task so as to avoid incidental loss of life, injury, damage to property, or combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

[117] Frances Harbour, "A just soldier's dilemma: facing a war that does not meet *jus ad bellum* criteria" (2008) 21 Cambridge Rev of Intl Affairs 421 at 430.

to the level of an armed attack against Canada. Heather Harrison Dinnis finds support for such action in several past decisions of the ICJ which validate the pin-prick doctrine and endorse the concept of an armed attack through cumulative incidents.[118]

Dinniss points out, however, that attributing multiple low-level cyber attacks could be a significant hurdle to applying the pin-prick doctrine in the cyber domain.[119] This is because in the *Oil Platforms Case* the ICJ established that it is the responsibility of the state using force in self-defence to prove that is has been subjected to an armed attack.[120] The Court further articulated that the offended state "must also show that its actions were necessary and proportional to the armed attack made on it" and that they directed their action at a military target open to attack in the exercise of self-defence.[121]

If CSE is capable of establishing attribution to a non-state actor, a second hurdle is the fact that directing an active operation in self-defence against the perpetrator would require the use of force in the territory of another state. Article 51 does not expressly preclude violence by non-state actors triggering the right to self-defence.[122] Nonetheless, in the *Wall Opinion* the ICJ found that acts of violence directed against a state by non-state actors did not trigger article 51 or the right to self-defence.[123] Thus, without a foreign state's consent, or unless Canada establishes that either a state is unwilling or unable to suppress the cyber

---

[118] Dinniss, *supra* note 60 at 95 points to the following ICJ decisions to support this position: *Oil Platforms Case*, *supra* note 98 at 191-192; *Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria)*, [2002] ICJ Rep 275 at 323, and; *Case concerning Armed Activities*, *supra* note 31 at 222-223.

[119] *Ibid.*

[120] *Oil Platforms Case*, *supra* note 98 at 186-187.

[121] *Ibid.*

[122] SC Res 1368 UNSCOR, 2001; SC Res 1373, UNSCOR, 2001; S/RES/1373 (2001) (the UN Security Council invoked the right to self-defence in condemning the terrorist acts of 9/11; an attack whose scale and effect directed against the U.S. was so significant that the international community accepted a response in self-defence. The North Atlantic Treaty Organization (NATO) also declared that the 9/11 attacks satisfied the requirements of an "armed attack" under Article 5 of the North Atlantic Treaty, triggering a collective response from NATO, see Press Release, "Invocation of Article 5 Confirmed" (2 October 2001). See also Darren C Huskisson, "The Air Bridge Denial Program and The Shootdown of Civil Aircraft Under International Law" (2005) 56 AFL Rev 109 at 144 ("The concept of an armed attack was left deliberately open to the interpretation of Member States and UN Organs, and the wording is broad enough to include the acts of non-State actors as 'armed attacks.'"); Carsten Stahn, "'Nicaragua is dead, long live Nicaragua'—The Right to Self-defence under Art. 51" in Christian Walter eds, *Terrorism as a Challenge for National and International Law: Security Versus Liberty* (Berlin: Springer, 2003) at 830.

[123] At least when the non-state actor operates from within that state or from a territory occupied by that state: *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, [2004] ICJ Rep 136 at 194. See also Case Concerning *Armed Activities*, *supra* note 31 at 223 ("the Court has no need to respond to the contentions of the Parties as to whether and under what conditions contemporary

activities of a non-state actor within its territory or that that state is responsible for the conduct of the non-state actor, CSE's actions may be a violation of article 2(4).[124] For this reason, Canadian decision makers should be conscious of the risks of failing to respond to a cyber operation in self-defence and the potential consequences for violating the prohibition on the use of force before leveraging CSE's new powers.

PART III: IHL & PARTICIPATION IN HOSTILITIES

Defining Armed Conflict

In times of armed conflict international humanitarian law will apply. "Armed conflict" is not a precisely defined term, and the existence of an armed conflict does not require a declared war.[125] Typically, armed conflict requires the use of military force beyond a minimum threshold of intensity.[126] Where this threshold lies varies depending on the international or non-international character of the conflict.

According to the International Committee of the Red Cross (ICRC), the threshold of violence giving rise to an international armed conflict is low:

---

international law provides for a right of self-defence against large-scale attacks by irregular forces.")

[124] *Tallinn Manual*, *supra* note 4 at 347; see also Ashley S Deeks, "'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense" (2012) 52 Va J Intl L 483 at 487-88 ("The "unwilling or unable" test requires a victim state to ascertain whether the territorial state is willing and able to address the threat posed by the non-state group before using force in the territorial state's territory without consent. If the territorial state is willing and able, the victim state may not use force in the territorial state, and the territorial state is expected to take the appropriate steps against the non-state group. If the territorial state is unwilling or unable to take those steps, however, it is lawful for the victim state to use the level of force that is necessary (and proportional) to suppress the threat that the non-state group poses.")

[125] Christopher Greenwood, "Scope of the Application of Humanitarian Law" in Dieter Fleck, ed, *The Handbook of Law in Armed Conflicts* (Oxford: Oxford University Press, 1995) at 41. Common Article 2 of the Geneva Conventions states that the Conventions "shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."

[126] International Law Association, *Final Report on the Meaning of Armed Conflict in International Law*, The Hague Conference (2010) at 28, online: <www.ila-hq.org/download.cfm/docid/2176DC63-D268-4133-8989A664754F9F87> ("armed conflict is to be distinguished from "incidents"; "border clashes"; "internal disturbances and tensions such as riots, isolated and sporadic acts of violence"; "banditry, unorganised and short lived insurrections or terrorist activities" and "civil unrest, [and] single acts of terrorism." The distinction between these situations and armed conflict is achieved by reliance on the criteria of organization and intensity.") See also *Prosecutor v Tadic*, IT-94-1-T, Opinion and Judgment (7 May 1997) at para 562 (International Criminal Tribunal for the former Yugoslavia, Trial Chamber).

> "[a]ny difference arising between two States and leading to the intervention of armed forces is an armed conflict . . . even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place."[127]

Conversely, the requisite threshold of violence for non-international armed conflicts is more demanding. Both the International Criminal Tribunal for the former Yugoslavia and Rwanda affirmed this principle when instructing that acts of violence between states and non-state actors must be "protracted" for a situation of "armed conflict" to arise.[128]

For an "armed" conflict to exist, armed forces need not conduct the violence, nor is there any requirement that conventional weapons be employed. Thus, cyber operations that result in physical damage or loss of life and meet the thresholds described above will trigger an armed conflict and the application of IHL.[129] Additionally, there is no requirement that both sides of a conflict resort to force. The *Law of Armed Conflict Manual* of the Canadian Armed Forces defines an armed conflict as "a conflict between states in which at least one party has resorted to the use of armed force to achieve its aims."[130] Consequently, a cyber attack by one state against another will be sufficient to give rise to an armed conflict.

Under the proposed *CSE Act,* there are two means by which this civilian agency could become engaged in an armed conflict. The first (and most likely) is through the provision of technical and operational assistance to the Canadian Armed Forces. The second is through the use of the Establishment's active cyber mandate either by: (1) engaging in a cyber operation against a foreign state, organization, or terrorist group that amounts to an armed attack, or; (2) in support of an armed conflict, such as the current conflict against ISIS, that has both a military element in Iraq and Syria, as well as a foreign and domestic counter-terrorism component.

---

[127] International Committee of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd ed (Cambridge: Cambridge University Press, 2016), online: < ihl-databases.icrc.org/ihl/full/GCI-commentary > ("For international armed conflict, there is no requirement that the use of armed force between the Parties reach a certain level of intensity before it can be said that an armed conflict exists.")

[128] *Tadic*, *supra* note 126 at para 70; *The Prosecutor v Zejnil Delalic*, Judgment, IT-96-21-T (16 November 1998) at para 184 (International Criminal Tribunal for the former Yogoslavia, Trial Chamber) ("to distinguish from cases of civil unrest or terrorist activities, the emphasis is on the protracted extent of the armed violence and the extent of organisation of the parties involved."); *The Prosecutor v. Jean Paul Akayesu*, ICTR-96-4-T, Judgment (2 September 1998) at para 619 (International Criminal Tribunal for Rwanda, Trial Chamber).

[129] *Tallinn Manual*, *supra* note 4 at 384.

[130] Canada, Office of the Judge Advocate General, *Law of Armed Conflict Manual: At the Operational and Tactical Levels,* B-GJ-005-104/FP-02 (Ottawa: Department of National Defence, 2001) at GL-2 [*CAF LOAC Manual*].

As noted at the outset of this article, the aim of this section is not to definitively determine the legality of CSE's participation in an armed conflict or to consider the policy implications of particular actions. Instead, this part attempts to identify the primary IHL issues arising from Bill C-59 and map out the central legal questions that must be asked, as well as the facts that must be ascertained, before the Establishment leverages their new mandate to engage in cyber warfare.

Participation in Hostilities

The law of armed conflict does not prohibit any category of individual from participating in hostilities.[131] This principle is no less true for cyber operations.[132] The question, therefore, is not whether CSE can participate in hostilities, but what status CSE employees would have under the laws of armed conflict.

When acting in support of the military, s. 26(1) of the *CSE Act* provides that Establishment employees shall be clothed in the same authorities and limitations "imposed by law" on the Canadian Forces.[133] Furthermore, under s. 26(2), persons authorized to provide assistance to the military on the Establishment's behalf "benefit from the same exemptions, protections and immunities as would persons authorized to act on behalf of the federal law enforcement or security agency, the Canadian Forces or the Department of National Defence, as the case may be, *if those persons were carrying out the activity*."[134]

As there are no qualifications on the phrase "imposed by law," one interpretation of this subsection would be that any constraints, limitations, and authorities granted to the Canadian Armed Forces while engaged in an armed conflict by international humanitarian law would apply equally to members of the Establishment as if they were themselves members of the armed forces and therefore privileged combatants under article 4 of the third *Geneva Convention*. Testifying before the Parliamentary Standing Committee on Public Safety and National Security, the comments of Harjit Sajjan, Minister of National Defence, could support this position:

> [w]e, in Canada, are leveraging a repository of phenomenal excellence that resides in CSE. . . The Canadian Armed Forces, with the new legislation, will be able to allow us to leverage that technology. Any type of military action that's taken, as with any other military operation, will be conducted with the proper targeting procedures, the proper rules of engagement, and in accordance with international law and, more importantly, our laws as well.[135]

---

[131] *Tallinn Manual*, *supra* note 4 at 401.

[132] *Ibid*.

[133] C-59, *supra* note 2, cl. 76, s. 26(1).

[134] *Ibid*, s. 26(2).

[135] SECU 101, *supra* note 20 at 5.

This statement is significant. Under article 43(2) of *Additional Protocol 1 to the Geneva Conventions of 12 August 1949*, all members of armed forces that are a party to conflict (except medical and religious personnel) are combatants.[136] What's more, the *Canadian Forces LOAC Manua*l restates article 43(3) of *AP 1*: "if a party to a conflict incorporates paramilitary or armed law enforcement agencies into its armed forces, it must inform other parties to the conflict of this fact. These forces are then considered lawful combatants."[137]

While not wholly analogous to a paramilitary or law enforcement agency, comments made by Minister Sajjan before the same House of Commons committee suggest that CSE, through its assistance mandate, will be incorporated into CAF operations:

> to enable CSE to better support Canada's military missions and the brave women and men of the Canadian Armed Forces serving in theatre. . .This legislation would allow CSE to do more to help them to, among other things, conduct active cyber-operations in support of government-authorized military missions. Bill C-59 will enable CSE and the Canadian Armed Forces to better co-operate to ensure the best use of tools and capabilities to meet mission objectives.[138]

Read together, the legislation and the Minister's comments could support the proposition that CSE employees will, under the law, be considered members of the Canadian Armed Forces when carrying out their assistance mandate. The consequence of this interpretation is that civilian employees of the Establishment, working from their offices in Ottawa and providing assistance to CAF members engaged in armed conflicts overseas may be categorized as combatants under IHL. As combatants, CSE employees could not only lawfully support the conduct of lethal operations and benefit from prisoner of war status, they could also be legally targeted. Importantly, for belligerents to benefit from combatants' immunity, and therefore be protected from prosecution under criminal law for having taken part in hostilities, they are required to conduct their operation in accordance with the laws of armed conflict.[139]

This interpretation raises another tricky question. If CSE employees are to be considered and conduct themselves as combatants under IHL, how might they comply with the rules of distinction when carrying out their operations in cyberspace?

---

[136] International Committee of the Red Cross, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, 1125 UNTS 3 [*AP I*] (recognized as customary international law: ICRC, "IHL Database," online: < ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule3 >).

[137] *CAF LOAC Manual*, *supra* note 130 at 3-3.

[138] SECU 101, *supra* note 20 at 1.

[139] Corn, *supra* note 96 at 138; Robert Kolb & Richard Hyde, *An Introduction to the International Law of Armed Conflicts* (Oxford: Hart, 2008) at 203.

The principle of distinction is "intransgressible,"[140] it demands that parties to a conflict only target other parties and not civilians or civilian objects.[141] In furtherance of this principle and the protection of civilians, article 44 of *AP I* stipulates that combatants must "distinguish themselves from the civilian population while they are engaged in an attack or in a military operations preparatory to an attack."[142] This article further recognizes that there are situations in armed conflicts where, owing to the nature of the hostilities an armed combatant cannot so distinguish himself, he shall retain his status as a combatant, provided that, in such situations, he carries his arms openly: (a) during each military engagement, and (b) during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate.[143]

Like the men and women remotely flying drones far away from the battle space in which they operate, distinguishing oneself by donning a uniform makes little sense for cyber warriors.[144] The concept of barring arms openly also has no natural equivalent in the cyber domain. What's more, the effectiveness of cyber operations is often dependent on obscuring its origin. Suggesting that cyber operators identify themselves and their "weapons" openly to comply with the principle of distinction is not just unlikely, it is unrealistic.[145]

Yet, under IHL, failure to abide by the principle of distinction forfeits a combatant's prisoner of war status.[146] While this may be of little concern for Establishment employees working from CSE headquarters in Ottawa, decision makers should consider this fact before deploying employees to conflict zones with the Canadian Armed Forces.

An alternative and more likely interpretation of the *CSE Act* is that through the provision of assistance to CAF, Establishment employees will be civilians directly participating in hostilities. Article 51(3) of *AP I* provides that civilians shall enjoy general protection against dangers arising from military operations "unless and for such time as they take a direct part in hostilities."[147] This principle applies equally to civilian participation in non-international armed conflicts.[148] Accordingly, CSE employees assisting the CAF during an armed

---

[140] *Nuclear Weapons Case supra* note 35 at 257.

[141] *AP I*, *supra* note 136, art 48.

[142] *Ibid*, art 44(3).

[143] *Ibid*.

[144] Kerschischnig, *supra* note 65 at 200.

[145] See, e.g., Woltag, *supra* note 46 at 217.

[146] *AP 1*, *supra* note 136, art 44(4).

[147] *Ibid*, art 51.

[148] International Committee of the Red Cross, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*, 8 June 1977, 1125 UNTS 609, art 13(3) [*AP II*].

conflict would lose the protections afforded civilians, may be lawfully targeted, and would not benefit from combatant immunity.[149]

To qualify as a civilian directly participating in hostilities or "DPH", the conduct of a CSE employee would be assessed against three criteria: threshold of harm, direct causation, and belligerent nexus.[150] These constitutive and cumulative elements are outlined in the ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*.[151]

First, the ICRC suggests that a threshold of harm must be met. This criterion requires that a civilian's action adversely affect the military operations or capacity of a party to the conflict, or inflict death, injury, or destruction on persons or objects protected against direct attack.[152] While non-binding, the *Interpretive Guidance* persuasively and authoritatively provides that interference with military computer networks, as well as wiretapping an adversary's command network, or transmitting tactical targeting information for an attack would meet the threshold of harm.[153]

Second, there must be direct causation, meaning a direct link between the civilian's actions and the resulting harm. In the context of a coordinated military/civilian operation, the civilian's actions must be an integral part of the operation.[154]

Some scholars, like David Turns, argue that this element makes it challenging to apply the concept of DPH to cyber operations, because the significant harm arising from a cyber attack is only likely to arise after several causal steps.[155] It is this author's opinion that this is an overly narrow view of causality.

Although the ICRC guidelines and the *Tallinn Manual*'s commentary on direct causation fails to address intent,[156] cyber operations designed specifically to deny or interfere with a military capability should not fall outside the scope of DPH simply because a series of dominos must fall between the operator's final keystroke and the manifestation of the intended harm. This position is supported by the International Group of Experts who agree that "clearly . . . any actions

---

[149] Woltag, *supra* note 46 at 242.

[150] International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, May 2009 at 46, online: <www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf> [*Interpretive Guidance*].

[151] *Ibid* at 47.

[152] *Ibid* at 46.

[153] *Ibid* at 48.

[154] *Ibid*.

[155] David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities" (2012) 17 J Conf & Sec L 279 at 289.

[156] Christopher Toscana, "Pouring New Wine into Old Bottles: Understanding the Notion of Direct Participation in Hostilities Within the Cyber Domain" 64 Naval L Rev 86 at 95.

that make possible specific attacks, such as identifying vulnerabilities in a targeted system or designing malware in order to take advantage of particular vulnerabilities" qualifies as an act of direct participation.[157]

Third, the ICRC submits that there must be a belligerent nexus motivating the civilian's actions. In other words, the actions taken must be intended to support one party to a conflict to the detriment of another.[158] Actions undertaken for purely criminal or private gain do not forfeit a civilian's protection under IHL.

Based on these criteria, CSE employees who are either: (1) directly supporting the Canadian Armed Forces in an armed conflict; or (2) engaging in active cyber operations to advance Canadian or allied interests in an armed conflict to the detriment of other parties, may qualify as civilians DPH.

As previously described, civilians taking direct part in hostilities may be targeted while conducting cyber operations, during "measures preparatory to the execution of a specific act of direct participation in hostilities, as well as during the deployment to and the return from the location of its execution."[159] This period would include an employee's travel to and from CSE headquarters before and after the execution of an operation. Furthermore, where an operation takes place over an extended period, the duration of the employee's participation will extend for as long as a causal link to the effects of the operation exists.[160]

One final consideration regarding participation in hostilities is that under IHL, persons engaged in espionage may be attacked, and if captured while doing so will not benefit prisoner of war status.[161] While not the subject of this article, CSE's primary mandate is the collection of foreign intelligence, and the Minister of National Defence recently recognized the important role CSE plays in providing intelligence to the armed forces.[162] Moving forward, the risks to CSE employees engaging in espionage on behalf of the CAF should be considered by decision makers prior to any overseas deployment.

PART IV: IHL & CONDUCT OF HOSTILITIES

In an armed conflict, CSE employees supporting the Canadian Armed Forces or directly participating through their active mandate will be required to comply with the laws of armed conflict including the principles of distinction and

---

[157] *Tallinn Manual*, *supra* note 4 at 430.

[158] *Ibid.*

[159] *Interpretive Guidance*, *supra* note 149 at 65.

[160] *Tallinn Manual*, *supra* note 4 at 431 (controversially, the *ICRC Guidelines* limit the civilian's loss of protected status to "the duration of each specific act amounting to direct participation in hostilities": *supra* note 152 at 46. This interpretation can result in what is referred to as the "revolving door" between combatant and non-combatant status, see Forcese & Sherriff *supra* note 34 at 169.

[161] *AP I*, *supra* note 136, art 46(1),

[162] SECU 101, *supra* note 20 at 1.

proportionality. They will also be responsible for abiding by the general precautionary principle that obliges all parties to a conflict to, at all times, protect civilians to the maximum extent feasible.[163]

Distinction

The principle of distinction described above not only requires combatants to distinguish themselves from civilians, it demands that military operations (or, for our purposes, cyber operations) be directed at military objectives.[164] Indiscriminate attacks — meaning those that are not directed at a specific military objective or those that employ a method or means of combat that (1) cannot be directed at; or (2) whose effects cannot be limited to a military objective — are illegal under customary international law.[165] Article 52 of *AP I* defines military objectives as "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[166]

Once again, applying the principle of distinction in a meaningful way in the cyber domain is problematic, this time because of the "pervasive nature of interconnectedness among military and civilian systems and the reliance of the military on civilian infrastructure."[167] The mere use of an object by the military can be sufficient to make it a military objective provided its destruction offers a direct military advantage.[168] As a result, the reliance by the military on civilian and commercial networks, data, servers, and communications infrastructure makes these targets valid military objectives. Even a city power grid that supplies a military's networked command and control system would be open to attack.[169]

Proportionality

Affirming that a target is a valid military objective is not the sole criterion for establishing the lawfulness of an attack. If an attack is expected to cause a loss of life or damage property in excess of the direct military advantage gained, it is by definition "indiscriminate" and will be unlawful.[170] This rule, known as the

---

[163] *AP I*, *supra* note 136 art 47; *CAF LOAC Manual*, *supra* note 130 at 4-5.

[164] *AP I*, *supra* note 136, art 48

[165] *Ibid*, art 51(4).

[166] *Ibid*, art 52(2).

[167] Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution" (2017) 26 Minn J Intl L 419 at 424 (this article provides an outstanding account of how to distinguish between civilian and military objectives).

[168] Roscini, *supra* note 49 at 185.

[169] For a more detailed discussion on the issue of distinction in cyberspace see Pascuicci, *supra* note 166, and for the issue of whether data is a valid military objective see Kubo Macak, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law" (2015) 48 Israel LR 55.

principle of proportionality, "establishes a link between the concepts of military necessity and humanity."[171]

Once again, the interconnectedness of military and civilian systems in the cyber domain complicates this balancing test. For example, the malware employed in the Stuxnet attack infected the computers of tens of thousands of civilians.[172] Fortunately, the impact of that particular malware on civilian networks was benign. However, in future cases it may not always be possible to control or anticipate the spread and destructive effect that a virus designed to attack a dual-use platform might have on civilian infrastructure. Where a cyber operation's effect on civilians is uncertain carrying out the attack will be unlawful regardless of the military advantage gained.[173]

Importantly, not all effects of a cyber attack will run afoul of this principle. As in the Stuxnet attack, if the level of harm does not rise to the level of "collateral damage," it need not form part of the proportionality calculation.[174] Inconvenience, irritation, stress, and fear do not amount to "incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof."[175] Even still, "there must be a rational balance between the legitimate destructive effect and undesirable collateral effect" resulting from a cyber attack.[176]

In practice, this principle will require that CSE employees conducting or supporting armed attacks be capable of calculating the anticipated direct and indirect collateral damage of their actions, and weigh those effects against the expected military advantage. To facilitate this assessment, Sasha Romanosky and Zachery Goldman adapted the American military's conventional collateral damage estimation model for use in cyber operations.[177] Whenever IHL applies, this author suggests that all CSE employees consider the following five questions derived from the Romanosky and Goldman estimation model before engaging in cyber operations:

---

[170] *AP I*, *supra* note 136, art 51.

[171] *CAF LOAC Manual*, *supra* note 130 at 2-2.

[172] Jeremy Rabkin & John Yoo, *Striking Power: How Cyber, Robots, and Space Weapons Change the Rules of War* (New York: Encounter Books, 2017) at 173.

[173] *Tallinn Manual*, *supra* note 4 at 456.

[174] *Ibid* at 457.

[175] *AP I*, *supra* note 136, art 51(5)(b); *Tallinn Manual*, *supra* note 4 at 472.

[176] *CAF LOAC Manual*, *supra* note 130 at 2-3.

[177] Sasha Romanosky & Zachery Goldman, "Understanding Cyber Collateral Damage" (2017) 9 J Nat'l Sec L & Pol'y 233 at 249-253.

1. Can the target's online persona, physical network, or logical network be positively identified as a military target?

   If the answer is no, the operation will not comply with the principle of distinction. Where the status of a person or object is unknown, IHL instructs us to presume it is civilian.[178] If yes, move to question 2

2. Are civilian systems or data located on, connected to, or dependent on the same network, system, or platform as the target?

   If yes, then the anticipated impact of the operation on civilians must be ascertained before moving to question 3.

3. Can the operational goal be achieved and the anticipated collateral damage be reduced or contained[179] by exploiting a different vulnerability, adjusting the circumstance of attack, or launching a different operation?

   If yes, the precautionary principle requires the employment of the operation which is least destructive to civilian infrastructure.[180]

4. What is the collateral damage estimate of the new operational plan?

5. Given the new estimate, does the anticipated collateral damage outweigh the operation's objectives?

   If yes, the attack is disproportionate and may not be carried out.

An assessment of proportionality is always prospective and "all apparently reliable information that is reasonably available must be considered."[181] That said, absolute certainty of the outcome or the impact of a cyber operation is not necessary. Ultimately, the reasonableness of CSE's operational decision making will depend on "whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties [or destruction] to result from the attack."[182]

Unlawful Tactics

To reinforce the principle of distinction, specific military tactics are prohibited at international law. For instance, it is prohibited to improperly use protective indicators such as the red cross and the red crescent, and to improperly

---

[178] *AP I*, *supra* note 136 arts 45(1), 52(3).

[179] While containment is not part of the estimation model proposed by Romanosky and Goldman, the containment inquiry is necessary to ensure those assessing the effects of a cyber operation turn their mind to the spread of malware, etc.

[180] *AP* I, *supra* note 136, art 57(2)(a)(ii).

[181] *Tallinn Manual*, *supra* note 4 at 475.

[182] *Prosecutor v. Stanislav Galic,* IT-98-29-T, Judgment (5 December 2003) at para 58 (International Criminal Tribunal for the former Yugoslavia, Trial Chamber).

use neutral party or enemy indicators such as military flags, insignia, and uniforms.[183] Perfidy is also prohibited if it results in a person's capture, injury, or death, though ruses are permitted.[184]

With respect to perfidy, article 37(1) of *AP I* stipulates that "[i]t is prohibited to kill, injure or capture adversaries by resort to perfidy. Acts inviting the confidence of adversaries and leading them to believe that they are entitled to protection or are obliged to grant protection under the LOAC, with intent to betray that confidence, constitute perfidy."[185] The feigning of civilian or non-combatant status is a listed example of perfidy.[186]

As noted, ruses are not prohibited. Ruses include acts "intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law."[187]

The *Tallinn Manual* expresses and applies these rules to the cyber domain using almost identical language.[188] The International Group of experts also notes that the person who is the target of the deception need not be the intended target of the attack that results in injury or death.[189] Nevertheless, the resulting injury or death "must be the proximate cause of the death or injury."[190] The term "proximate" is not intended to impose a temporal limit, rather, it requires that the links in the causal chain foreseeably lead to death or injury.[191]

These are crucial considerations for CSE. Cyber operations rely on deception to succeed.[192] As Heather Roff notes, "the very nature of a cyberweapon is deceitful, and deployment will more than likely rely on the use of a protected status."[193]

Certainly, many cyber attack vectors involve tricking a person, a software program, or a network into believing that a message, link, or IP address is or comes from a trusted source. In practice, it may be lawful to camouflage the

---

[183] *AP I*, *supra* note 136, arts 38, 39.

[184] *CAF LOAC Manual*, *supra* note 131 at 6-1 to 6-2.

[185] *AP I supra*, note 136, art 37(1).

[186] *Ibid*, art 37(1)(c).

[187] *Ibid*, art 37(2).

[188] *Tallinn Manual, supra* note 4, r 122-126.

[189] *Ibid* at 492.

[190] *Ibid*.

[191] *Ibid* at 493.

[192] Heather Roff, "Cyber Perfidy, Ruse, and Deception" in Fritz Allhoff et al, eds, *Binary Bullets: The Ethics of Cyberwarfare* (New York: Oxford University Press, 2015) 219; see, e.g., "William Boothby, Cyber Deception and Autonomous Attack — Is There a Legal Problem?" in K Podins, J Stinissen & M Maybaum, eds, *5th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE, 2013).

[193] *Ibid* at 213.

origin of an attack through the use of bots or IP spoofing. Influencing the enemy through the provision of false information or decoy websites would also be permissible.[194] However, spear phishing operations designed to make the recipient of an email containing an infected attachment or link believe that the communication comes from a trusted source like the UN, their own headquarters, or even a neutral state would violate IHL. That same operation designed to make the target believe that the communications comes from a trusted civilian non-combatant or the ICRC would be perfidious and prohibited under IHL if the result of that deception was a proximate cause of injury or death. As such, CSE must be aware and cautious to avoid using these prohibited tactics when planning active operations and assisting the CAF in operations during an armed conflict.

PART V: CONCLUSION

Canadian lawmakers and CSE decision-makers should not overlook the possible international legal implications that could result from the employment of CSE's expanded mandate proposed by Bill C-59.

First, any active cyber operation carried out by CSE during peace-time which is directed at persons or infrastructure within the sovereign territory of another state without consent would be an exercise of Canada's enforcement jurisdiction and violate the principle of non-intervention. Violating Canada's international legal obligations is not permitted under the *CSE Act*. As such, only in circumstances where an exception to article 2(4) applies could Canada legally call on CSE to act and exercise the state's enforcement jurisdiction abroad.

Second, before leveraging their new powers, the Establishment ought to assess whether their operation could foreseeably result in damage to property and whether that damage might rise to the level of a use of force. If so, the state in which that operation is carried out may legally respond with countermeasures against Canada. Should the damage brought about by CSE's actions rise to the level (or be perceived to rise to the level) of an armed attack, the targeted state may respond or even pre-emptively strike in self-defence. While international law requires that a response in self-defence be proportionate, the targeted state can use whatever type of force, be it cyber or kinetic, that it deems necessary to repel CSE's attack.

Third, if CSE exercises their new active mandate during an armed conflict, the civilian employees of the Establishment are likely to meet the test for direct participation in hostilities. So long as those employees provide direct support to the cyber operation (including preparatory activities) throughout the entire duration of the operation, those civilians could be lawfully targeted in Canada or abroad.

These implications would also attach to CSE employees providing technical and operational assistance to CAF during an armed conflict. What's more, given

---

[194] Roscini, *supra* note 49 at 216.

the language of the *CSE Act,* it is conceivable that CSE employees providing operational assistance to CAF and cloaked in their authorities and legal constraints would be characterized as combatants. As combatants, CSE and its employees could be targeted at any point during a conflict so long as any resulting collateral damage does not exceed the direct military advantage gained by the targeting state.

Finally, while operating under either the active or assistance mandate during an armed conflict, CSE must comply with international humanitarian law. CSE decision-makers must ensure that every course of action taken in support of hostilities abides by the principles of distinction, proportionality and precaution. Decision-makers must also be aware of the line between a permitted ruse and a prohibited perfidious act. By their very nature, cyber operations are deceitful. In selecting the attack vector and the means of deceit, CSE must avoid the use of protected and prohibited symbols and ensure that no one is killed, injured or captured as a result of perfidy. Failure to comply with the laws of armed conflict could result in the commission of war crimes by CSE.

Bill C-59 is not yet law. The *CSE Act* is still subject to amendment and time remains to have a meaningful conversation about the very real, and very serious, international legal implications of this proposed legislation. Canada should not make its decision to join in the ranks of Iran, Russia, and North Korea and engage in state-sponsored cyber attacks in a vacuum. The implications for our country's status within the international community and the safety of CSE's civilian employees are too important to make this choice blindly.