L'Institut CAD

Cahier Vimy

CDA Institute

Vimy Paper

Canada's Civilian Cyber Warriors and the International Legal Implications of a "Strong, Secured, and Engaged" Cyber Policy

BY LEAH WEST

FEBRUARY 2019

Conference of Defence Associations Institute

The Conference of Defence Associations Institute is a charitable and non-partisan organisation whose mandate is to provide research support to the CDA and promote informed public debate on security and defence issues and the vital role played by the Canadian Armed Forces.

Conference of Defence Associations Institute 75 Albert Street, suite 900 Ottawa, Ontario K1P 5E7 613 236 9903 www.cdainstitute.ca

Views expressed here are those of the authors and do not necessarily reflect those of the CDA Institute.

All logos and trademarks used are the property of their respective holders. Use in this publication is under non-commercial and normative fair use provisions of applicable Canadian law.

Institut de la Conférence des associations de la défense

L'Institut de la Conférence des associations de la défense est un organisme caritatif et non partisan dont le mandat est de fournir l'appui de recherches à la CAD, et de promouvoir le débat public sur les questions de sécurité et de défense, et le rôle essentiel des forces armées canadiennes.

Institut de la Conférence des associations de la défense 75 rue Albert, bureau 900 Ottawa (Ontario) K1P 5E7 613 236 9903 www.cdainstitute.ca

Les opinions exprimées sont celles des auteurs, et ne reflètent pas nécessairement les opinions de L'Institut de la CAD.

Tous les logos et les marques de commerce utilisés sont la propriété de leurs détenteurs respectifs.

L'utilisation qui en est faite dans cette publication l'est en vertu des dispositions de la loi canadienne applicable sur l'utilisation équitable non commerciale et nominative.

Canada's Civilian Cyber Warriors and the International Legal Implications of a "Strong, Secure, and Engaged" Cyber Policy

LEAH WEST

University of Toronto

Table of Contents

ABOUT THE AUTHOR

Leah West is an SJD Candidate at the University of Toronto Faculty of Law where she studies the application of National Security, International Humanitarian and Constitutional Law in cyberspace. Leah was formerly Counsel with the National Security Advisory and Litigation Group of the Department of Justice. Before attending law school, Leah served as an Armoured Officer in the Canadian Armed Forces. She is a graduate of the Royal Military College and holds advanced degrees in law and intelligence.

EXECUTIVE SUMMARY

The past two years have marked a turning point in Canada's cyber defence and security policy. In "Strong, Secure and Engaged," the Government of Canada called on the Canadian Armed Forces (CAF) to adopt a more assertive cyber posture. To implement this policy, the CAF will have to rely heavily on Canada's civilian signals intelligence agency, the Communications Security Establishment (CSE). Under the proposed Bill C-59: *An Act Respecting National Security Matters,* CSE's responsibilities will be expanded to include the provision of technical and operational assistance to CAF and the Department of National Defence, and a mandate to engage in defensive and active cyber operations. This paper assesses the international legal implications arising from CSE's expanded mandate and the risks of relying on civilians to engage in offensive operations in an armed conflict. Looking to our five eyes partners for guidance, the paper also makes a series of policy proposals to minimize the risks to Canadian security and international relations arising from those implications.

Introduction

Strong, Secure and Engaged, Canada's defence policy released in 2017, sets out a more assertive cyber posture and stipulates that Canada shall conduct "active cyber operations against potential adversaries in the context of government-authorized military missions."[1] At this time, the Canadian Armed Forces' (CAF) capacity in the cyber domain is modest at best.[2] Therefore, to pursue this policy objective, Canadian military leaders will have to rely heavily on a civilian organization: Canada's signals intelligence agency, the Communications Security Establishment (CSE or "the Establishment").

Reliance on CSE is, however, entirely dependent on the passage of *Bill C-59: An Act Respecting National Security Matters.* Should this Bill become law, it will give CSE the authority to both support the CAF and engage in active cyber operations to, "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[3] Importantly, *Strong, Secure and Engaged a*lso makes clear that all military "cyber operations will be subject to all applicable domestic and international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments."[4] These latter constraints, while common considerations for the CAF, are unfamiliar concepts for a civilian organization whose core mandate has always been the collection of foreign signals intelligence.

If and how the CAF chain of command will be involved in the planning and execution of CSE's active cyber operations is unknown. What is apparent is that civilians will be directly involved in the selection of targets and attack vectors, the assessment of collateral damage, and the execution of attacks in foreign states in unprecedented ways. This reality raises a host of novel legal and policy issues for both CSE and the CAF, not least of which is how these organizations will work together to ensure Canada complies with its international legal obligations when engaging in cyber operations.

Broken down into four parts, this paper identifies the core international legal considerations triggered by cyber operations and offers suggestions to help ensure CSE's active cyber operations comply with international law. Part I briefly outlines the mandate of CSE and its role in national security and defence, as well as the new powers proposed in Bill C-59. Part II then identifies three critical issues likely to arise through Canada's engagement in international cyber operations under both the international legal regime governing the use of force and international humanitarian law (IHL). First, unilateral action by CSE could result in a kinetic attack on Canada in self-defence or draw Canada into an armed conflict. Second, CSE's civilian employees who participate in hostilities may be at risk both legally and physically. Third, due to the nature of cyber operations, leveraging certain cyber capabilities in an armed conflict could violate the IHL principles of proportionality and distinction. For each issue, I describe the relevant law and the possible

implications for Canadian security and international relations and provide recommendations for minimizing the negative consequences that could result from a more aggressive cyber posture.

The Mandate of the Communications Security Establishment

CSE has a long history of working with the Canadian Armed Forces. In fact, the agency originated as the Canadian military signals corps during the Second World War before evolving in the postwar era into the National Research Council's secretive Communications Branch.[5] It was not until the passage of the *Anti-Terrorism Act 2001* that Parliament gave the agency a statutory footing and publicly clarified CSE's powers with an amendment to the *National Defence Act* (*NDA*).[7]

PHOTO CREDIT: Chris Mikula/Ottawa Citizen

The current mandate of CSE is set out in Part V.1 section 273. 64(1) of the *NDA*. The three elements, referred to as the "A," "B" and "C" mandates are (a) foreign signals collection; (b) electronic and information infrastructure defence; and (c) assistance to security and law enforcement agencies.[6]

In the years since the codification of CSE's tripartite mandate, communications technology and the associated security risks have evolved exponentially. Unsurprisingly, CSE's role in national security, cyber defence and intelligence gathering has grown with it; doubling the size and significantly expanding the budget of the agency in recent years.[7] In November 2017, Minister of Public Safety Ralph Goodale introduced Bill C-59 with the aim of "updating our national security laws to ensure that our agencies can keep pace with evolving threats."[8] The *Communications Security Establishment Act* (*CSE Act*), as proposed in Bill C-59, significantly expands the Establishment's mandate to include: "foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations

and technical and operational assistance." Importantly, section 20 of the *CSE Act* expands what is currently "mandate C" under the *NDA* to include the CAF:

> [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.[9]

Section 19 also creates an entirely new line of operations for CSE:

> 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 a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.[10]

Under the proposed act, the Minister of National Defence must authorize all active cyber operations, and subparagraph 30(1) stipulates that the minister may do so despite, "any other Act of Parliament or of any foreign state.[11] Without adopting some of the recommendations identified below, this provision may prove to be problematic.[12] While parliament may authorize the violation of Canada's international legal obligations (even though doing so would not absolve Canada of state responsibility), this is not what subparagraph 30(1) of the *CSE Act* does.[13] The language in this provision only authorizes violations of Canadian legislation or the legislation of a foreign state. It does not extend to violations of international customary law, international treaties, or bilateral treaties which Canada has signed and ratified. As such, we must presume that parliament intends for CSE and the minister to comply with Canada's international obligations when engaging in active cyber operations.

"How…attacks are categorized and qualified under international law could have significant implications for Canadian security and international relations."

The term, "cyber operation," is not defined in the *CSE Act*. For our purposes, we shall rely on the *Tallinn Manual*, the leading text on the application of international law in cyber operations. This document defines cyber operations as, "the employment of cyber capabilities to achieve objectives in or through cyberspace."[14] The *Tallinn Manual* also defines, "cyber attack," 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.[15] Therefore, applying the guidance of Tallinn's international experts, CSE will be authorized under

the act to conduct cyber attacks against other states. How those attacks are categorized and qualified under international law could have significant implications for Canadian security and international relations.

Issue 1: CSE and the Risk of Armed Conflict

The effects of cyber operations can vary across a spectrum from espionage and interference on one end, to violent physical destruction on the other. The following section outlines how the effects of a cyber attack impact its characterization under international law, highlights some of the resulting implications for Canadian defence and international relations and concludes with one straightforward policy recommendation.

Use of Force

Article 2(4) of the *United Nations Charter* is the core prohibition on the use of force in interstate relations. This 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 state, or in any other manner inconsistent with the Purposes of the United Nations."[16]

Defining what is a use of force is the subject of significant debate amongst international law scholars and establishing a threshold for the use of force in the cyber context is even less settled. However, the International Court of Justice'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.[17] In other words, some cyber operations may qualify as a use of force.

PHOTO CREDIT: Department of National Defence

Cyber operations that injure or kill persons or result in physical damage or destruction will undoubtedly constitute a use of force.[18] As Harold Koh, former legal advisor to the US Secretary of State, famously stated, "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."[19] In practice, this line is not that clear-cut. The International Court of Justice has made clear that armed actions without direct destructive effects may also qualify as a use of force. [20] As such, the question of whether a proposed CSE action qualifies as a use of force should be a crucial consideration for Canadian officials involved in authorizing and engaging in active cyber operations abroad.

State Sovereignty & Counter-Measures

Offensive cyber operations that fall short of a use of force may still unlawfully impinge the sovereignty of other states. The idea that, failing a permissive rule, a state may not exercise its power beyond its territory, and the principle of non-intervention are core elements of sovereignty.[21] Without the consent of the host state, actions taken under section 19 of the Act, in the territory of another state may violate both principles. Moreover, if the Establishment aims its operation at the international affairs, defence or security of another state it would "absolutely [be] unlawful because it violates that State's right to respect for its territorial integrity.[22]

"…any CSE operation directed within the territory of a state under this provision without that state's consent will leave Canada susceptible to countermeasures."

On this issue, the *UN Declaration on Friendly Relations* provides important guidance: "[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." [23] 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."[24] Despite this limit, article 19 of the *CSE Act* explicitly authorizes interference with the capabilities, intentions and activities of a foreign state. Consequently, any CSE operation directed within the territory of a state under this provision without that state's consent will leave Canada susceptible to countermeasures.

Countermeasures are actions that would otherwise violate international law but are permissible when used to induce another state to comply with its international obligations,[25] and this too must be carefully weighed by CSE before engaging a target. While countermeasures must be proportionate to the harm suffered, there is no requirement that a foreign state's response to CSE's action suspend the performance of the same or even a closely related international legal obligation.[26]

Armed Attack

Up the scale from a use of force is an armed attack. To qualify as an armed attack, a cyber operation must result in "considerable loss of life and extensive destruction of property,"[27] and these consequences must be the foreseeable, if not intended, effects of the operation.[28] Experts agree that if the threshold of an armed attack is met by a cyber operation, responding with force in self-defence under Article 51 of the *UN Charter* would comply with international law so long as it is both proportionate and necessary.[29]

Should a state carry out a cyber-attack against Canada, it is likely that the CAF will be called upon to defend Canadian interests with the assistance of CSE under its technical and operational assistance mandate. Nevertheless, it is conceivable that CSE could be called upon directly to employ its active mandate in self-defence against non-state actors whose actions, either through a cumulative series or a single attack, rise to the level of an armed attack against Canada.[30] In either scenario, if a cyber-attack or CSE's response moves to the level of an armed attack and into the sphere of armed conflict, international humanitarian law applies.

Armed Conflict

'Armed conflict' is not a precisely defined term, and the existence of an armed conflict does not require a declaration of war.[31] Typically, armed conflict arises through the use of military force beyond a minimum threshold of intensity.[32] Where this threshold lies varies depending on the international or non-international character of a conflict. In either case, there is no requirement for armed forces to perpetrate the violence, nor is there any requirement that conventional weapons be employed. Thus, cyber operations resulting in physical damage or loss of life and meeting the threshold will trigger an armed conflict and the application of IHL.[33]

Recommendation: Limit the permissible effect of CSE active cyber operations

The Government of Canada should delineate that any action undertaken under s. 19 of the *CSE Act* must fall below the threshold of a use of force.[34] Any CSE operation that crosses the threshold of a use of force should only be undertaken in support of the CAF as authorized by s. 20 of the *CSE Act*.

Implementing this simple policy measure will decrease the likelihood that the actions of a civilian state organization will give rise to an attack against Canada in self-defence. This policy would also reduce the chance of CSE's actions rising to the level of an armed attack, triggering an armed conflict with a foreign state or non-state actor, and the application of IHL. Even with the proposed limit in place, CSE's cyber

operations could still constitute a violation of Canada's international legal obligations, thereby resulting in the use of countermeasures. However, before taking countermeasures, the law requires that the offended state call on Canada to fulfill its obligations, give notice of their intent to take countermeasures, and offer to negotiate the matter with the Government of Canada;[35] a process which is far more likely to be resolved peacefully than the invocation of Article 51.

Issue 2: Civilians or Combatants?

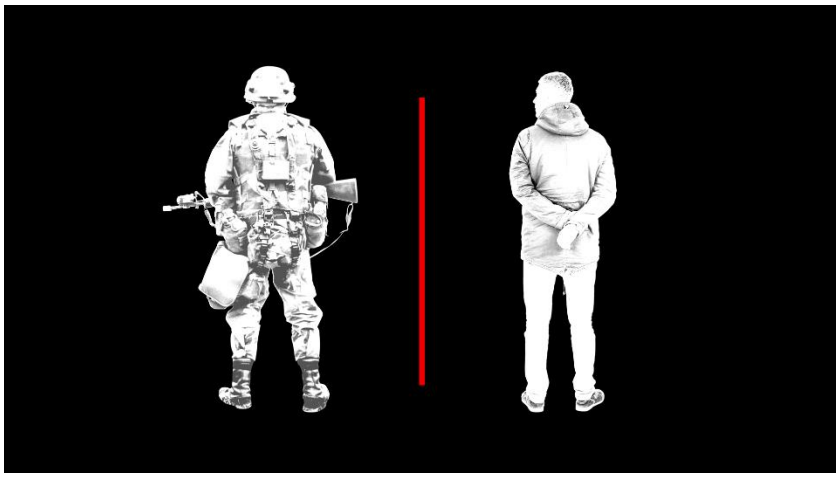


ILLUSTRATION CREDIT: Jim Cooke/GMG

IHL grants combatants and civilians differing protections and privileges. As such, a person's status under the law is an important consideration. As a starting point, civilians are generally considered non-combatants and may not legally engage in hostilities.[36]

When acting in support of the military in an armed conflict, unless Establishment employees take direction and fall directly under the CAF chain of command, they will be considered civilians directly participating in hostilities. Article 51(3) of *Additional Protocol I to the Geneva Conventions 1977*, stipulates 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."[37] This principle applies equally to civilian participation in non-international armed conflicts.[38]

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.[39] First, a civilian's action must 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.[40] Second, there must be 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.[41]Third, the actions taken by a civilian must be intended to support one party of a conflict to the detriment of another.[42]

Based on these criteria, CSE employees either directly supporting the CAF in an armed conflict or engaging in active cyber operations to advance Canadian or allied interests in an armed conflict to the detriment of other parties, will likely qualify as civilians DPH. As such, they 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."[43] 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.[44]

Furthermore, civilians DPH do not benefit from a combatant's immunity; meaning, they can be held criminally liable for any damage caused, or for killing or injuring enemy personnel and civilians during hostilities. [45] Lastly, if captured, CSE employees would not benefit from prisoner of war status which bestows a wide array of rights including humane treatment, protection from violence, adequate food, facilities and medical aid, and repatriation at the end of hostilities.[46]

Recommendation: Adopt the Australian Cyber Operations Model

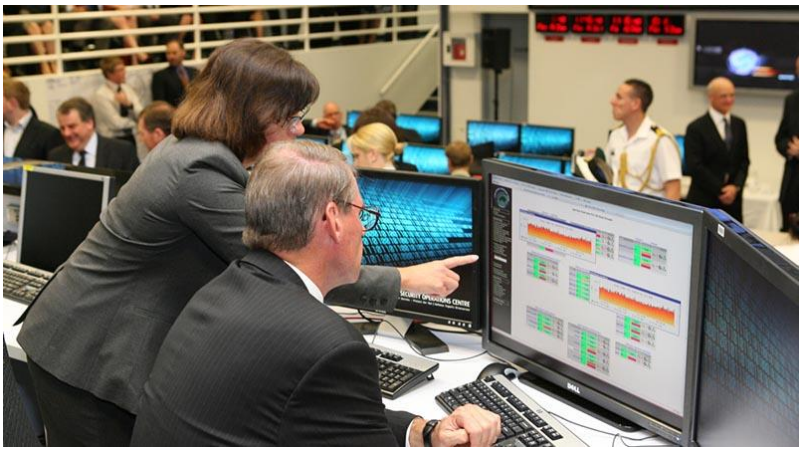
PHOTO CREDIT: Australian Strategic Policy Institute

To protect CSE employees and facilitate compliance with international law, CSE and CAF should establish a partnered organizational framework like the structure implemented by the Australian Signals Directorate (ASD) and the Australian Defence Force (ADF).

Australia is the advisable model for several reasons. First, along with CSE, and the signals intelligence agencies of the United Kingdom, the United States and New Zealand, the ASD is a member of the "Five-Eyes," widely regarded as the most important intelligence alliance in the world. For the past 70 years, these agencies have readily shared volumes of information, intelligence and knowledge of evolving threats and how to counter them.[47] Second, amongst the Five-Eyes partners, CSE and the ASD are most comparable in terms of size and budget.[48] Third, like CSE, Australia's offensive cyber capabilities reside solely within the ASD and - with the passage of Bill C-59 - the agencies will provide similar support to military operations.[49] Fourth, Canada and Australia's armed forces are also of a comparable size, and have a long history of cooperation, including most recently as partners in the International Security Assistance Force in Afghanistan.[50]

These close relationships stem in large part from the country's common values including a commitment to human rights and the rule of law.[51] Finally, despite the similarities, where Canada and Australia differ is in the robustness and maturity of the two state's national cyber policy. At the time of writing, Canada's parliament has yet to give CSE the authority to support and conduct cyber operations. Conversely, Prime Minister Malcolm Turnbull confirmed Australia's offensive cyber capabilities in 2016, and "Australia's International Cyber Engagement Strategy" published in October 2017, presents a clear picture of how the ASD and ADF work together to "deter and respond to unacceptable behaviour in cyberspace," and sets out Australia's interpretation of international law as it applies to state conduct in that domain.[52]

While the ASD has no explicit authority to engage in active cyber operations independently, like CSE, the provision of support to military operations is not restricted to assisting forces with intelligence collection or securing communications infrastructure. Instead, the Australian Defence Force's Joint Cyber Unit embeds staff within ASD, and they carry out offensive cyber operations jointly.



Senator John Faulkner, Australia's former Minister for Defence at the 2010 opening of a new Cyber Security Operations Centre in Canberra.

PHOTO CREDIT: Bryan Doherty

Specifically, cyber operations are planned and executed by ASD and the ADF's Joint Operations Command under the direction of military leadership.[53] The targeting process carried out for cyber operations is conducted in the same manner as traditional kinetic operations -by what one might call a "cyber fires" team- and is governed by the military's rules of engagement. The personnel who carry out the attacks are most often civilians from ASD; however, those civilians are provided guidance on and expected to plan their operations according to the law of armed conflict.[54] The Minster of Defence approves all operations, which are subject to additional independent oversight by the Inspector-General of Intelligence and Security.[55]

It is apparent that in arranging this partnership, the Australians recognized that operational planning, a formalized process that demands situational awareness, consideration of broader mission objectives, and an understanding of humanitarian law, is a military discipline not quickly or easily replicated in a civilian organization.[56] The Australian model also facilitates command responsibility, a principle of customary international law that holds military commanders responsible for war crimes committed by their subordinates if they fail to take measures to prevent crime or punish those responsible.[57] At the same time, the structure gives military commanders the opportunity to easily leverage the technical capacity of the ASD and the expertise and experience of the directorate's civilian employees.

Canada should adopt this model by modifying existing command and targeting structures within the CAF. Staff from Canadian Joint Operations Command (CJOC) should be embedded within CSE to assist in operational development. CAF should also integrate CSE cyber teams into the targeting cycle and co-locate them within the joint fires group both at CJOC and in forward deployed headquarters.

"Placing CSE civilians within the CAF chain of command would…eliminate confusion about their status in an armed conflict."

Placing CSE civilians within the CAF chain of command would also eliminate confusion about their status in an armed conflict.[58] According to Additional Protocol I (*AP I*), "armed forces" includes groups that are under the command responsibility of the military and subject to that force's internal disciplinary system. Thus, like civilian drone operators who operate weapon systems and identify and engage targets fair away from the front lines, under the proposed structure CSE personnel would qualify as combatants. As such, they would not simply be legitimate targets - a status they would nevertheless acquire as civilians DPH- but CSE personnel would benefit from a combatant's immunity and prisoner of war status.[59]

Issue 3: Principles of IHL

Regardless of the organizational structure adopted, CSE employees supporting the CAF in an armed conflict or directly participating in hostilities through their active mandate will be required to comply with IHL including the principles of distinction and proportionality.

The principle of distinction demands that military operations be directed at military objectives.[60] 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."[61] Distinction in the cyber domain is problematic because of the "pervasive nature of interconnectedness among military and civilian systems and the reliance of the military on civilian infrastructure."[62] 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.[63] As a result, the reliance of the military on civilian and commercial networks, data, servers, and communications infrastructure make 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.[64]

That said, CSE is also required to ensure that if an attack is expected to cause damage collateral to the military objective, that the damage is not excessive in relation to the direct and concrete military advantage gained.[65] The term "collateral damage" refers to the incidental death of or injury to civilians and the incidental damage and destruction of civilian objects. For example, if CSE were to engage in a cyber attack against a power grid that controlled an enemy's air defence system, the Establishment must assess the unavoidable consequences of that attack on civilian life. For example, does that power grid also control civilian air traffic systems? If so, CSE must evaluate whether the foreseeable loss of life resulting from the attack is proportionate to the military advantage gained from taking out the enemy's defences. If the incidental consequences of the attack are excessive, it is prohibited under IHL. Moreover, if a cyber operations' effect on civilians is uncertain, carrying out the attack would be considered unlawful regardless of the military advantage gained.[66]

"CSE must evaluate whether the foreseeable loss of life resulting from the attack is proportionate to the military advantage gained from taking out the enemy's defences."

This rule, known as the principle of proportionality, "establishes a link between the concepts of military necessity and humanity."[67] CSE employees conducting or supporting armed attacks must be capable of calculating the incidental effects of their actions and weighing those effects against the expected military advantage.

To reinforce the principle of distinction, international law prohibits specific military tactics. For instance, it is illegal to improperly use protective indicators like the Red Cross and the Red Crescent, or to improperly use neutral party or enemy indicators such as military flags, insignia and uniforms.[68] Perfidy- inviting the confidence of adversaries and leading them to believe that you are entitled to protection under the law with intent to betray that confidence- is also prohibited if it results in a person's capture, injury or death.[69] These are crucial considerations for CSE as cyber operations rely on deception to succeed.[70]

In truth, almost all 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.[71] As such, CSE must be aware and cautious to avoid using prohibited tactics when planning active operations and assisting the CAF in operations during an armed conflict. Failure to do so could lead to prosecution for war crimes.

Recommendation: Provide IHL Training to CSE Employees

Every soldier, seaman and airman or woman in the CAF is expected to know, understand and apply the law of armed conflict. To accomplish this, the military incorporates IHL into the training received by its members virtually from the moment they join until the day they retire. Likewise, CSE employees supporting CAF or conducting offensive cyber operations in an armed conflict must learn to identify how international law governs their actions. For this reason, military lawyers from the Office of the Judge Advocate General (JAG) should provide law of armed conflict training on a continual basis to all CSE personnel deployed or working with the CAF. JAG lawyers should also be seconded to work with CSE legal services, and IHL training for CAF personnel must be updated to include cyber operations.

Conclusion

There is no doubt that the future of warfare will increasingly see the deployment of offensive cyber capabilities alongside conventional weapons. Indeed, this is what the government calls for in *Strong, Secure and Engaged*. Correspondingly and with growing frequency, states are affirming that international law applies to the conduct of states in cyberspace and vowing to hold violators of the law accountable. Implementing the policy, organizational and training recommendations outlined above, will help ensure that CSE and the CAF plan and conduct offensive cyber operations in accordance with Canada's international legal obligations. ◆

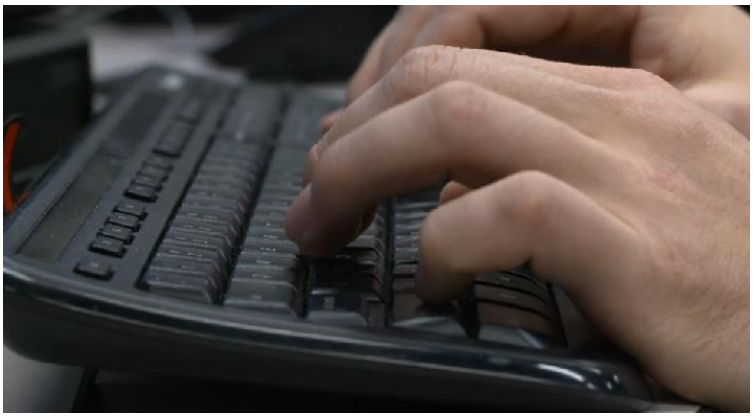


PHOTO CREDIT: Department of National Defence

ENDNOTES

[1] Department of National Defence (DND), *Strong, Secure Engaged: Canada's Defence Policy* (2017), p. 15.

[2] Alex Boutillier, "Canada's Military Seeks Major Cyber Defence Upgrade" *Toronto Star* https://www.thestar.com/news/canada/2017/12/27/canadas-military-seeks-major-cyber-defence-upgrade.html

[3] 1st Sess, 42nd, Parl, 2018 (As passed by the House of Commons, June 19, 2018) cl 76, s 30(1) [C-59].
[4] *Ibid.*

[5] "History," Communications Security Establishment (24 April 2018), online: CSE, https://www.cse-cst.gc.ca/en/history-histoire
[6] SC 2001, c 41, Part IV.; RSC, 1985, c.N-5, s 273.64(1) [*NDA*].

[7] Colin Freeze, "How CSEC became an electronic spying giant" Globe and Mail (25 March 2017), online: Globe and Mail <https://www.theglobeandmail.com/news/politics/how-csec-became-an-electronic-spying-giant/article15699694/>.

[8] Canada, Parliament, *House of Commons Debate*, 42nd Parl, 1st Sess, No 234 (20 November 2017) at 15289 (Hon Ralph Goodale).

[9] C-59, *supra* note 3, cl 76, s 20.
[10] *Ibid,* cl 76, s 19.
[11] *Ibid*, cl 76, s. 30(1).
[12] Craig Forcese, "Does CSE risk a Re X moment with the current drafting in C-59?" *National Security Law* (2 February 2018) online: *National Security Law* <http://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>.
[13] *R v Hape*, 2007 SCC 26, at 53; see also *Suresh v Canada (Minister of Citizenship and Immigration)*, [2002] 1 SCR 3 at 78.

[14] Michael Schmitt, ed, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017) at 564 [*Tallinn Manual*].
[15] *Ibid* at 415.

[16] Some might question whether the traditional concept of territoriality applies in the context of cyberspace. It is this author's opinion that such arguments are misguided. Cyber actors and cyber infrastructure, including hardware, software and the electronic information store therein, will always be physically located within the territory of a state; the reality that infrastructure and information may be accessed online from multiple jurisdictions at once does not negate the relevance of territoriality.

[17] June 26, 1945, 59 Stat. 1031, T.S. 993, 3 Bevans 1153, entered into force 24 October 1945; *Legality of the Use by a State of Nuclear Weapons in Armed Conflicts*, Advisory Opinion, [1996] ICJ Rep 226 at 244 [*Nuclear Weapons Case*].

[18]*Tallinn Manual, supra* note 14 at 333; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Cambridge: Cambridge University Press, 2014) at 53.

[18] Harold Koh, "International Law in Cyberspace" (2012) 54 Harv Int'l LJ Online at 4.
[19] *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America),* [1986] ICJ Rep 14 at para 228 [*Nicaragua Case*]; *Corfu Channel Case (UK v Albania) (Merits)* ICJ Reports 4, 13, 35 [*Corfu Channel*].
[20] *SS Lotus (France v Turkey)*, 1927 PCIJ (ser A) No 10 at 18, 19*; Nicaragua Case* at para 202; John Currie, Public International Law (Toronto: Irwin Law, 2001) p 292-293.
[21] Menno T Kamminga, "Extraterritoriality," Max Planck Encyclopedia Of Public International Law (last updated November 2012), online: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040?rskey=74KqX2&result=1&prd=EPIL.
[23] *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.

(There are scholars who interpret article 2(4) more narrowly in order to justify humanitarian intervention. This debate is beyond the scope of this paper as it remains, for the time being, tangentially connected to the use of offensive cyber operations. For more on humanitarian intervention see: Celeste Poltak, "Humanitarian Intervention: A Contemporary Interpretation of the Charter of the United Nations" (2002) 60 UT Faculty L Rev 1.)

[24] *Ibid.*
[25] International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts" (November 2001) Supplement No. 10 (A/56/10), art 49 [*Draft Articles*].

[26] *Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia) [1997] ICJ Rep 7 at 56*; *Draft Articles supra* note 29 at 129.

[27] See discussion in Karl Zemanek, "Armed Attack," *Max Planck Encyclopedia of Public International Law* at para 9-10 (last updated: October 2013), online: Oxford Public International Law <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241>; *Tallinn Manual supra* note 18 at 341; Heather Harrison Dinnis, Cyber Warfare and the Laws of War (Cambridge: Cambridge University Press, 2012) at 81. See also discussion in International Law Association, *Draft Report on Aggression and the Use of Force,* Johannesburg Conference (May 2016) at 4.

[28] *Tallinn Manual, supra* note 14 at 343.
[29] *Nicaragua Case* at para. 176, 191; not just any violation of article 2(4) necessarily gives entitlement to a right of self-defence. See also *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, ICJ General List No 90 (6 November 2003) at para 76 [*Oil Platforms Case*].

[30] Dinnis at 95 citing *Oil Platforms* at para 64; *Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v Nigeria)* (2002) ICJ Rep at para 323, and; *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (2005) ICJ Rep at para 146.

[31] 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."

[32] International Law Association (ILA), "Use of Force, Final Report on the Meaning of Armed Conflict in International Law," The Hague Conference (2010) at 28, online: ILA <http://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, unorganized 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*, Case No. IT-94-1-T, Opinion and Judgement (Trial Chamber), 7 May 1997 at para 562.

[33] *Tallinn Manual supra* note 14 at 384.

[34] The author acknowledges that defining what is and is not a use of force is a matter of fact and law, and debate amongst scholars, especially in the cyber domain. For this reason, publicly stipulating that CSE's actions should fall below the use of force line may help offended parties identify the intent behind Canadian cyber operations and gauge their response accordingly. For more on this debate see: 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; 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*, vol 3 (Oxford University Press, Oxford 2008) 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: Just Security <https://www.justsecurity.org/55005/legality-international-law-force-deter-chemical-warfare/>.

[35] Draft Articles on the Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission (2001), UN GAOR, 56 sess, Sup No. 10 A/56/10, c IV, E1, art 49; John Currie et. al, *International Law: Doctrine, Practice and Theory* (Toronto: Irwin Law, 2007) p 761, 817 (the draft articles are generally accepted by states as a reliable restatement of customary international law).

[36] 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 3-2.

[37] 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, art 51 [*AP 1*].

[38] International Committee of the Red Cross (ICRC), *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*].

[39] 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: ICRC <https://www.icrc.org/eng/ assets/files/other/icrc-002-0990.pdf> [*Interpretive Guidance*].

[40] *Ibid* at 46.
[41] *Ibid.*
[42] *Ibid.*
[43] *Ibid* at 65.

[44] *Tallinn Manual supra* note 14, at 431. Controversially, the *ICRC Guidelines, supra* note 39, at p 46 limit the civilian's loss of protected status to "the duration of each specific act amounting to direct participation in hostilities." This interpretation can result in what some refer to as the "revolving door" between combatant and non-combatant status: 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 169.

[45] *AP 1*, supra note 37, art 43(2).
[46] Johann-Christoph Woltag, Cyber Warfare: Military Cross-Border Computer Network Operations under International Law (Cambridge: Intersentia, 2014) at 242; *Geneva Convention (III) Relative to the Treatment of Prisoners of War of August 12, 1949,* Geneva, art 14-15

[47] J. Vitor Tossini "The Five Eyes – The Intelligence Alliance of the Anglosphere," United Kingdom Defence Journal (14 November 2017) online:< https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere.

[48] In 2015, CSE's budget was reportedly $829 million CAD, and reporting from 2018 indicates the agency has approximately 2,200 employees. The most recent defence budget in Australia put ASD's budget at $827 million AUD, and staffing at approximately 1,900 people. Parliament of Australia, "Defence budget overview" (May 2018) online: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201819/DefenceB#_ftn14; Tom McIlroy, Australian Signals Directorate $75 million Canberra upgrade gets go ahead, *The Canberra Times* (13 September 2017); Jim Bronskill, "CSEC, Canada's Electronic Spying Agency, Gets $385-Million Budget Boost While Watchdogs Face Cuts" *Canadian Press* (9 April 2014); Richard Yerema and Kristina Leung: CSE Recognizes as one of National Capital Region's Top Employers," MediaCorp Canda, (30 Jan 2018) online: < https://content.eluta.ca/top-employer-communications-security-establishment/>.

[49] Australia, *Intelligence Services Actu 2001*, No. 152, 2001, s 7: The ASD is governed by the *Intelligence Services Act 2001,* which prescribes the seven functions of this civilian agency. The primary mandate of the ASD is the collection and communication of signals intelligence about the capabilities, intentions or activities of people or organizations outside Australia for the purposes of meeting the requirements of the Australian Government. Other functions include: preventing and disrupting offshore cyber-enabled crime; providing cyber security advice and assistance to Australian governments, businesses and individuals; protecting the specialized tools ASD uses to fulfil its functions; cooperating with and assisting the national security community in the performance of its duties; and; supporting military operations.

[50] National Defence and the Canadian Armed Forces, "Canada-Australia Defence Relations" (last modified 6 July 2018) online http://www.forces.gc.ca/en/news/article.page?doc=canada-australia-defence-relations/hgq87xs8.
[51] *Ibid.*
[52] Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October 2017).

[53] *Ibid*, p 54.

[54] *Ibid* p 55

[55] *Ibid*.

[56] See Government of Canada, "The Canadian Forces Operational Planning Process" (April 2008) online: http://publications.gc.ca/collections/collection_2010/forces/D2-252-500-2008-eng.pdf.
[57] *Hadžihasanović and Others case, Decision on Joint Challenge to Jurisdiction,* ICTY- 01-47-PT (12 November 2002) at para 202 (International Tribunal for the Former Yugoslavia, Trial Chamber).
[58] *AP 1*, *supra* note 36, Art 43 (1).

[59] ICRC, "The use of armed drones must comply with laws: Interview of Peter Maurer, ICRC President" (10 May 2013) online: ICRC < https://www.icrc.org/eng/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm>.

[60] *AP I* art 48

[61] *Ibid* art 52 (2)

[62] Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution" (2017) 26 Minn J Int'l L 419 at 424.

[63] Roscini at 185

[64] For more detailed discussion on the issue of distinction in cyberspace see Pascucci, *above* note 62.

[65] *AP I* art 51 (b).

[66] *Tallinn Manual* at 456.

[67] 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 2-2 citing *AP 1* supra note 36, Arts (5) (b), 56 (3), 57 (2) (a) (iii) & (b) & 85 (3) (b) & (c).

[68] *AP I supra* note 37, art 38, 39.

[69] *CAF LOAC Manual, supra* note 67, at 6-1, 6-2.

[70] Heather Roff, "Cyber Perfidy, Ruse, and Deception" in Fritz Allhoff et al "Binary bullets: the ethics of cyberwarfare" (New York: Oxford University Press, 2015) at 213.

[71] Canadian Centre for Cyber Security, "An Introduction to the Cyber Threat Environment" (6 December 2018) online: < https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment>.