National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

COMPREHENSIVE CYBER OPERATIONS: ATTRIBUTION, EFFECTS AND POLITICAL WILL

Maj M.C. Koppang

JCSP 42

Master of Defence Studies

PCEMI 42

Maîtrise en études de la défense

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 44DL – PCEMI 44AD
2015 – 2017

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

COMPREHENSIVE CYBER OPERATIONS: ATTRIBUTION, EFFECTS AND POLITICAL WILL

Maj M.C. Koppang

Word Count: 24,131

Compte de mots: 24,131

TABLE OF CONTENTS

INTRODUCTION

The operations of Canadian security agencies encompass warfare, espionage and law enforcement. Cyber incidents impact profoundly on the security of Canada and its citizens. Such incidents are hardly new but have increased in frequency and sophistication. For decades women and girls have been killed by sexually motivated predators, soldiers have been killed by extremists, spies have stolen government secrets, activist groups have protested through interference with government services and people have trafficked in drugs. Canadian security agencies have been slow to address the challenges posed by the emerging cyber domain.

The internet no more exists for cyberwar than a poppy field did for trench warfare. Nor does it exist for cyber crime, any more than a dark alley does for a murderer. In the cyber domain the dominant adversary can change the poppy field into a mountainside while the conflict is unfolding, and the successful murderer can erase the alley from existence after the murder has taken place. These analogies illustrate three key points that underlie analysis of operations in the cyber domain: it is entirely artificial, it was not designed for security operations, and it can and is being changed every moment of every day. Technology has challenged the ability of Canadian security agencies to protect Canadians as they work largely in isolation from each other. Struggling alone, Canadian security agencies are defining their cyber operations through the narrow lens of their traditional jurisdictions, failing to leverage the globally based technical realities of cyberspace. Canadian security agencies can only begin to effectively respond to the spectrum of cyber threats by leveraging each other, along with government, industry and private resources. The necessity of integration presents an uncomfortable prospect for all

Canadian security agencies. Operationalizing a comprehensive approach is one way to achieve the level of integration and outreach required to succeed. Lessons from past operations teach us that getting the comprehensive approach past idealized concept is difficult and requires effective structure and commitment from those involved. These lessons have also taught us that for complex threats, the comprehensive approach is Canada's best chance for success in this domain. Canadian security agencies have the capability to build those effective structures that can adapt to this ever-changing operational domain.

The internet was designed for the free flow of information between people. The cyberspace has become a fundamental part of society. Individuals use it for many aspects of daily life and governments use it as a primary means for accessing services. It incorporates entertainment, commerce, all manner of inter-personal communications, education, government interaction, health care delivery and security. Almost every aspect of everyday life is reflected or impacted by or through the cyber domain. The interconnectedness creates an incredibly complex operating environment for security operations. The way in which the internet is organized and structured informs the operational environment. This knowledge is critical to understanding why the definition of cyber operations must remain broad and inclusive of the realities of the cyber domain, and not get locked into describing only one or two aspects.

The internet operates through various aspects of infrastructure and software applications that are designed and supported through public organizations and private corporate service providers. From a security operations perspective, this environment allows any person or group to interact with a high degree of anonymity. This anonymity

makes discriminating questions of who and where a primary security focus. In an offensive capacity it is imperative, and legally required, to know specifically where and who the target is. Put another way, a hostile actor could base operations anywhere in the world, including from within Canada. Knowing who is launching a cyber operation and where it is emanating from is the critical first step in formulating an effective response, both from defensive and offensive perspectives. Attribution is the term used to describe these issues. Accurately attributing a cyber operation is critical because it is one of three factors that determine what legal regime applies.

As a democracy existing in an international order the rule of law is paramount in Canada. The rule of law is the concept that all human activities and interactions are governed by rules and conventions that allow reasonable predictability in engaging in those activities and interactions. For Canadian defence and security agencies, this principle is paramount as each agency is given extraordinary powers that impact people in profound ways. Included in these powers is the deployment of highly intrusive surveillance technologies, interference with free movement, detention and arrest leading to expulsion from the country or lengthy incarceration. Defence and security agencies must therefore operate within a legal context.

To better understand the legal context, the three legal regimes applicable to cyber operations were examined. Professor Michael Schmitt's works represent current views of international legal communities regarding key aspects of cyber operations. The two international legal regimes relevant to cyber operations as peacetime international law and the Law of Armed Conflict (LOAC). Understanding the legal thresholds for transition between these legal regimes provides key context for what factors countries are

using to respond to hostile cyber actions. International law predominantly emphasises effects to determine what responses were lawfully available to impacted states. Key executive political decisions are required when operating in these legal regimes, such as withdrawing diplomats, taking economic measures or even declaring war. The international considerations for making these decisions is quite different than those assessed for establishing domestic jurisdiction.

Canadian legislation that governs the military, intelligence and police provides insight into how the four key agencies, the Canadian Armed Forces (CAF), the Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), and the Royal Canadian Mounted Police (RCMP) have approached cyber operations. Domestic mandates will show how attribution questions such as where, who and why predominately decide domestic agency jurisdiction.

This review of international and domestic law demonstrates how attribution, effect and political will are required to determine what legal regime governs cyber operations. Three legal regimes potentially apply to Canadian defence and security agency's cyber operations: peacetime international law, LOAC, and/or domestic law. The importance of correctly determining the applicable legal regime cannot be overstated. The legal regime will inform not only the responsive cyber operations lawfully available, but also the restraints and constraints placed upon the agency conducting those cyber operations. Once a legal regime is determined, the next most significant factors impacting a responsive cyber operation in Canada are constitutional questions.

Privacy is currently at the center of constitutional applicability. The dialectic around privacy involves the metaphors and analogies law makers and judges use. The

Supreme Court of Canada and lower federal and provincial courts have replaced actual legal analysis of cyber operations with imperfect metaphor and analogy. Looking at some of the novel pragmatic approaches to privacy advocated by Professor Daniel Solove suggest a way forward that can be realized through a comprehensive approach. Applying a pragmatic approach to privacy ought to be important because different views of constitutional restraints and constraints are currently being applied to similar cyber operations by different agencies. Different approaches create potentially significant impacts on the legality of these cyber operations and public perception. The effectiveness of a pragmatic approach to privacy specifically, and effective cyber operations generally, is reliant upon taking an overall comprehensive approach.

A comprehensive approach has many advantages that account for mandates informed by the overarching legal environment. A coordinated integration of cyber operations provides an operational environment where effective attribution, effects and political will can be applied to determine the applicable legal regime for a given cyber operation. In an integrated environment, operational leaders could leverage the unique capabilities of multiple agencies to make informed decisions on the types of cyber operations that would best meet both agency mandates and overall benefit Canadians. A common operations coordination center could provide actual de-confliction to avoid "friendly fire" incidents and a host of other second order benefits including enhanced information sharing and coordinated capability development. This comprehensive approach must include an effective investigative function to provide attribution, effective networking/communication to measure effect properly, and effective political-operational interface to provide timely, legitimate and transparent political direction.

Underlying any proposed increase in operational effectiveness is the requirement for security agencies to emerge from the background into the light. Defence and security agencies routinely engage in extra-ordinary operations that are beyond everyday experience for most Canadians. In these specialized roles, these agency personnel are in a unique position to explain the necessity of cyber capabilities as contribute to the discussion about how best to balance privacy interests with defence and security mandates. Maintaining public trust in security institutions is fundamental and could be enhanced through coordination and accountability to effective senior operational, political and judicial oversight. Far from just being a comforting notion, public confidence in transparent cyber operations is arguably essential in a modern democracy. Transparency enhances operational effectiveness by increasing the engagement of private citizens and corporations, who can trust that their cooperation in security matters will not compromise their own interests. Public trust underpins the business of securing Canada and Canadians. Employing an effective comprehensive approach has the potential to provide a multitude of operational benefits. To achieve these benefits, Canadian defence and security agency leaders need to put aside narrow views to understand cyberspace and the domestic and international laws that apply to it.

CHAPTER 1 - THE CYBER DOMAIN

What constitutes the cyber domain? Recent release of the *Canadian Armed Forces Joint Doctrine Note* (Joint Doctrine Note) has clarified institutional understanding of cyber operations.[1] The cyber domain from this perspective has been organized into five layers that constitute "all infrastructure, entities, users and activities related to, or affecting, cyberspace."[2] Cyberspace constituted three of these layers. The first called "logical persona," includes how people represent themselves in cyberspace, such as user accounts, email and web pages. The simple term "persona" is used here to describe this layer. The second called "logical network," includes the software, operating systems and communication protocols. The final layer called the "physical network" includes the actual devices people use to access the internet as well as the hardware, wires, satellites or other physical means of operating these systems. The remaining two layers that complete the whole of the cyber domain are the actual people that use cyberspace and the "geographical" that represent the physical location of either people or infrastructure.

The five-layer model is useful because it provides common language to describe key components of cyber operations. The five-layer model provides a frame of reference to understand the complexity. Most importantly, the interaction between the two uniquely cyber layers of persona and logical network provides the framework to understand how cyber operations differ from the other physical domains of air, space, land and sea. The logical network is the key to understanding attribution challenges. From a legal perspective, sometimes it will be a person that is important to attribute the cyber

---

[1] Joint Doctrine Branch, Canadian Forces Warfare Centre, *Joint Doctrine Note - Cyber Operations* (Ottawa: Department of National Defence, 2017). It is recognized that the different provisions within the Joint Doctrine Note are designated with different levels of maturity.
[2] *Ibid*., 2-1.

operation to, but in other situations it will be acceptable to attribute the geography of the physical network.

Internet Organization

How the cyber domain operates is key to understanding attribution and effects. How the internet is structured and operates is also key to engaging in an analysis of legal issues, including privacy considerations. When dealing with security issues in the cyber domain, having only a superficial knowledge of internet organization is comparable to operating a ship on the ocean with superficial knowledge of tide, navigation rules and nautical charts. Like this analogy, security and legal professionals sometimes engage in cyber operations without sufficient technical understanding. Important decisions are being made substituting actual technical understanding with inaccurate jargon and colloquial beliefs.

As a technology, Internet Protocol (IP) addresses allow networked devices to communicate. These IP addresses are commonly expressed in a dotted-decimal format called version 4 (v4). An IP address is assigned to every device on the internet that allows other devices to find it and communicate. A significant issue facing current internet operation is that the world has run out of v4 IP addresses.[3] Significant to all security agencies is the development of version 6 (v6) IP which utilize a hexadecimal format, allowing for an exponentially greater number of IP addresses. The specific security issues raised with v6 are numerous but deserve mention as an emerging security issue.

Most users connect to the internet through an Internet Service Provider (ISP). In Canada many commercial services are available, but the most common are concentrated

[3] "IPV6 Info Center," last accessed 28 March 2018, https://www.arin.net/knowledge/ipv6_info_center.html.

in large ISP companies like Bell, Telus, Shaw and Rogers. These ISP companies sell access to services, and in return are responsible for assigning IP addresses to devices. The ISP retains customer information, as well as usage information on their customers. The software that accesses the ISP from devices is largely owned by large multi-national corporations like Apple, Microsoft and Google. These companies keep even more extensive customer information including patterns of life such as movement, location services, shopping habits, search and browsing histories.

The ISP companies get IP addresses assigned by Regional Internet Registries (RIR). Canada is serviced by the American Registry for Internet Numbers (ARIN), which handles IP addresses for Canada, the United States, parts of the Caribbean and Antarctica.[4] ARIN services governments, corporations and ISP demands for IP addresses. ARIN works with other RIRs to develop guidelines on how the limited number of IP addresses are distributed and recycled to ensure sufficient IP addresses are available for everyday device loads.

The internet does not work simply on these numerical IP addresses, as most internet browsing software utilizes text searches to find word-based internet content. The words attached to website naming are called domain names. The coordination of domain names is done at the highest level by the International Corporation for Assigned Names and Numbers (ICANN) an international non-profit organization.[5] ICANN coordinates the unique names and IP addresses globally. Without this coordination, there would be no

---

[4] American Registry for Internet Numbers, "Regional Internet Registries," last accessed 28 March 2018, https://www.arin.net/knowledge/rirs.html.

[5] International Corporation for Assigned Names and Numbers, "International Domain Names," last accessed 28 March 2018, https://www.icann.org/resources/pages/idn-2012-02-25-en.

global internet. ICANN uses the Domain Name System (DNS).[6] These "top level" domain names include the ubiquitous ".com" as well as national and open identifiers like ".ca," ".org" and ".gov." By working with each RIR, ICAN ensures that global rules are followed to ensure that when a user types in a website name they are directed to the correct numerical IP address. The DNS works only through the function of groups of servers located around the world known as Root Name Servers.[7] For the internet to function the DNS is always accurate. In other words, the Root Name Servers will always produce a given IP address for a specific domain name, routing the user reliably to the same information content they are seeking. The complexity of this system and the number of actors involved is not apparent to the end user. Public oversimplification is rampant, when most end users just type a query into Google and their webpage appears. This complex system makes the end interaction extremely easy for the end user.

ICANN also organizes a system by which domain names are registered by specific users. The registration process is managed through a system of registries. ICANN manages the "top-level" domain names and designates those to ICANN accredited "registrars."[8] Individuals wishing to acquire a domain name must register with these accredited registrars, usually at a fee. Canada has more than twenty accredited registrars, where people or corporations can register a domain name of their choice.

A basic understanding of internet organization demonstrates that the key enablers of internet infrastructure is a complex network of public international bodies and for-

---

[6] International Corporation for Assigned Names and Numbers, "Domain Name Registration Process," last updated July 2017, https://whois.icann.org/en/domain-name-registration-process.
[7] PCnames.com, "How Domain Names Work," last accessed 28 March 2018, http://www.pcnames.com/Articles/How-Domain-Names-Work.
[8] International Corporation for Assigned Names and Numbers, "Information for Registrars," last accessed 28 March 2018, https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en.

profit businesses. To obtain access to this infrastructure requires in every instance personal information to be shared. In most cases, depending upon individual usage, core biographical information that goes well beyond simply name and address will be shared with multiple public and private bodies including ISP, operating system providers, software companies and domain name registrants. Some of this information is easily available to the global internet community, while the rest is used by the multi-national corporations for a wide variety of reasons largely aimed at selling things to the end user. Review of usage agreements reveals that often this highly personal information is sold and re-sold for profit. When a user enters cyberspace, the ISP that a user engages will usually be readily available to anyone who searches for that IP address. Those ISPs maintain customer information, including IP address activity.

Understanding these basic technical infrastructures is important because they comprise the persona, logical and physical network levels. This understanding can also better inform discussions around privacy issues. The technical infrastructure can then be applied to conceptually organizing cyberspace into operational levels. Operational levels assists in understanding methods of attribution and the level of sophistication required to accomplish it.

Operational Levels of Cyberspace

Cyberspace consists of the persona, logical networks and physical networks. It is estimated that approximately 1.7 billion people are networked through cyberspace and this number grows everyday.[9] In an operational context, cyberspace can be further organized into levels that are described through the degree of knowledge or software

[9] Elias Bou-harb, Mourad Debbabi, and Chadi Assi, "Cyber Scanning: A Comprehensive Survey," *IEEE Communciations Surveys & Tutorials* 16, no. 3 (Third Quarter 2014): 1496.

required to access the devices or information that comprise cyberspace. The terms "surface web," "deep web" and "dark web" are commonly used to describe three distinct operational levels within cyberspace. The persona, logical networks and physical networks are present in all three operational levels of cyberspace.

The surface web consists of information and webpages that are readily indexed through traditional search engines such as Google.[10] Access is accomplished through a process of continual indexing of static and linked webpages.[11] By some estimates, only four percent of the total content of information in cyberspace is available on the surface web.[12]

The deep web constitutes most of the information on the internet, estimated to be thousands of times larger than surface web content.[13] Simplistically, the deep web is content that can only be accessed with special knowledge. More specifically, each website has content that is found within that website. The internal content is the reason most websites have a search function. The content can only be identified with a specific search of that website. Access can be free, subject to a fee or may require the searcher to create a persona utilizing a username and password to access the website content. Many common examples of deep web content include travel websites where you need to search that website to find your flight or hotel, or websites that allow you to search for judicial decisions. This content cannot be located through a search such as Yahoo or Google. Those surface web search engines will direct the user to a range of webpages that then

---

[10] Dilip Kumar Sharma and A.K. Sharma, "Deep Web Information Retrieval Process: A Technical Survey," *International Journal of Information Technology and Web Engineering* 5(1) (January-March 2010): 1.
[11] Michael K. Bergman, "White Paper: The Deep Web: Surfacing Hidden Value," *Journal of Electronic Publishing* 7(1) (August 2001): 1.
[12] Firecompass, "Understanding Surface Web, Dark Web, Deep Web and Darknet," last modified 5 October 2017, https://www.firecompass.com/blog/darkweb-deepweb-darknet-browsers/.
[13] Sharma, *Deep Web Information*…, 1.

require a second search in the deep web to obtain the specific content the user is looking for.

The dark web is a small area of cyberspace that is accessed by special encryption software. There are a variety of different software packages that can be utilized, with the most common being the "The Onion Router" ("Tor") browser. This software is free to anyone to install on their computer. With Tor, encrypted networks are created that allow users to communicate anonymously. Using common but powerful encryption technology, users can create personae that allow direct anonymous communication and participation in online marketplaces, discussion forums, file exchange sites or messaging functions. Often the dark web is utilized for illicit activity due to the effectiveness of the encryption technology. These networks are highly resistant to indexing, and very few effective search engines exist for the dark web. The dark web is estimated to occupy a very small amount of cyberspace.[14] Despite its relatively small footprint, the dark web has gained significant notoriety due to the use of this anonymizing technology by criminals, spies, terrorists and militaries. Despite the notoriety, the dark web has legitimate uses, particularly in support of free speech in areas lacking robust civil liberties.

Understanding these basic concepts of how the cyber domain functions and how people interact with the technology and each other using the technology, sets out the first, and arguably most critical step in understanding security operations in the cyber domain. Attribution is the term used to describe the process by which one identifies actual people, personae, logical networks, physical networks and physical location. A given cyber operation may emphasize one or more of the five layers. Gaining a technical and

[14] BrightPlanet, "Clearing Up Confusion – Deep Web s. Dark Web," last modified 27 March 2014, https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.

operational understanding how cyberspace works allows us to define the attribution problem.

Attribution

Security agencies both battle with and utilize the inherent attribution issues in cyberspace. Attribution has been repeatedly acknowledged as one of the most challenging areas of cyber operations.[15] When a cyber operation is underway it has been practically impossible to instantly assign attribution.[16] A basic understanding of cyberspace technology and infrastructure provides clear insight as to why.

The first issue is understanding IP addresses. In the physical world, people have traditional, long term unique identifiers such as names, addresses, and phone numbers assigned and formally registered to them. Although every networked device gets an IP addresses, it changes regularly. If you utilize your cell phone at the coffee shop, while driving your car and then at a shopping mall, you will likely move through a variety of IP addresses assigned to your cell phone that handle your internet traffic. Telephone service providers will have certain IP addresses to handle internet traffic on the cellular network, while the WiFi at your mall and coffee shop will provide your cellular phone a different IP address for each time you connect. There will of course be different IP addresses necessary for the tablet, home computer or television you may have in your home.

Unlike traditional identities, IP addresses will not be assigned to a device for long periods of time. IP addresses are not the same as physical addresses in the sense that they cannot be simply attributed to a single person in the first instance. Put another way, one

---

[15] Michael N. Schmitt, "The Law of Cyber Warfare: *Quo Vadis*?" *Stanford Law & Policy Review* 25, (2014): 278; Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution," *Journal of Conflict & Security Law* 17, no. 2 (2012): 233.

[16] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 33.

cannot usually identify a person solely through the knowledge of their IP address since IP addresses are assigned in batches through RIRs to ISPs.

Attribution is further complicated through the regular use of internet personae. It is very common that individuals will have many personae. Email addresses, usernames for cellular phone service, internet services, television services, social media, and operating systems will all require the person to create a username to access the network services. There is no rule that the username must be descriptive of the person, and often the username is not the person's actual name. Many service providers do not require identification or bother verifying a person's actual identity. Since many companies have no "know your customer" policies, services such as email addresses and cellular phone contracts can be obtained using an alias. The potential for anonymization increases in the deep web since access to network services and contracts can be done utilizing other people's identities or fictional identities.

Finally, many security agencies deal with issues related to the dark web. Anonymizing technology utilized as part of the infrastructure of the dark web makes it ideal for concealing identity. Regularly encountered tactics include routing web traffic through multiple international servers that bury true IP addresses, with logical networks and physical networks hidden behind multiple layers of random hardware, software and ISPs. The use of anonymizing technologies like encryption can be combined with less technical means such as an alias to obtain a persona, making the attribution of a person and their location difficult.

Canadian security agencies have been operating for decades in complex environments and have responded to these technologies, albeit slowly. A basic technical

understanding of cyberspace organization assists with assessing the Canadian government response to cyber operations. Examining the current state of Canadian cyber security policy begins to reveal significant shortcomings in the effectiveness of defence and security agency's approach to cyber threats.

Definition of Cyber Operations

No consistent definition of a cyber operation in Canadian security vernacular exists in the various Canadian defence and security agency's cyber strategies. Cyber operations are defined in the Joint Doctrine Note as:

> An operation whose primary purpose is to achieve an objective in or through the cyber domain. Cyber operations consist of offensive cyber operations, defensive cyber operations and support cyber operations.[17]

The Joint Doctrine Note sets out a four-level organization of cyber operations that leaned heavily on Public Safety Canada definitions.[18] The first two levels are called a "cyber event" and "cyber incident," taken from the 2015 *Government of Canada Cyber Security Event Management Plan*.[19] This plan sets out that events and incidents must impact Government of Canada information technology ("IT") systems before they rate in classification as a level 1 or 2 event or incident in the military spectrum. A level 3 "significant cyber incident" entails a cyber event or incident that could or did impact military operations.[20] The Joint Doctrine Note describes that a level 3 incident becomes a "defence matter."[21] The highest cyber operation is level 4 which is described as a "cyber-

---

[17] Canadian Forces Warfare Centre, *Joint Doctrine Note…*, 2-2
[18] *Ibid.*, 3-9.
[19] Government of Canada, "Government of Canada Cyber Security Event Management Plan," last modified 11 December 2015, https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.
[20] Canadian Forces Warfare Centre, *Joint Doctrine Note…*, 3-9.
[21] *Ibid.*

attack."[22] Level 4 envisions a cyber operation of such significant effect as to rise to the level of an "armed attack" under international law. This type of cyber operation would then be a "matter of national defence" and governed by LOAC according to the Joint Doctrine Note. Interestingly, the Joint Doctrine Note defines a "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."

CSIS does not have a publicly available definition of cyber operations. However, examination of CSIS publications gives Canadians some sense of their cyber operational focus. In one publication on cyber threats, CSIS described a focus on "preventing infections rather than merely reacting to them."[23] It also speaks to "…combating cyber exploitations that target government and business secrets…"[24] In another publication, the discussion focussed around state and non-state actors use of cyberspace to conduct highly effective disinformation campaigns.[25]

The RCMP define cyber operations in terms of "cybercrimes."[26] The RCMP breaks cybercrime into "technology-as-target" and "technology-as-instrument" and defines it as any crime where "cyber…has a substantial role in the commission of a criminal offence."[27] The RCMP further organize the "roles and responsibilities" into three areas: criminal intelligence, criminal investigations and specialized services. In this way, RCMP cyber operations appear to be a blend of proactive intelligence gathering,

---

[22] *Ibid*.
[23] Angela Gendron and Martin Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, (Ottawa: Canadian Security Intelligence Service, 2012), 9.
[24] *Ibid*., 10.
[25] Canadian Security Intelligence Agency, *Who Said What? The Security Challenges of Modern Disinformation*, (Ottawa: Canadian Security Intelligence Service, 2017), 90.
[26] Royal Canadian Mounted Police, *Royal Canadian Mounted Police Cybercrime Strategy*, (Ottawa: Her Majesty the Queen in Right of Canada, 2015), 7.
[27] *Ibid.*, 7.

responsive criminal investigation using specialized Technical Investigations Services and operational support by the Integrated Technological Crime Units.

A definition of cyber operation common to all agencies provides some advantages. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* ("Tallinn Manual 2.0") simply defined cyber operations as "The employment of cyber capabilities to achieve objectives in or through cyberspace."[28] This definition does not distinguish between military and civilian operations and is preferable to that of separate definitions for police, espionage and military cyber operations for several reasons. The first and most important reason is that using consistent definitions to describe the same thing across agencies enables an accurate assessment of what legal regime applies to a particular cyber operation. Assessing the correct legal regime then presents the defence or security agency a range of legal response options that are available. Further benefits would be realized with enhanced communications between agencies utilizing consistent terminology. Communication issues are central to any discussion of Canadian cyber policy.

Canadian Cyber Policy

To date, Canada has taken a distinctly defensive posture in managing hostile cyber operations. The *Canadian Cyber Security Strategy* (CCSS) sets three national strategy pillars: securing government systems, partnering to secure vital cyber systems outside government, and generally helping Canadians to be secure online.[29] If a cyber operation has identified criminal activity, terrorist activity or national defence, the

---

[28] Int'l Grp. Of Experts at The Invitation of The NATO Coop. Cyber Def. Ctr. Of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. Michael N. Schmitt, (Cambridge: Cambridge University Press, 2017), 564.

[29] Government of Canada, *Canada's Cyber Security Strategy* (Ottawa: Her Majesty the Queen in Right of Canada, 2010),7.

government plan recommends reporting these incidents to the Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS) and the Department of National Defence respectively. However, these are only three of nine agencies responsible for implementing the CCSS, which also include: Public Safety Canada (PSC), Shared Services Canada (SSC), Communications Security Establishment (CSE), Treasury Board of Canada Secretariat (TBS), Global Affairs Canada (GAC), and Justice Canada (JUS).[30] Peripheral stakeholders in the CCSS include Public Services and Procurement Canada (PSPC), the Privy Council Office (PCO) and Innovation, Science and Economic Development Canada.

Some agencies have begun the process of more closely integrating respective cyber operations capabilities. The extent of collaboration between the CAF and CSE was highlighted in Canada's recently updated Defence Policy. The CSE is cited in this policy as one agency that the CAF "works closely with" on cyber issues.[31] The updated Defence Policy was the first official acknowledgement by Canada that it intends to engage in offensive cyber operations "focused on external threats to Canada in the context of government-authorized military missions."[32] Given the mandate of the CSE and the specific citation in policy, it is probable that offensive cyber capabilities will be developed in partnership between the two organizations. This close collaboration was partly acknowledged by CSE Chief Greta Bossenmaier's public statement of CSE

---

[30] Public Safety Canada, *Horizontal Evaluation of Canada's Cyber Security Strategy Final Report*, (Ottawa: Public Safety Canada, 2017), 2.
[31] Department of National Defence, *Strong Secure Engaged, Canada's Defence Policy*, (Ottawa: Her Majesty the Queen in Right of Canada, 2010), 72.
[32] *Ibid.*

support to the CAF in Iraq.[33] Although this collaboration is positive, the military does not handle the majority of hostile cyber operations.

Hostile cyber operations in Canada are mostly handled and managed through Canadian domestic law, with over 4,000 such incidents reported in 2012 alone.[34] Even some defence commentators have argued that governments ought to focus more on cyber crime as the most common and serious threat.[35] Some data suggests this assessment may be accurate. The RCMP published statistics in 2014 that analyzed 2011-2012 incidents of cybercrime that suggested it was rapidly increasing.[36] The report described the scope of incidents including approximately 4,000 incidents of cybercrime, 16,000 cyber-related complaints to the Canadian Anti-Fraud Centre, and 9,000 reported incidents of online child sexual exploitation. These statistics indicate the majority of cybercrimes are investigated pursuant to the *Criminal Code*. The number or incidents are believed to be expanding since then.

PSC is supposed to provide the strategic oversight and coordination to Canadian Cyber Security. PSC purportedly provides this oversight through the Canadian Cyber Incident Response Centre (CCIRC) and when necessary, the Government Operations Center (GOC) and interdepartmental committees or working groups. Strategic guidance is provided through a governance structure that moves from Cabinet through to the specific agencies, see Figure 1.

Cabinet

[33] Chris Madsen, *Military Law and Operations* (Toronto: Carswell, 2017), 30, para. 3:20.100.
[34] Royal Canadian Mounted Police, *Cybercrime: An Overview of Incidents and Issues in Canada*, (Ottawa: Her Majesty the Queen in Right of Canada, 2014), 7.
[35] Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* (Spring 2011): 84.
[36] RCMP, Cybercrime…, 7.

<table>
<tr><td colspan="12">Deputy Ministers Committee on Cyber Security (DM Cyber)</td></tr>
<tr><td colspan="12">Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber)</td></tr>
<tr><td colspan="6">Directors General Committee on Cyber Security (DG Cyber)</td><td colspan="6">Directors General Committee on Cyber Security Operations (DG Cyber Ops)</td></tr>
<tr><td>PSC</td><td>CSIS</td><td>RCMP</td><td>DND</td><td>CSE</td><td>DRDC</td><td>GAC</td><td>JUS</td><td>PSPC</td><td>SSC</td><td>TBS</td><td>PCO</td><td>ISEDC</td></tr>
</table>

Figure 1 - Government of Canada Cyber Governance Model
Source: *Canadian Cyber Security Strategy*, 2.

The Horizontal Evaluation of this governance model after seven years in use identified some definitive shortcomings. Most troubling, but perhaps not surprising are three key shortfalls: a lack of common understanding of roles and responsibilities, developing separate cyber capabilities produces repetition and inefficiency, and lack of effective information sharing between agencies.[37] These shortcomings indicate a lack of overall oversight and coordination. A brief review of the CAF and RCMP cyber operations policies exemplifies the manifestation of these shortcomings.

The Joint Doctrine Note contemplates a largely military-centric attribution process citing intelligence at the tactical unit level and strategic analysts "providing insight" into actor and sponsor trends.[38] This approach, which included the CSE, has no mandate to investigate domestic attribution.[39] It is hard to contemplate how this policy can be effective. Given the nature of attribution, one does not know the who or where of a hostile cyber operation. Is this policy to be interpreted by the CAF as to stop the attribution investigation when they discover a Canadian IP address? This policy gap is the first of several attribution "blind spots" evident in the current CAF approach to cyber operations.

---

[37] Public Safety Canada, *Horizontal Evaluation*…, 7.
[38] Canadian Forces Warfare Centre, *Joint Doctrine Note…,* 4-17.
[39] *National Defence Act*, R.S.C., c. N-5 s. 273.64(2) (1985). This section sets a prohibition that CSE activities shall not be directed at Canadians or any person in Canada.

Another policy gap is utilizing an armed attack threshold to establish military jurisdiction which ignores other potentially significant cyber operations that may be considered a use of force.[40] Depending on the attribution, potential internationally wrongful acts may invite an array of national level responses that could include the military, but could also be appropriately conducted by Global Affairs, CSIS, the RCMP, or even the Prime Minister. Furthermore, unless these incidents resulted in Canada recognizing a state of armed conflict, LOAC would not apply even if the hostile cyber operation met the definition of an armed attack. These are executive political directions that the CAF will receive, although currently there exists no clear model as to how these decisions would be made.

A cyber operation that impacted military operations does not necessarily allow for CAF jurisdiction. In recent domestic attacks such as on military recruiting centers or the murder of CAF personnel by ISIS-inspired jihadists the police asserted jurisdiction because these incidents were treated as domestic criminal matters. Using similar rationale, a cyber attack impacting military operations in Canada would most likely engage the police to investigate as a crime or CSIS to investigate as a national security threat, unless the effects were significant enough to engage international law.

These military examples demonstrate lack of coordination with other security agencies, other than the CSE. Nowhere in this policy are there mechanisms that contemplate transitioning cyber operations from CAF control to a security agency or vice versa. These shortcomings are not unique to the CAF policy.

The RCMP divides its cyber operations into three areas: criminal intelligence, criminal investigations, and specialized services. The RCMP addressed cyber operations

---

[40] Canadian Forces Warfare Centre, *Joint Doctrine Note…, 3-9*

through the creation of a dedicated cybercrime intelligence unit and a "new investigative team dedicated to combat cybercrime," that will reach full implementation in 2017 and 2020 respectively.[41] The RCMP also plans to establish a "governance structure for cybercrime priorities and operations" which is described as devoting personnel for oversight and accountability for the cybercrime investigative team.[42] This governance structure also aims to "provide tactical operational support, advice and direction to all major investigational cybercrime projects."[43] In other words, the RCMP has adopted a central control approach to the development of cyber capabilities.

Like the CAF policy, the RCMP policy fails to present how cyber operations would transition into RCMP jurisdiction or to another defence or security agency. The RCMP policy does not refer to the CAF, CSIS or CSE. Capabilities are discussed only in terms of cyber crime and internal to the RCMP specialized units. Reviewing this policy shows the similar shortcoming evidenced in the CAF policy, largely surrounding a narrow view of cyber operations existing in a larger Canadian security context.

Although one view may be that these symptoms simply denote signs of leadership failures, there may be an alternate legal explanation of why these phenomena developed. Examining the legislation creating Canadian security agencies reveals the specifics of the jurisdictional overlap. The mandating legislation also reveals how the security agencies traditionally recognize matters within their jurisdiction. Recognizing that three distinct legal regimes may govern cyber operations introduces a level of complexity that is beyond the capabilities of any single agency to work through alone. Despite the capability of each defence and security agency to work both domestically and abroad,

---

[41] RCMP, *Cybercrime Strategy*…, 12.
[42] *Ibid.*
[43] *Ibid.*

each agency's mandating legislation set conditions that indicate the legal regime they were designed to serve. Understanding these complexities offers a better explanation for the shortcomings identified in the Horizontal Evaluation.

In a democratic state like Canada, responses to cyber operations with unlimited methods and means are rare, if not impossible, due to legal and policy restrictions informed by public sentiment. A unique aspect of the cyber domain is the intimate accessibility to a global infrastructure. Neither domestic or international law have contemplated capabilities of an adolescent in rural Saskatchewan or contracted operators in a Chinese warehouse capable of possessing the means to cause catastrophic harm to government institutions or infrastructure anonymously. Examining international and domestic law is fundamental to understanding the framework in which governments and security agencies are permitted to respond to this developing technology.

CHAPTER 2 - LEGAL REVIEW FROM A CANADIAN PERSPECTIVE

An old adage is that law develops slowly. Therefore, it should come as no surprise that in the face of incredibly fast technological change that has brought significant social change, the law has struggled to keep up. Internationally, significant efforts have been made to align traditional law to the technological change.

It is now well established that the traditional tenets of international law can and should apply to the cyber domain and regulate normative behaviour.[44] It ought to be self-evident that Canadian domestic laws will govern most Canadian cyber operations. Key to Canadian operational effectiveness in the cyber domain is understanding what circumstances require the application of international law, domestic law or both. This exercise will remain imperfect while international and domestic legal norms continue to evolve, but critical nonetheless if Canadian security agencies wish to adhere to the laws they are designed to protect.

Peacetime international law or LOAC may apply to Canadian cyber operations. Understanding the legal tests for a cyber operation to transition from peacetime international law to LOAC is critical for a country engaging in cyber operations. International legal thresholds predominantly focus on an effects-based analysis. Impact, often measured in physical terms, has been the determinative factor in applying the different international legal regimes. Although attribution is an important factor in responsive cyber operations from a practical perspective, attribution is not strictly necessary to determine what international law should apply. The application of domestic legislation has a different analytical basis.

---

[44] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal* 54, (December 2012): 17.

In Canadian domestic legislation, applicable cyber operations attribution analysis is more important than the effects-based analysis. Who, where and why questions are legally more significant than whether the effect was a denial of service or theft of information. Enabling legislation and Canadian Government policy has largely taken an effects-based approach to organizing areas of responsibility and jurisdiction. By focussing almost solely on cyber operation effects, Canadian security agencies can confuse their mandates, promote unclear communication which can result in redundant capabilities development.[45]

Interaction of attribution and effect determines what legal regime applies to cyber operations in the Canadian context. The lawful response options are established by the applicable legal regime. The context for applying political will in determining the appropriate legal regime is assessed which leads to a discussion of privacy. Privacy related to cyberspace has both political and legal dimensions. Canadian security agencies would become more operationally effective by understanding the implications of constitutional compliance for cyber operations, particularly privacy. Failure to get the privacy analysis right has the potential to undermine defence and security agency mandates. Success in balancing cyber operations with civil liberties through a pragmatic approach could see significant operational benefit. Understanding the legal dynamics impacting Canadian cyber operations emphasises the necessity of taking a comprehensive approach.

International Law

[45] Public Safety Canada, *Horizontal Evaluation*…, 7.

The deployment of new technologies to further state's interests has challenged international law. Tremendous uncertainty has surrounded the understanding of international law applied to the cyber domain.[46] The Tallinn Manual 2.0 has assisted significantly with balancing this uncertainty. The second version of the Tallinn Manual 2.0 was written by a group of international legal experts including Canadians.[47] The manual was never meant to have the force of international law, such as a treaty. Instead it represented non-legally binding expert consensus on what the international law was at the time of publishing.[48] Although not legally binding on states, the consensus achieved has contributed to a more stable interpretation of traditional international law principles to cyber operations.

At a basic level, international law simply represents the nation state consensus on rules that govern their interactions.[49] Uncertainty has been created through the natural progression of new legal norms emerging while other are rendered obsolete.[50] The high pace of change in the artificial domain strains this natural progression which creates greater uncertainty. Some have even called for an entirely new international legal regime to govern cyber activities.[51] This view proposes new extra-territorial application to domestic criminal laws and to domestically legislate permissible countermeasure actions in line with new treaties on cyber attacks. These proposals are aimed at speeding up and clarifying the law to address serious hostile cyber operations. The main weakness with

---

[46] Chris Reed, *Making Laws for Cyberspace* (Oxford: Oxford University Press, 2012), 17.
[47] Tallinn Manual…, xiv. Not only was there Canadian input, but the Canadian Judge Advocate General was one of the legal peer reviewers.
[48] *Ibid*., 2.
[49] Michael N. Schmitt, "The Law of Cyber Warfare: *Quo Vadis*?" *Stanford Law & Policy Review* 25, (2014): 272.
[50] *Ibid.*, 272.
[51] Oona A.Hathaway *et al,* "The Law of Cyber-Attack," *California Law Review* 100, (2012): 821; Kristen E. Eichensehr, "The Cyber-Law of Nations," *The Georgetown Law Journal* 103, (2015): 357.

creating new legal regimes to deal with emerging problems is the second and third order effects that these legal regimes will have. Equal to the threat of hostile cyber operations is introducing unpredictability in otherwise well established and functioning international relationships based on many years of state practice. One of the main areas that these novel proposals would fundamentally alter is the concept of sovereignty.

Sovereignty and Jurisdiction

Sovereignty is important to the analysis of cyber operations. The general principle of state sovereignty has underpinned modern international law for a long time.[52] At its core, sovereignty means "the totality of international rights and duties recognized by international law that reside in a State."[53] Through this basic principle, many aspects of state interactions are measured. Some authors have questioned whether sovereignty exists in cyberspace.[54] Questioning this basic principle can in turn cast uncertainty on international legal regimes with sovereignty as their base. The international group of experts unanimously endorsed the first rule of the Tallinn Manual 2.0: "The principle of State sovereignty applies in cyberspace."[55] Recognizing the applicability of this basic principle provides a stable basis for further analysis of international law principles in cyberspace.

Recognizing state sovereignty in cyberspace is important for two reasons. The first is that this principle means Canada asserts sovereign jurisdiction over all cyber

---

[52] Liisi Adamson, "Sovereignty in Cyberspace: Organized Hypocrisy?" (master's thesis, University of Tartu School of Law, 2016), 16.
[53] *Ibid.*, 17.
[54] Peter C. Combe II, "Traditional Military Activities in Cyberspace: The Scope of Conventional Military Authorities in the Unconventional Battlespace," *Harvard National Security Journal* 7 (2016): 562.
[55] Tallinn Manual…, 11; United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: UN, 2013), 8.

activities taking place on Canadian territory which includes cyber infrastructure.[56] In terms of the Joint Doctrine Note, four layers: persona, cyber persona, logical network and physical network pertain to Canadian sovereign territory and are subject to Canadian law.[57] The law of non-intervention applies. This law describes a state's right to choose political, economic, social and cultural systems free from outside interference or coercion.[58]

The second way sovereignty bears on this analysis is sovereign responsibility. The principle of sovereignty applied to cyberspace means that Canada, like all other nations is responsible for the cyber operations that occur on its sovereign territory. When a State breaches one of its international obligations, it is considered to have committed an "internationally wrongful act."[59] There are two ways that a cyber operation may rise to the level of an internationally wrongful act. The first is violations of sovereignty through the principle of non-intervention, such as interfering with a state's electoral process. The second is unlawful use of force that does not rise to the level of an armed attack, such as the destruction of critical data.[60] In either case, the victim state is permitted a range of responses under peacetime international law.

Law of Non-Intervention

Principles of non-intervention spring from customary international law. One of the clearest expressions of this principle came from the International Court of Justice in

---

[56] Schmitt, *Quo Vadis…*, 274.
[57] Tallinn Manual…, 13.
[58] Thomas Payne, "Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations," *Lewis & Clark Law Review* 20, no. 2, (2016): 699.
[59] United Nations General Assembly, *Responsibility of States for Internationally Wrongful Acts*, (New York: UN, 2002), 2.
[60] Payne, *Old Law New Tricks*…, 693.

Nicaragua v. *United States of America.*[61] In that case, the court described the purpose of the principle of non-intervention was to protect the right of sovereign states to conduct "affairs without outside interference."[62] Interestingly, the court defined the extent of the principle quite broadly, in terms of a state freely choosing "political, economic, social and cultural" systems including foreign policy.[63] The court established the test for violating this principle as one of using "methods of coercion in regard to such choices, which must remain free ones."[64] This case could be interpreted to mean that any cyber operation that coercively impacts these areas amounts to an internationally wrongful act.

There are limits to broadly applying the *Nicaragua* case to cyber operations. One limitation of the *Nicaragua* case was that the court specifically defined the non-intervention principle only in terms "relevant to the resolution of the dispute."[65] The facts of the case involved economic, logistic and direction to armed rebels engaged in attempts to overthrow the government of Nicaragua. A strong statement of the existence of a law of non-intervention, the *Nicaragua* case is persuasive precedent for the broader application to cyber operations.

The *Nicaragua* case is not the only support for a broad international law of non-intervention. Beyond the *Nicaragua* case is the *United Nations Declaration of Principles of International Law Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations* ("UN Declaration of Friendly Relations).[66] This declaration documented a mixture of duties and rights related to non-interference which

---

[61] 1986 ICJ Reports 14.
[62] *Ibid.*, para. 202.
[63] *Ibid.*, para. 205.
[64] *Ibid.*
[65] *Ibid*.
[66] General Assembly resolution 2625.

are relevant to cyber operations. Relevant duties include not to intervene in the "domestic jurisdiction" of a state, to respect human rights and fundamental freedoms, and to conduct international relations in accordance with the "principles of sovereign equality and non-intervention." The Declaration also sets out an "inalienable right" to choose political, economic, social and cultural systems without interference from other states.

These issues are not academic. Well publicized cyber operations have impacted a wide range of areas that could be seen to contravene international laws against non-intervention. Interference and influence activities occurred with both the Ukrainian and United States leadership elections, in addition to cyber operations that disabled three Ukrainian power plants between 2014 and 2016.[67] Sophisticated ransomware like WannaCry and NotPetya caused massive disruptions in 2017 to computers, including government infrastructure. Ironically, WannaCry allegedly utilized a security vulnerability in Windows software that a United States security agency had developed and had stolen.[68] Aside from the disruption caused, this incident raised questions around the responsibility of security agencies in capability development and duties owed to their own citizens and corporations.

In the cyber domain, laws with respect to non-intervention create significant challenges in determining the permissible avenues of state practice. To classify a cyber operation as an unlawful intervention, it must exercise coercion against an outcome that a State has a sovereign right to control. Coercion may commonly manifest itself as a cyber

[67] Dan Tynan, "Cyberwar is not coming to the US – it's already here," *Guardian*, "4 August 2016.
[68] Josh Fruhlinger, "What is a cyber attack? Recent examples show disturbing trends," *Network Asia* 11 March 2018.

operation intended to force the victim State to change policy.[69] This concept of an internationally wrongful act is separate and distinct from a use of force.

Use of Force

The second type of internationally wrongful act is a use of force. The Tallinn Manual 2.0 set out that any cyber operation is unlawful if it constitutes a threat or actual use of force against the territorial integrity or political independence of a state, or is otherwise inconsistent with the purposes of the United Nations.[70] This rule reflected the long standing customary international law surrounding article 2(4) of the United Nations Charter, that nations ought to refrain from the threat or actual use of force against other nations.[71] The Tallinn Manual 2.0 went on to define that a use of force for a cyber operation occurs when "…its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[72] Although seemingly straightforward, this analysis poses certain challenges because cyber operations are inherently non-kinetic.[73] Historically, all measures of use of force were done in a kinetic effects spectrum from physically pushing another person, up to dropping a bomb to cause a nuclear explosion. In the cyber domain kinetic and non-kinetic effects can be delivered in ways that would not traditionally be viewed as a use of force.[74] Questions then arise when determining whether cyber effects meet the use of force legal threshold.

---

[69] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict & Security Law* 17 No. 2 (2012): 224.
[70] Tallinn Manual…, 329.
[71] Schmitt, *Quo Vadis*…, 279.
[72] Tallinn Manual…, 330.
[73] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* 56, no. 3 (2011): 573.
[74] Hrafn Steiner, "Cyber Operations, Legal Rules and State Practice – Authority and Control in International Humanitarian Law," (master's thesis, Stockholm University Faculty of Law, 2017), 49.

Cyber operations that deliver analogous kinetic damage such as destruction of property, injury or death will clearly be considered a use of force under international law, as described in Rule 69 of the Tallinn Manual 2.0.[75] However, decisions of the International Court of Justice have been seen to support the idea that cyber operations rendering significant, although non-kinetic effects, could amount to a use of force.[76] Proposed principles can assist in predicting whether a non-kinetic cyber operation amounts to a use of force.[77] These principles include severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy. In these situations, development of state practice on what cyber operations rise to the level of a use of force remain unclear.

Several other important considerations flow from international law pertaining to the use of force. The first is that a use of force should not be confused with an armed attack. A state subject to a use of force is generally not permitted to reply in kind.[78] The term "armed attack" is the threshold that invokes the states right to use force in response. Second, the article 2(4) United Nations Charter prohibition on the use of force only applies to states. Therefore, non-state actors who are not considered to be acting on behalf of a state cannot violate these use of force prohibitions.[79] This consideration is key when discussing the different responses available to address state versus non-state actors. Finally, the present context of use of force analysis in international law does not include

---

[75] Schmitt, *Jus Ad Bellum Revisited*…, 573.
[76] Schmitt, *Quo Vadis*…, 280. See *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Merits, Judgement, I.C.J. Reports 1986.
[77] Michael N. Schmitt, "Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework," *Institute for Information Technology Applications*, Research Publication 1 (June 1999): 18.
[78] Schmitt, *Jus Ad Bellum Revisited*…, 574.
[79] *Ibid.*, 578. Note however, Tallinn Manual…, 345 Note 18, which discussed the post 9/11 position of whether non-state actors can perpetrate an armed attack.

pressures of a political or economic nature, nor does it include acts of espionage.[80] Cyber operations that aim their effects in these areas have not traditionally been viewed as a use of force. These factors need to be considered to determine what response options are considered lawful.

Internationally Lawful Peacetime Cyber Responses

States subject to an internationally wrongful act from a use of force or a violation of non-intervention can utilize retorsion, seek reparations or engage in countermeasures. Retorsion is a lawful, but unfriendly State action.[81] Such actions may include trade sanctions and expelling or withdrawing diplomats. Reparations consist of either monetary or other compensation, attempts to make right the damage done or obtain a public apology from the responsible state. [82] The victim state may also take countermeasures.[83] The range of responses provide increasingly strong options for states to manage hostile cyber operations. Countermeasures provide the strongest response option.

Countermeasures are essentially actions that would otherwise be unlawful but for the internationally wrongful act and do not rise to the level of a use of force. They are designed to induce the state to comply with its obligations. Attempting to disable the command and control of certain types of cyber operations would be an example of a countermeasure, a practice known as "hacking back."[84] There are numerous restraints and constraints on the use of countermeasures, such as having to protect fundamental human rights and respecting the inviolability of diplomatic and consular agents. Yet

---

[80] *Ibid.*, 576; Gary Brown, "Spying and Fighting in Cyberspace: What is Which?" *Journal of National Security Law Policy* 8 (2016): 2.
[81] Schmitt, *Jus Ad Bellum Revisited*…, 582.
[82] United Nations General Assembly, *Responsibility of States*…, 8. These reparations can be restitution, compensation and satisfaction detailed in articles 35 to 37.
[83] *Ibid.*, 11.
[84] Corey T. Holzer, "The Ethics of Hacking Back," *The Center for Education and Research in Information Assurance and Security* 1 (2016): 3.

countermeasures could prove a useful means to address hostile cyber operations.[85] These response options are lawfully available to only states.

An emerging issue in this area is availability of countermeasures to non-state actors, specifically large corporations. The availability of corporate hack back options for victims of cyber operations that steal intellectual property or impair corporate operations has generated significant discussions in the United States.[86] Strictly speaking, countermeasures under international law are only available to nation states, but the execution can be delegated.[87] In any context, attribution continues to be a critical factor to contend with. If the perpetrator's identity remains unknown, a state cannot determine whether countermeasures are lawfully conducted against another state. In the Canadian context, the ability to utilize countermeasures will likely hinge on the applicability of domestic legislation and the *Canadian Charter of Rights and Freedoms* (*Charter*).[88] Specifically, whether a defence or security agency is legally entitled to utilize countermeasures remains a significant issue. What, if any, domestic law governs the methods and means of using countermeasure remains to be determined.

The nature, extent and impact of a hostile cyber operation influence whether it rises to the level of a use of force. International law defines a nation's right to self-defence. The use of the term "self-defence" in this context must not be confused with its use in the domestic law or colloquial sense. Although similar hack back techniques may be used by individuals, industry and government, the legal context changes how these may be viewed.

---

[85] Schmitt, *Jus Ad Bellum Revisited*…, 582.
[86] Holzer, *Ethics of Hacking Back*…, 3.
[87] Michael Schmitt, "International Law and Cyber Attacks: Sony v. North Korea," *Just Security* (2014), 5.
[88] *Canadian Charter of Rights and Freedoms*, part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11.

Self-Defence

The bright line rule in international law that may transition normal inter-state relations into an armed conflict is the notion of an "armed attack." Article 51 of the United Nations Charter allows a State to respond with force in "self-defence" only in the face of an armed attack.[89] Therefore, to understand the international law concept of self-defence, understanding what constitutes an armed attack in the cyber context is crucial.

Various factors inform this effects-based analysis. The Tallinn Manual 2.0 sets out that a cyber operation can constitute an armed attack depending on its scale and effects.[90] Currently, the customary international law of self-defence likely does not justify non-physically destructive or non-injurious cyber operations as armed attacks.[91] However, both the United States and the Netherlands have made it clear that cyber operations that cause interference with serious state functions like financial systems or military systems would likely qualify.[92] Canada has yet to clarify its position in this regard and state practice will evolve the customary international law.

Armed Conflict

The significance of defining the effects of a given cyber operation becomes clearer when one understands that if defined as an armed attack the legal paradigm could shift. Specifically, the cyber operation can transition from peacetime international law into LOAC. However, simply defining a cyber operation as an armed attack is not the single trigger to transition to LOAC. Yet, for security leaders it is imperative to

---

[89] *UN Charter*, Art. 51.
[90] Tallinn Manual…, 339. See rule 71.
[91] Schmitt, *Quo Vadis*…, 283.
[92] *Ibid*.

understand these distinctions because state practice in this area continues to be defined, which means potential unpredictability when cyber effects are not strictly controlled.

A single cyber event, even one deemed an armed attack does not itself trigger an armed conflict. Before LOAC can be applied, there must exist a state of armed conflict.[93] Although seemingly a trite statement, in the context of cyber operations and the use of force it raises some unique issues. A state of armed conflict involves some form of hostilities that apply the means and methods of warfare.[94] However, the international group of experts failed to reach accord on the issue of duration or intensity of hostilities that would amount to an armed conflict.[95] This lack of consensus means divided opinion whether a single or smaller scale cyber armed attack could trigger a state of armed conflict or not. Ultimately determining an event meets the armed attack threshold is a political decision for state leaders, policy makers and perhaps legislative assemblies.

Distinction between an international armed conflict and a non-international armed conflict essentially depends upon the conflict occurring between two states or a state and an "organized armed group" internal to that state.[96] Also, "armed" conflict does not necessitate a requirement that armed forces be engaged in the hostilities.[97] This law has impact on cyber operations as civilian agencies could engage in actions that amount to armed attacks, which in turn could trigger armed conflicts. Unresolved issues of states'

---

[93] Tallinn Manual…, 375. See Note 111; Common Article 2 , *Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva Convention (III) relative to the Treatment of Prisoners of War, Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War*, opened for signature 12 August 1949, 75 UNTS 31, 85, 135, 287 (entered into force on 21 October 1950), (collectively, *1949 Geneva Conventions*).
[94] Schmitt, *Quo Vadis*…, 290.
[95] Tallinn Manual…, 383. See Note 112.
[96] Tallinn Manual…, 385; *1949 Geneva Conventions*…, Common Article 3
[97] Tallinn Manual…, 384. See Note 14.

use of civilians in cyber combat operations remain.[98] These issues include questions of how close a nexus is necessary for civilian cyber operations to become attributable to their governments. Russian "troll factories" provide a concrete example.[99]

Distinction principles also raise issues of non-state actors who engage in cyber operations that amount to an armed attack. For example, if the activist group "Anonymous" disabled the New York Stock Exchange, would the United States government treat it as a criminal act or as the latest in a series of armed attacks from this cyber non-state actor? Current views are that in most cases, cyber activist groups would not meet the customary international law definition of "organized" nor would the degree of destruction or lethality meet the degree of intensity required to rise to the level of an non-international armed conflict.[100] On an effects-based analysis, traditional views of intensity involve questions of destruction and lethality which the disruption of services, even on the scale of a stock exchange, would not meet. Similarly, isolated groups of hackers working towards a common purpose do not meet traditional evaluations of command and control and uniforms, nor does malicious code meet current understandings of the term armed. However, these examples demonstrate areas where state practice will be potentially determined in the years to come.

Military leaders conducting operations under LOAC are familiar with the principles that guide the application of force during conflict. Residing in these principles are proportionality, distinction, necessity and the review of the weapons to avoid

---

[98] Christopher E. Bailey, "Cyber Civilians as Combatants," *International and Comparative Law Journal* 8, no. 1 (2017): 5; Jake B. Sher, "Anonymous Armies: Modern 'Cyber-Combatants' and Their Prospective Rights Under International Humanitarian Law," *Pace International Law Review* 28 (2016): 265.
[99] Alexander Panetta, "Russian troll factory also went after Canadian targets including oil, Justin Trudeau," *The Canadian Press*, 18 March 2018.
[100] Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Anallytical *Vade Mecum*," *Harvard National Security Journal* Vol. 8 (2017): 263.

unnecessary suffering. These factors are essentially the same whether an international or non-international armed conflict.[101] LOAC principles apply in conducting operations in the cyber domain, although each raises its own unique challenges given the nature of cyberspace.

Attacks, Distinction and Proportionality

Among the first challenges presented in applying LOAC to cyber operations is the definition of "attack." The term attack in the cyber context is difficult to apply to the traditional legal threshold of an armed attack in determining when a state can respond in national self-defence. Defined in Additional Protocol I of the Geneva Conventions, an attack is either an offensive or defensive act of violence against an adversary.[102] There is some traditional disagreement as to exactly what constitutes an attack in the conventional sense, revolving around the inclusion of operations such psychological or economic warfare like propaganda and embargoes.[103] The definition of attack applied to cyber operations is less settled, except where consensus exists with respect to operations resulting in death, injury or physical damage to objects are attacks.[104] The Tallinn Manual 2.0 also took the position that loss of infrastructure functionality is damage in terms of determining whether a cyber operation meets the legal threshold of attack.[105] It is through this effects-based analysis that the customary international law may evolve. Using the loss of infrastructure functionality as a measure of cyber effects means that the loss of a stock exchange could meet the definition of an armed attack. Whether the stock exchange

---

[101] Schmitt, *Vade Mecum*…, 263.
[102] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of victims of Inernational Armed Conflicts, art. 49(1), June 8, 1977, UN Doc A/32/144. (*Additional Protocol I*)
[103] Ido Kilovaty, "Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under International Humanitaran Law," Michigan Telecommunications and Technology Law Review 23 (2016): 117.
[104] Schmitt, *Vade Mecum*…,, 266.
[105] Schmitt, *Vade Mecum*…, 266.

example met the armed attack threshold would be an executive political decision for state leaders, policy makers or legislative assemblies to make.

If a cyber operation meets the definition of an armed attack it is subject to further LOAC analysis including the principle of distinction. This rule is in place to ensure civilians are accorded as much protection as possible during armed conflicts. The rule focuses on distinguishing civilian populations from combatants and military objectives and civilian objects.[106] Although the rule is well understood, its application in the cyber domain is full of unresolved issues.

Military distinction challenges are caused by a domain that is entirely artificial and whose logical and physical levels are largely held and managed by multi-national corporate ownership. Distinguishing civilian cyber infrastructure from valid military objectives requires a nuanced and contextual analysis.[107] Any object by their "nature, location, purpose or use," making effective contribution to military action is a viable target under LOAC.[108] As with all methods of warfare, conduct of cyber operations must be focussed on valid military objectives. Significant practical issues present themselves when applying cyber operations to data, infrastructure with both civilian and military uses and questions about war-supporting objectives.[109] Connected to the legal requirements to distinguish targeting civilian from military objects, is the capability of weapons to do the same.

Principles of distinction also pertain to weapons assessments. Like the methods of warfare, the means of warfare require legal analysis. Cyber weapons, like all weapons

---

[106] *Additional Protocol I*…, art. 48.
[107] Schmitt, *Vade Mecum*…, 268.
[108] *Additional Protocol I*…, art. 52(2).
[109] Schmitt, *Vade Mecum*…, 269.

deemed lawful to use in armed conflict must conform to rules to avoid unnecessary suffering and civilian casualties. Pursuant to Additional Protocol I, countries are required to conduct a legal assessment of all weapons used in armed conflict.[110] Care must be taken to ensure that the use of malware has sufficient targeting criteria to ensure it does not contravene international law by not being capable of sufficient distinction between civilian and military targets.[111] The Stuxnet virus if employed during an armed conflict, would likely have met the requirements of distinction.[112] Although widely disseminated throughout cyberspace, the virus utilized specific technical targeting criteria that sufficiently distinguished its intended military target, a nuclear reactor in Iran from other civilian infrastructure. Issues of distinction go beyond just infrastructure and hardware.

Another key distinction issue involves the increasing difficulty differentiating combatants from civilians. It has long been settled that civilians who accompany armed forces such as members of air crews, contractors, labourers and war correspondents have been granted combatant status.[113] In a modern context, civilians working to enable military cyber operations may be considered combatants. In Canada the CSE is a civilian establishment that has significant links in supporting military operations. CSIS agents are also civilian intelligence officers who also have a legislated role to play in supporting military operations domestically and abroad. Both agencies have cyber operations capabilities. Even the latest Defence Policy, *Strong, Secure, Engaged* cites the utilization of civilian cyber operators and increased role for reserve CAF members to engage in

---

[110] *Additional Protocol I*…, art. 36.
[111] Schmitt, *Vade Mecum*…, 265.
[112] Kilovaty, *Cyber Ops*…, 137.
[113] *1949 Geneva Conventions*…, Common Article 4.

cyber operations.[114] The question of whether any or all of these "cyber civilians" qualify as combatants is still unresolved.[115] These considerations are important for civilian public servants since cyber operations in an armed conflict can be responded to through traditional kinetic means. Further questions relate to when a civilian cyber operator remains a combatant? Is it only when they are at work they remain combatants or can the enemy state target these operators at home when not directly engaged in hostilities? Civilians do not accept the military terms of unlimited liability as a condition of their employment yet could unwittingly be targeted as if they had. The analysis does not stop there from a Canadian perspective.

Another aspect of the combatant issue comes from Canada being a signatory to Additional Protocol I. Article 43 stipulates that members of the armed forces include any groups and units under a command that is responsible for their conduct, as well as paramilitary and armed law enforcement agencies.[116] There is growing support that in using these definitions, civilian cyber operators can have international legal obligations imposed upon them if they are operating in support of parties to an armed conflict.[117] These principles stand for the proposition that civilian intelligence officers such as CSE or CSIS and armed law enforcement such as the RCMP could be deemed combatants pursuant to article 43. Arguably, responsible command is an even wider standard for inclusion than accompanying the armed force. To apply these standards would require a blending of attribution and effects-based analysis. Essentially, for the lawful targeting of a civilian cyber operator, the enemy would have to assess that an effect was making an

---

[114] Department of National Defence, *Strong, Secure, Engaged Canada's Defence Policy* (Ottawa: Minister of National Defence, 2017), 69.
[115] Bailey, *Cyber Combatants*…, 11.
[116] *Additional Protocol I*…, art. 43.
[117] Bailey, *Cyber Combatants*…, 13.

effective contribution or participation to hostilities and then attribute that effect to the civilian. Issues of distinction are separate from consideration of issues surrounding proportionality.

Further protection is afforded civilians under LOAC through the principle of proportionality. This principle recognizes that despite other rules of war being applied, incidental loss of civilian life, injury or damage to civilian objects can still occur. To minimize this incidental damage, the proportionality principle states that an attack is prohibited if the incidental civilian damage would be "excessive in relation to the concrete and direct military advantage anticipated."[118] This principle again engages an effects-based analysis at the time of the anticipated incidental civilian damage.

In the cyber domain, application of the proportionality principle is oftentimes difficult. Issues include measuring collateral civilian damage, and even understanding what constitutes damage in a cyber sense. Practical issues include the difficulty to control the overall spread of malware directed at otherwise legitimate military objectives and understanding whether a serious disruption in cyberspace constitutes damage.[119] The malevolent use of the government developed WannaCry virus could serve as a specific example. The loss of civilian cyber infrastructure function would likely qualify as collateral damage.[120] Combining difficult to control cyber weapons with difficult to measure effects makes application of the proportionality principle difficult to quantify. While proportionality is another effects-based determination, the requirement that the effects be measured against civilians and civilian infrastructure includes aspects of attribution.

---

[118] *Additional Protocol I*…, art. 51(5)(b).
[119] Kilovaty, *Cyber Ops*…, 122.
[120] Schmitt, *Vade Mecum*…, 277.

In many cases, cyber attacks may be exponentially less damaging to civilian infrastructure than conventional munitions. Examples that have been cited are neutralizing air defence systems or disrupting resupply by sea through cyber means.[121] These examples highlight new ways of viewing collateral damage estimates and highlight the anticipatory nature of the proportionality principle. It is not the actual collateral damage that is ultimately determinative, but that which was reasonably anticipated.[122] Applying a "functionality" approach to cyber collateral damage would include a loss of system functionality in the collateral damage assessment.[123] CAF cyber operators therefore need to anticipate a wider range of potential collateral damage. For example, malware utilized to target air defence communication, cyber operators would need to anticipate even temporary loss of wider communications for the civilian population.

Effects-Based Analysis

Current international law offers some logical conclusions for cyber operations from a Canadian perspective. It is reasonable to predict that for Canada to interpret a given cyber operation as an armed attack, the potential effect to critical Canadian infrastructure or people would have to be very significant. LOAC manages the introduction of cyber warfare as simply the latest in a long line of technical evolutions in warfare.[124] Leaders in cyber security understand that most cyber operations fall under peacetime international law, domestic law or both. A reasonable international legal framework exists that will guide political and operational decisions for hostile cyber

---

[121] *Ibid.*
[122] *Ibid.*, 278.
[123] Kilovaty, *Cyber Ops*..., 139.
[124] Schmitt, *Quo Vadis*…, 289.

operations deemed internationally wrongful acts or armed attacks triggering the two international legal regimes.

Overall, most legal thresholds in international law applicable to cyber operations are effects-based. Effects matter whether determining an internationally wrongful act through use of force or violation of sovereignty, an armed attack or collateral damage has occurred. Generally, the greater the damage or disruption, the higher the level of response permitted. A primary focus on effects should not be understood to preclude important attribution-based assessments such as identifying lawful combatants or weapons assessments as to whether the malware can distinguish friend from foe. Importantly, the key determinants of what international legal regime will apply is based largely on the evaluation of cyber operation effects, usually focussed on the extent of the disruption or damage.

Finally, many international cyber operations mounted by Canadian security agencies will emanate from secure locations within Canada. These domestically-based operations raise issues not normally seen before. Traditionally, police, spies and soldiers embarked on Canadian missions abroad meant physical location outside of Canada. Historically, soldiers creating effects in foreign countries were either under LOAC or operating with host nation consent. Spies and police operating abroad did so subject to the foreign country's domestic laws. Due to these practicalities, Canadian domestic law did not normally apply to these operations through the legal concept of comity and the principles behind sovereignty. No longer the case with cyber operations, the question of domestic law applicability, even to international operations, becomes relevant to all Canadian security agencies.

Canadian Domestic Law

Given Canada's geographic size and diversity of political leadership at the national, provincial, and municipal levels, an equally large and diverse amount of domestic law exists. The federal government has taken the lead on updating legislation related to cyber operations, including the *Criminal Code* and some of the mandating legislation for Canadian security agencies operating in cyberspace. Although significant cyber operations are regulated through federal legislation, it would be a mistake to discount provincial and municipal efforts.

Nova Scotia was the first and only province to pass cyber-bullying legislation. In October 2017, the Nova Scotia Legislature passed the *Intimate images and Cyber-protection Act* which is awaiting royal assent. This act updated the first attempt by the Nova Scotia government to address the public outcry at the suicide of Rehtaeh Parsons through the *Cyber Safety Act*. The *Cyber Safety Act* was struck down as unconstitutional by the Nova Scotia Supreme Court.[125] The goal of the legislation was to provide alternatives to a civil suit for defamation and options for justice to victims of cyberbullying.[126] Attribution issues were central to one of the successful constitutional arguments.[127] To deal with the constitutional attribution issues, the new act allows for identification of the respondent by IP address, and other persona.[128] The new act allows for the Minister of Justice for Nova Scotia to establish an agency that among other things,

---

[125] 2015 NSSC 340.
[126] *Crouch v. Snell* 2015 NSSC 340, para. 141.
[127] *Ibid.*, para. 152.
[128] Bill No. 27, *An Act Respecting the Unauthorized Distribution of Intimate Images and Cyber-protection Act*, 1st s. 5(4).

provides support and assistance to victims of cyber-bullying and provide public information and education regarding harmful on-line conduct.[129]

In addition to Nova Scotia's efforts, many provincial and municipal security agencies are working to develop cyber operations capabilities. Some agencies, such as the Calgary Police Service and Toronto Police Service already have significantly advanced cyber operations capabilities in furtherance of local law enforcement mandates. Any effort by the federal government security agencies to coordinate cyber security operations would be well served by including select provincial and municipal organizations in planning and operational coordination efforts. These provincial and municipal agencies conceivably fall under the CCSS but are not often considered when analysing a federal cyber security strategy.

The CCSS has taken a largely effects-based approach to defining the roles of Canada's security agencies in cyber operations. Specifically, the strategy addresses the roles of the four main security agencies in terms of effects.[130] The strategy does not speak to attribution and instead bases jurisdiction on recognizing the effect of the cyber operations as a threat against Government networks, a threat to the security of Canada, a crime or a matter of national defence. As the Horizontal Evaluation revealed, key cyber security agencies are struggling with developing redundant capabilities, a lack of information sharing and confused, overlapping jurisdictional issues. Understanding enabling legislation and the mandated jurisdictions for each agency is the first step to untangling the issue and moving forward in a cohesive way.

---

[129] *Ibid.*, s. 12.
[130] Government of Canada, *Cyber Security Strategy*…, 10.

Application of Canadian domestic law to cyber operations has been largely left to each defence and security agency to work through and apply in traditional areas of responsibility. These areas of responsibility are set out in the respective enabling legislation. Attribution and not effects are the predominant factor that has traditionally defined each agency's jurisdiction over a given incident.

Mandating Legislation – Defence, Intelligence, Law Enforcement

The four main security agencies engaged in cyber operations owe their existence to three federal acts. Generally, these agencies are mandated with national defence, foreign signals intelligence, threats to national security and the prevention and detection of crimes. Available cyber operations policies revealed significantly overlapping views of jurisdiction. These attempts to meet the CCSS through defining the focus of their cyber operations through effects-based analysis revealed the overlap of jurisdiction. Equally important are cyber operations that may not be caught by any agency's jurisdiction. Examining the mandating legislation for each agency provides the legal basis for jurisdictional determinations, including in the cyber domain.

The first legislation examined is the *National Defence Act*. ("*NDA*")[131] Under this act the Minister of National Defence is charged with "…all matters relating to national defence…" and is responsible for the creation and maintenance of defence establishments and research related to the defence of Canada.[132] The statute allows the Minister to organize the CAF in to various commands, formations, units and other elements. The commands include the Royal Canadian Navy, the Canadian Army, the Royal Canadian Air Force and the Canadian Special Forces.

---

[131] RSC 1985, c N-5.
[132] *Ibid.,* s. 4.

Unlike the United States, Canada has not developed a cyber command to date. Instead, the CAF rely on the joint task force model and interdepartmental bodies on the policy side, to manage cyber operations in its defence of Canada mandate. Added to their capacity is the CSE. The legislative basis for CSE, an organization dating from the early days of the Cold War, resides in Part V.1 *NDA*. As a statutory agency, the provisions of the *NDA* provide an understanding of its mandate and the legal powers it can utilize to fulfill that mandate.

The CSE has a widely defined purpose. The primary mandate of the CSE is to utilize "the global information infrastructure" to gather foreign intelligence, protect electronic information and infrastructure, and provide assistance to federal law enforcement and security agencies.[133] Unlike the other statutory security agencies, the CSE does not have its own act, but is aligned under the Minister of National Defence.[134] The agency is headed by a Chief who is statutorily responsible for the management and control of the CSE.[135] This position, at least in recent times, has been staffed with senior career civilian bureaucrats.[136] The relationship between the RCMP and CSIS is defined as one of CSE support to those agencies when formally requested and within the bounds of existing laws on privacy respecting the collection of information against Canadian citizens. The relationship with the CAF is much different.

The Minister of National Defence can authorize the CSE to intercept private communications to acquire foreign intelligence or protect Government of Canada computer systems. The Minister of National Defence can direct the CAF to "support" the

---

[133] *Ibid.*, s. 273.64(1).
[134] *Ibid.,* s. 273.61.
[135] *Ibid.,* s. 273.62(2).
[136] Chris Madsen, *Military Law and Operations* (Toronto: Carswell, 2017), 29, para. 3:20.100.

CSE in carrying out those activities.[137] This provision places the CAF in a unique relationship with the CSE. Specifically, it allows the Government of Canada to utilize armed forces to support its foreign intelligence collection and defence of its computer systems.

What cyber operations matter to national defence? Traditionally, defining an operation that related to national defence has not posed much of a problem. Canadian troops have been mandated by the Government of Canada to engage in the application of coercive force to achieve national objectives. The military is normally a means of last resort and "their raison d'etre remains armed conflict."[138] When faced with large scale armed threats to national interests, questions of jurisdiction are obvious. Many nations decide military deployments based on these types of existential threats. Yet in Canada, military deployments have been traditionally decided by questions of who and where. Canada, by geography, has largely been exempt from existential threats. Therefore, an effects-based analysis related to how capable or grave the threat posed although a factor is not decisive. The Canadian government routinely decides CAF commitments based on who is involved and where the conflict is unfolding. Arguably, decisions to deploy the CAF or not in Kosovo, Libya, Afghanistan, both Iraq wars, and most recently Mali were not decided on the threat posed to Canada. Instead, government policy and international politics informed by who was involved in the conflict and where it was taking place were deciding factors in CAF deployments. In domestic deployments, the CAF invariably are subject to the jurisdiction of a requesting provincial or federal agency. Closely aligned with a defence of Canada mandate is the national security mandate of CSIS.

---

[137] *NDA…,* s. 273.65(6).
[138] Department of National Defence, B-GJ-005-000/FP-001, *Canadian Military Doctrine* (Ottawa: DND Canada, 2009), 2-2.

Focused on threats to national security, CSIS was born from a desire to separate national security intelligence from law enforcement after an embarrassing commission of inquiry into RCMP activities and allegations of illegalities. CSIS receives its legal authorities through the *Canadian Security Intelligence Services Act* ("*CSIS Act*").[139] This act defines the duties and functions of CSIS in s. 12 to collect, analyze and retain "information and intelligence" that on a legal standard of reasonable suspicion constitute "threats to the security of Canada." The act specifically defined these threats as including espionage or sabotage; clandestine, deceptive or threatening foreign influenced activities that are detrimental to the interests of Canada; activities that involve the threat or actual violence against people or property for political, religious or ideological objectives; and activities that are directed toward the destruction or violent overthrow of the constitutionally established system of government in Canada.[140] The statutory limit on the collection of intelligence is only "…to the extent that it is strictly necessary…."[141] CSIS has statutory authority to operate domestically and outside Canada. These statutory powers establish jurisdiction for CSIS to investigate a wide range of threats to national security including those of both domestic and foreign origin.

The *CSIS Act* also provides CSIS agents the freedom to operate within Canada and abroad. Traditionally CSIS was designed as a domestic information and intelligence gathering agency only.[142] However, in 2015, CSIS received significant new authorities to take "measures, within or outside Canada, to reduce the threat."[143] The *CSIS Act* does not include a definition of "measures." However, it does set the legal standard of reasonable

---

[139] R.S.C., 1985, c. C-23.
[140] *Ibid.,* s. 2.
[141] *Ibid.*, s. 12.
[142] *RE: CSIS Warrants – Metadata,* [2016] FC 1105, para. 137.
[143] *CSIS Act*…, s. 12.1.

grounds to believe that the "particular activity constitutes a threat to the security of Canada." With the addition of new threat reduction measures the lines between CSIS acting domestically and traditional National Security law enforcement with the RCMP have become blurred. In 2008 the Supreme Court of Canada noted the convergence of RCMP and CSIS activities[144] The increasing convergence requires improved communication between the two agencies to prevent redundant or cross-purposed operations.

Notwithstanding these new powers, the Federal Court in 2016 reaffirmed CSIS's essential function as the investigation of threats to the security of Canada, and made it clear they are not a law enforcement agency.[145] Concerns about intelligence collection methods and the purposes to which it is used prompted the *One Vision 2.0* document.[146] The document represented a formal agreement between CSIS and the RCMP to engage in structured cooperation recognizing the challenges associated with utilizing national security intelligence as evidence in prosecutions. The agreement also mandated clear consultation when CSIS utilized their new powers in taking "threat reduction activities."[147] *One Vision 2.0* is evidence of the challenges inherent in overlapping jurisdictions.

Like the CAF and CSE, CSIS has an attribution-based analysis to determine jurisdiction. Looking at the CSIS mandate, terrorism, espionage, sedition or treason all require an attribution analysis. The threat will be determined by the who, where and why

---

[144] *Charkaoui v. Canada* [2008] 2 SCR 326, 341.
[145] *RE: CSIS Metadata*…, para. 160.
[146] Canadian Security Intelligence Agency, "CSIS-RCMP Framework for Cooperation One Vision 2.0, 10 November 2015," Access to Information Request Number 117-2015-645 – Documents Related to Frameworks for Cooperation with Key Government Partners (July 2016).
[147] *Ibid.*, 3.

on a standard of reasonable suspicion before CSIS can establish jurisdiction. Intelligence that an unknown person will commit a heinous effect in another country will generally preclude CSIS jurisdiction. Information that a person is planning violence or destruction in Canada will normally be a police responsibility. What usually establishes CSIS jurisdiction is the added information that the person is acting on behalf of a foreign power, for religious, political or other ideological reasons. These qualifiers involve questions of attribution. The extent of damage the person intends to do is not a determinative factor in whether CSIS engages.

A similar but far simpler attribution analysis takes place to establish law enforcement jurisdiction. In the cyber domain, the scope of the *RCMP Cybercrime Strategy* outlines the wide array of actions that attract law enforcement attention and potential criminal sanction. The *Cybercrime Strategy* roots RCMP mandate in the *Royal Canadian Mounted Police Act* section 18 that describes the duties of peace officers to include:

> …preservation of the peace, the prevention of crime and of offences against the laws of Canada and the laws in force in any province….and the apprehension of criminals and offenders and others who may be lawfully taken into custody."[148]

From this authority the RCMP sees itself as:

> …the only federal organization with the mandate and authority to investigate criminal offences related to cybercrime, such as those targeting government systems and networks or other critical infrastructure sectors.[149]

Legislatively, the RCMP establishes jurisdiction based largely on geography. Any incident that breaches a domestic law of Canada establishes *prima facia* jurisdictional authority to investigate that crime. The attribution question is simply one of where the effect occurred. Questions of who and why may be of interest, but not legally

---

[148] *Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10.
[149] RCMP, *Cybercrime Strategy*…, 8.

determinative of jurisdiction. Similarly, how great or small the disruption or damage effect from the cyber operation is of no consequence to the jurisdictional analysis. By legislative design, the RCMP has very wide jurisdictional mandates. The RCMP or other police of jurisdiction manage the majority of cyber operations impacting Canadian security, largely by default. Due to capacity, little further attribution or effects analysis are being conducted on most of these incidents. The RCMP Cybercrime Strategy recognizes the inherent technical attribution challenges. The complexity and transnational character of these cyber operations makes evidence transient and dispersed throughout multiple jurisdictions.[150] Like the other defence and security agencies, it is difficult for the RCMP to identify a cybercrime based only on its effects.

Significant overlap of security agencies jurisdictions exists in responding to and conducting cyber operations. This overlap is not necessarily a bad thing. To function effectively, overlapping jurisdictions require enhanced coordination and clear communication. The CCSS has the objective of such coordination and communication but based on knowing that a given cyber effect is a crime, espionage, impacting a government system or an act of war. Examining the mandating legislation, it becomes apparent how traditional means of establishing jurisdiction become difficult when applied to cyberspace.

Many examples exist of overlapping jurisdictions. Both the RCMP and CSE assert jurisdictions pertaining to government systems and networks. In intelligence gathering, the CSE, CAF, CSIS and RCMP all reasonably engage in investigating and developing cyber capabilities to protect "government IT systems." CSIS is specifically mandated with the collection of information in relation to the defence of Canada, a clear

[150] RCMP, *Cybercrime Strategy*…, 6.

overlap with the CAF.[151] The CAF, by interpreting most cyber operation in terms of their defence of Canada mandate, fails to recognize concurrent or wider police jurisdiction. Any number of hostile cyber operations may be interpreted as a threat to Canada that attracts CAF, CSIS and RCMP attention. With the majority of hostile cyber operations being reported as crimes based on the expansive jurisdiction given to the RCMP, it becomes very difficult to determine if theft of data is a true domestic crime or an act of foreign espionage or a prelude to war.

Added to the jurisdictional questions, is the possibility that three separate legal regimes may be applied to cyber operations resulting in further difficulties. The CAF, CSE or CSIS have no legislative mandate to conduct law enforcement. Cyber operations experienced by those agencies will therefore not normally be interpreted as crimes. Similarly, the average RCMP officer knows very little about LOAC, as most police officers do not work in that legal regime. Combining these complex considerations exemplifies why a more unified approach to cyber operations is necessary.

For a comprehensive approach to cyber operations to be effective, a balanced attribution and effects-based analysis mechanism would be required. Ideally, the analysis encompasses the range of operational leadership from the four main cyber security agencies who each bring a unique skill set and perspective. Collaboratively, both legal regime and domestic jurisdiction could be effectively established. More than one defence or security agency has jurisdiction and the interests of Canada would best be served by pursuing a joint operation. Alternately, multiple agencies could be tasked with pursuing different aspects of the same threat down separate lines of operation, but centrally coordinated. In the case of proactive or offensive cyber operations, a consistent

[151] *CSIS Act*…, s. 16.

evaluation of attribution and assessment of effects maintains consistency across the full spectrum of national cyber operations. As comprehensive as a coordinated effects and attribution analysis would be, it is still missing one component, political will.

Political Will

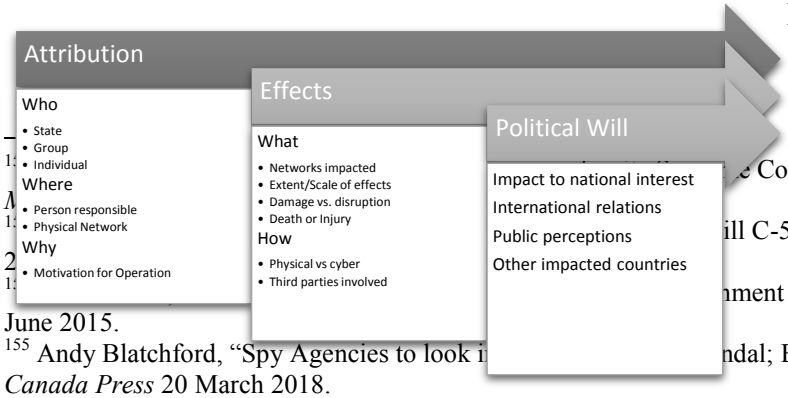
Legal analysis of cyber operations shows that three possible legal regimes apply to cyber operations conducted by Canadian security agencies: peacetime international law, LOAC, and domestic law. Within Canadian domestic law, a cyber operation may be within the jurisdiction of one or more security agencies. Currently in the cyber domain no clear lines delineate when each of these legal regimes are engaged. Two factors, attribution and effects, are central to the determination of what legal regime applies to any Canadian cyber operation. However, a third important factor of "political will" is implicit when examining the law and policy around cyber operations.

Political will emerges as a factor in the context of the international law responses to internationally wrongful acts. It is an executive political decision whether to withdraw diplomats or seek reparations. The Prime Minister holds prerogative authority to engage in armed conflict. There is no head of a government agency that possesses decision making power in these areas. Given that the threshold responses in international law involve political decision making, political will becomes the third essential factor in determining the correct legal regime to be applied to cyber operations. Political will also factors into decisions of domestic jurisdiction. For Canada to act under the rule of law conducting cyber operations that impact the security of Canadians, effects must be appropriately measured and determined, accurate attribution made and timely political

will expressed. It is only in this way that the correct legal regime and appropriate agency can be ascertained and engaged. Figure 2 sets out a simplified process diagram.

Domestically, the broadly defined issue of privacy has both legal and political aspects. In 2014, Bill C-13 faced criticism from privacy advocates as it provided law enforcement warrantless access to ISP subscriber information.[152] While the bill was moving through Parliament, the Supreme Court of Canada (SCC) released a decision that effectively made a key component of the Bill unconstitutional. The Harper government introduced Bill C-51 in 2015 which added new powers to CSIS. This bill prompted a "national day of action" protest that was centered on the perceived infringement of civil liberties and privacy.[153] The bill's passing was cited by the online group Anonymous as the reason for denial of service attacks on the Senate, Justice Department, CSE and CSIS.[154] Most recently, the current Liberal government has expressed the willingness to enact further legislation to increase internet privacy rights.[155] Privacy concerns all security agencies working in cyberspace in order to manage operations not only in accordance with the law, but also the political executives they serve. When examining privacy in cyberspace related to security organizations, section 8 of the *Charter* is the starting point.

Hostile Cyber Operation Response Process



Court Decision," *The Globe and*

ill C-51," *Vancouver Sun* 14 March

nment to protest Bill C-51," *CBC* 18 June 2015.

[155] Andy Blatchford, "Spy Agencies to look i ndal; Brisson hints at tougher laws," *Canada Press* 20 March 2018.

Figure 2 – Determination of Legal Regime

Charter Application to Cyber Security Operations

Section 8 of the *Charter* is the citizen's constitutional protection against unreasonable search and seizure. It is this section that has attracted the most judicial attention related to cyberspace. It is of concern to anyone conducting cyber operations on behalf of the Canadian government because the definition of "search" has been interpreted very broadly by the courts. Definitionally, government actors engage in a "search" anytime they obtain information from someone who has a "reasonable expectation of privacy."[156] Dickson J. summed up a reasonable expectation to privacy as an assessment of "…whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals…"[157] He also went on to state that "…where it is feasible to obtain prior authorization, I would hold that such authorization is a precondition for a valid search and seizure."[158] State actors looking to acquire information from a person protected by s. 8 will in most cases need a pre-authorized judicial authorization to engage in the information gathering process.

Section 32 of the *Charter* sets out that the *Charter* applies to the government of Canada. This section has been consistently interpreted as applying to all actions by public

[156] *Hunter et al.,* v. Southam [1984] 2 SCR 145, 159.
[157] *Ibid.*
[158] *Ibid.*, 161.

servants acting under the authority of a Minister.[159] Operationally, the *Charter* is applied to virtually every aspect of law enforcement operations. The *Charter* has also been found to apply to exercises of Crown prerogative.[160] Much of the recent judicial attention applying the *Charter* to cyber operations comes from a law enforcement context. Despite the general application of s. 32, extra-territorial exclusions for *Charter* application continue to exist.[161] These exclusions are based on principles of sovereign equality and comity that support the basic principle that Canadian laws cannot be projected onto foreign sovereign lands.

In *Amnesty Intl. v. CAF,* the question was whether the *Charter* applied to either CAF members or detainees held in Khandahar by the CAF. Ultimately, the answer was that the *Charter* did not apply extra-territorially in these circumstances.[162] Whether the CAF had "effective control" over their operating territory in Afghanistan or alternately, had the Afghanistan government consented to the application of Canadian domestic law were the principal issues. Since neither condition manifested itself, LOAC was found to be the legal regime that applied to the situation.

In *P.M.* v. *Khadr,* released while the *Amnesty* case was before the Federal Court of Appeal, the SCC recognized an exception to the rule that the *Charter* does not apply to Canadian officials operating outside of Canada:

> The jurisprudence leaves the door open to the exception in the case of Canadian participation in activities of a foreign state or its agents that are contrary to Canada's international obligations or fundamental human rights norms.

The Federal Court of Appeal in *Amnesty* rejected the argument wide *Charter* exceptions to extra-territorial applications existed. The Federal Court of Appeal

---

[159] Peter Hogg, *Constitutional Law of Canada* (Toronto: The Carswell Company Limited, 1985), 671.
[160] *Khadr* v. *Canada (Attorney General)* (2016) FC 727, para. 61.
[161] *R.* v. *Hape* [2007] 2 SCR 292.
[162] *Amnesty International Canada* v. *Canada (Chief of the Defence Staff)* 2008 FCA 401, para. 36.

highlighted the SCC passage that set out that "…comity cannot be used to justify Canadian participation in activities of a foreign state or its agents that are contrary to Canada's international obligations."[163] The principles set out in these rulings are consistent with the approach taken by CSIS where judicial review of s. 21 warrant provisions is for the purpose of balancing s. 8 considerations, including extra-territorial operations.[164] These warrant provisions provide a good example of where the *Charter* applies to CSIS operations, even when the targets of those operations do not enjoy the same protections.

The *CSIS Act* provides CSIS with specific warrant authorities in s. 21 and s. 21.1. The first is to either intercept communications or performing duties and the second is for threat reduction "measures." The s. 21 warrant shares similarities to a Part VI wiretap authorization and general warrant requirement under the *Criminal Code* in terms of affidavit requirements and terms and conditions. Unlike a standard police wiretap authorization, the statute provides the ability for a judge to authorize these activities extra-territorially. The duration of these warrants is either sixty days or one year. The Federal Court has imposed upon s. 21 warrants jurisprudence similar to that of a *Criminal Code* wiretap authorization.[165] It is also clear that the Federal Court has interpreted the provisions of s. 21 to mandate "judicial control" through an "objective, detached analysis of the facts asserted on the application for a warrant…"[166] Further, CSIS has acknowledged that obtaining subscriber information from ISPs requires judicial pre-

[163] *Amnesty*…, para. 19.
[164] *Canadian Security Intelligence Service Act (Re)(TD)* [1998] 1 FC 420, 6.
[165] *Ibid*..., 9.
[166] *Ibid*..., 10.

authorization to comply with s. 8.[167] Overall, these rulings demonstrate an acquiescence on the part of CSIS that the *Charter* applies to many aspects of their operations, including cyber operations. In the new powers granted to CSIS in 2015, the *Charter* was expressly referred to as a limiting factor. The *Charter* provides a measure that an issuing judge can balance the methods and means in which CSIS reduces the threat to national security. The judge obtains jurisdiction through the s. 21.1 warrant requirements.

The s. 21.1 warrants were new in 2015. The *CSIS Act* explicitly requires CSIS agents to obtain the warrant when taking measures that may "contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms*" or contravene a Canadian law. [168] Taking these measures also requires the approval of the Minister of Public Safety. As with s. 21 warrants, these warrants can authorize extra-territorial activities by CSIS agents. Broad powers to issue assistance orders to any person and ensure that assistance remains confidential are also included.[169] The new measures introduced in 2015 contemplated *Charter* compliant operations. The legislation would also have contemplated cyber operations, as the bill in which these new powers were granted was aimed at cyberbullying and prompted a hostile cyber operation.

CSIS also has secondary mandates whose rules are not as clear, nor has the Federal Court ruled on them. CSIS is mandated for four secondary functions: to provide "security assessments" to the Government of Canada, provinces and police forces; enter into "arrangements" with foreign partners; provide advice to ministers of the Crown on matters related to the security of Canada; and collect information concerning foreign states or persons in relation to the defence of Canada or the conduct of international

---

[167] *X (Re)* 2017 FC 1048, para. 3.
[168] *CSIS Act*…, S. 21.1.
[169] *Ibid*., 22.3.

affairs.[170] Given the clear tendency by both Parliament and the Federal Courts towards *Charter* compliance, it would seem unlikely that CSIS could argue an unstated *Charter* exemption for these secondary mandates. The defence of Canada secondary mandate may offer the only exception to *Charter* compliance.

The military *raison d'etre* is armed conflict which normally engages LOAC as the governing legal regime. Normally, domestic legislation like the *Charter* does not apply in such situations.[171] *Amnesty* focussed on the concept of CAF effective control of a territory or the application of foreign domestic law. These principles cover most situations where the CAF deploys, are reasonably predictable and underscore the reason for instruments like Status of Forces Agreements. LOAC also explains why in most cases the *Khadr* exception would not be required. LOAC represents Canadians upholding international obligations during armed conflicts. By definition, Canadians meeting their international obligations excludes the *Khadr* exception. Therefore, any CSIS, CSE or RCMP member operating under LOAC as lawful combatants would also not be subject to their normal *Charter* obligations. However, the situation changes considerably when engaged in operations that are not in furtherance of an armed conflict.

Most international cyber operations to date have occurred under peacetime international law and treated as such by most nations. The *Amnesty* case stands apart from the SCC decision in *Khadr*. The *Amnesty* case did not imbue the CAF with *Charter* immunity as an organization. The case recognized the severe limitations and impracticalities of layering domestic civil rights into an armed conflict, over and above those existing in LOAC. Considering cyber operations from the perspective of peacetime

---

[170] *Ibid*., ss. 13, 14 and16.
[171] *Amnesty*…, para. 38.

international law, then the issues of comity, sovereign immunity, non-interference and Canada's recognized international obligations become much more prominent.

The Joint Doctrine Note suggests that the CAF can engage in offensive cyber operations and conduct response action as part of active cyber defence. This doctrine contemplates the CAF engaging a "hack back" technique that physically damages the attacking computer on the basis of its attack on the CAF computer system.[172] Similarly, the CSE's mandate is to "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence."[173] These activities taking place in the context of an armed conflict are likely excepted from *Charter* compliance. In the context of peacetime international law or domestic law, it is likely that they fall under the normal rules for a government agency, which includes *Charter* compliance.

The argument that a cyber operation is exempt from domestic legislation because a foreign national or foreign equipment is the object of the effect and does not enjoy *Charter* protection seems quite weak. Reliance on the principle that the foreign national has no *Charter* rights based on sovereign immunity and comity is this argument's weakness. The argument fails to appreciate that a lack of *Charter* protection for a particular person does not relieve the government actor of their duty to conduct operations in accordance with *Charter* principles. In respect of peacetime international law, Canada is subject to internationally recognized obligations, including the duty of non-interference and a host of customary and treaty-based obligations. These obligations include internationally recognized rights of privacy endorsed by Canada that have now

---

[172] Canadian Forces Warfare Centre, *Joint Doctrine Note…*, 4-5.
[173] Communications Security Establishment, "Foreign Signals Intelligence," last modified 2017-06-22 https://www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement.

arguably become customary international legal obligations.[174] The question becomes whether the situations described engage the *Khadr* exception or not. *Charter* applicability to peacetime CAF and CSE extra-territorial cyber operations seems likely as it is hard to distinguish these cyber operations from those that CSIS engages.

There is no indication in either CAF or CSE policy that the prospect of *Charter* compliant cyber operations has been considered, likely because of the question around extra-territorial application. The currently tabled bill C-59 proposes to provide the CSE with its own mandating *Communications Security Establishment Act*.[175] This bill does not reference *Charter* compliant operations, but instead continues the practice of Ministerial authorizations for a range of activities including defensive and active cyber operations. The bill includes a section that mandates the CSE to "…ensure that measures are in place..." to protect privacy.[176] The bill also mandates that CSE activities are not to be directed at a Canadian or any person in Canada.[177] However, the CSE acknowledges that in the complexity of cyberspace, Canadian metadata will likely be collected.[178] The CSE feels that *Charter* compliance will be accomplished through Ministerial authorizations and oversight by the Intelligence Commissioner.[179] These new provisions do not seem to address the public concerns with Five Eyes intelligence sharing arrangements where Canada could extra-judicially intercept the communications of citizens from allied nations, such as the United States, Australia and the United Kingdom, and then freely

---

[174] Schmitt, *Vade Mecum*…, 256: see also United Nations, *International Covenant of Civil and Political Rights*. New York: UN, 1976; United Nations General Assembly. *Universal Declaration of Human Rights* New York: UN, 1948.
[175] Bill C-59, *An Act Respecting National Security Matters*, 1st Sess., 42nd Parl.,2017 [hereinafter "Bill C-59]
[176] Bill C-59…, s. 25.
[177] Bill C-59…, s. 23.
[178] Canadian Security Establishment Canada, "Briefing Binder C-59 November 29, 2017," Access to Information Request Number A-2017-00077 – CSE Briefing Binder Bill C-59 (March 2018), 15.
[179] *Ibid., 34.*

share the fruits of those interceptions with the host countries, and vice versa.[180] Given the difficult nature of attribution, these provisions do not help explain what degree of attribution certainty is required before a cyber operation will be permitted. It also raises questions of how quickly attribution could be determined prior to an active defence cyber operation was authorized? The concern being how could one know in a timely manner that the perpetrator of a hostile cyber operation is not a Canadian masking their IP address or utilizing a foreign IP address. To address these issues, the CAF and CSE would be well advised to ensure robust *Charter* analysis formed part of their cyber operations strategies.

Since the *Charter* will impact most cyber operations, understanding the direction and impact of recent judicial decisions is essential for leaders in cyber security agencies. The judiciary are determining acceptable cyber operational techniques through the lens of privacy rights. The lack of technical understanding evident in some cases complicates the legitimate needs of Canadian security operations. A Canadian pragmatic approach to privacy will be advocated as it provides a practical framework for security agencies to contribute their unique knowledge and experience to privacy decision makers. A pragmatic approach to privacy issues would be most effective if done collectively. Understanding recent judicial decisions will also demonstrate the consequences for security agencies who fail to apply these constitutional considerations to their cyber operations.

Conceptualization of Privacy in Cyberspace

[180] Editorial, "CSE: What do we know about Canada's eavesdropping agency?" *CBC,* 14 June 2013.

The fundamental technology that underpins cyberspace ought to inform views on privacy in cyberspace. It is difficult to use the internet without some manner of core biographical information being shared with other internet users or service providers. Even using advanced cryptographic methods, all internet users leave some digital evidence of their usage. Even in the dark web core biographical information such as comments on market sites, purchase history and cryptocurrency usage is available to any internet user. Although anonymized by the cryptographic software, it is not private by any definition of that term.

Privacy is a very broad legal concept. Solove observed that legal problems in this area are not well articulated, with the result that "we frequently do not have a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems."[181] When this lack of articulation is married with a serious lack of a technical understanding of how cyberspace works, results are confused at best. Courts struggle to conceptualize an all-encompassing privacy doctrine for cyberspace. Diverse privacy issues are being converged with lack of technical knowledge to pronounce vague and confusing judgements. The converged issues mix concepts like freedom of thought, bodily integrity, with protection of our homes, information and reputation. Decision makers attempt to balance these converged privacy interests against restraints on government's ability to interfere with any of those things.[182] These combined difficulties to the conceptualization of privacy provide a daunting challenge for decision makers.

---

[181] Daniel J.Solove, "Conceptualizing Privacy," *California Law Review* 90, No. 4 (July 2002): 1090.
[182] Solove*, Conceptualizing Privacy*…, 1088.

Examples of this confusion in recent Canadian jurisprudence include the recently decided Supreme Court case *R*. v. *Marakah*. Nour Marakah conspired with Andrew Winchester to sell firearms illegally. During the process of selling these firearms, Marakah and Winchester communicated through text messages on their cellular telephone devices. The central issue on appeal was whether the law ought to recognize Marakah's privacy interest to the text messages obtained by the police on Winchester's device. The Supreme Court held that Marakah possessed a reasonable expectation of privacy on his messages stored on Winchester's cellular phone.

In *R.* v. *Spencer*, the issue before the SCC was whether the request by police to the ISP for subscriber information was a breach of Spencer's reasonable expectation of privacy. In this case Spencer was sharing child pornography using a readily available file sharing service. The SCC ruled that Spencer had a reasonable expectation of privacy with respect to his subscriber information held by the ISP and that the police request to the ISP for voluntary disclosure constituted a search. This ruling is now interpreted as a requirement to obtain a search warrant for ISP subscriber information.

In these important privacy cases, the SCC engaged metaphor and analogy to replace an actual understanding of cyberspace to arrive at their conclusions. Furthermore, both cases show a propensity to conflate various privacy issues to reach their conclusions. These cases are simply two examples of several recent decisions that are setting a course for Canadian privacy rights in cyberspace. Understanding the thinking behind these two decisions provides insight for Canadian security agencies currently engaging in cyber operations. Specifically, without clear credible rationale for cyber operational techniques,

the courts are reluctant to give government actors much self-regulatory power in applying those techniques.

In *Marakah*, the technology at issue was "short message service" (SMS) messages sent from Marakah's device to Winchester's device. This is a technology that allows small amounts of text to be transmitted over cellular networks. Critically, the Chief Justice defined the subject matter of the search as the "electronic conversation" not the messages left on the phone.[183] In her analysis, the Chief Justice recognized that historically in Canada a person's expectation of privacy was often "designated by place, as evident in the old dictum that every man's home is his castle…."[184] The Chief Justice went on to explain that "electronic conversations" do not easily translate into the conceptualization of territorial privacy interests. Nevertheless, the Chief Justice then analogized that the "interconnected web of devices and servers…is every bit as real as physical space."[185] She described her metaphor as "There, we seclude ourselves and convey our private messages, just as we might use a room in a home or an office to talk behind closed doors."[186] Going even further, the Chief Justice stated, "The phrase 'chat room' to describe an Internet site through which people communicate is not merely a metaphor."[187] Specifically included within this metaphor were several online based communication platforms including Apple iMessage, Google Hangouts and BlackBerry Messenger.[188] This reasoning concluded that the chat rooms are the place of the search

[183] *R.* v. *Marakah* 2017 SCC 59, para. 17.
[184] *Ibid.*, para. 25.
[185] *Ibid.*, para. 28.
[186] *Ibid.*
[187] *Ibid.*
[188] *Ibid.*, para. 18.

and electronic conversation the object of the search. These conclusions changed Canadian law and are important for Canadian security agencies to understand.

Traditionally, if police searched a home and found a letter, the letter could be seized as representing the contents of the communication while other evidence would need to be put forward to establish who wrote the letter. At no point was the letter found in the home treated like an "intercepted private communication," a term of art in the criminal law, defined in Part VI of the *Criminal Code* related to what is commonly known as wiretap.[189] Prior to *Marakah*, most text messages, emails or any other electronic communication had been considered "delivered" and more analogous to a letter sitting on the recipient's table, than a letter being moved through Canada Post or an intercepted phone conversation. The concept being that one had a great deal more privacy in "moving" communications as opposed to communications that where stored or filed, and even less when the communication was in another's possession. *Marakah* has potentially dramatically increased the reasonable expectation of privacy on all manner of electronic or online communication, including copies of communication that are no longer in an individual's possession.

Marakah is not the only case to utilize questionable analogies and conflated privacy analysis to reach a conclusion. In *Spencer* Cromwell J. writing for a unanimous SCC found that the subject matter of the search was "…a subscriber whose Internet connection is linked to particular, monitored Internet activity."[190] Cromwell J.'s finding is significant, because from the police perspective they simply asked for the name and address of the person who contracted with the ISP. Instead of this, a unanimous court

[189] *Criminal Code* RSC, 1985, c. C-50, s. 183.
[190] *R.* v. *Spencer* 2014 SCC 43, para. 32.

determined that the police were actually obtaining the *person* behind the internet activity they were monitoring. With a basic technical understanding, one can see how in one sentence the SCC converged the information being sought by the police with many other pieces of information held by a variety of people and companies. Some of the attribution information implicit in Cromwell J.'s sentence include the subscriber information held by the ISP, the particular personas utilized by the one or more users of that IP address, the devices and equipment making up the users physical network, the geographic information attached to the IP address used in the file sharing and the geographic information attached to the physical network. All of these pieces of information are all distinct attribution questions which when put together may indicate the actual identity of the user, but most were not part of the police request. Different parts of the information are available to any internet user, to the ISP provider, to the user's software provider, to the administrator host of the file sharing service, to the ISP, to the physical network administrator if different from the end user (in this case Spencer's sister), and the end user themselves.

Like in *Marakah* many distinct privacy issues were conflated in *Spencer* to result in difficult to understand decisions that arguably do not reflect the reality of cyberspace. In justifying his conclusions, Cromwell J. blended informational and territorial privacy interests. He concluded "…because the computer identified and in a sense monitored by the police was in Spencer's residence, there is an element of territorial privacy…."[191] These conclusions were reached despite explicitly stating that there was "little information on the record about the nature of IP addresses in general or the IP addresses provided by Shaw to its subscribers."[192] In *Marakah* the Chief Justice used similar

[191] *Ibid*., para. 37.
[192] *Ibid*., para. 8.

conflations of territorial and informational privacy to describe text messages by using a range of metaphorical space. At one end is the "high expectation of privacy" in one's own phone, a "lesser expectation of privacy" in a friend's phone, and "no reasonable expectation of privacy" in messages displayed to the public.[193] In both cases the SCC used analogies and metaphors without clear understanding of the underlying technology, as well as trying to make one judgement speak to multiple aspects of privacy issues.

A particularly insidious analogy was Cromwell J.'s comparison of anonymity on the internet with an author who publishes a book but wishing to remain anonymous. In this situation, Cromwell J. cites many places in cyberspace where user information is collected and retained, such as "browsing logs," search engines, advertisers and the use of "cookies" leading him to the conclusion that:

> The user cannot fully control or even necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous - by guarding the link between the information and the identity of the person to whom it relates – the user can in large measure be assured that the activity remains private.[194]

Legitimate reasons to remain anonymous exist, although most of those are for citizens of countries where open speech and dissent from those in power can have violent consequences. It is highly questionable whether being an anonymous author of a published book is really connecting with the realities of modern technology users and the many issues involving privacy in cyberspace. Does the Court's analogy better compare to an analogy of a general right to be disguised in public places, which currently does not exist? Even more disappointing is the suggestion that anyone's privacy can be "assured" online through anonymity obtained by requiring government actors to obtain a warrant requesting IP address subscriber information from an ISP. Nevertheless, from the

---

[193] *Marakah*…, para. 29.
[194] *Spencer*…, para. 46.

perspective of security agencies conducting cyber operations, these cases represent the privacy law of Canadian cyberspace as it now stands, devoid of pragmatism and awash in inaccuracy. Some cyber security operators may dismiss these cases as relatively inconsequential to their operations but ignoring privacy issues can have serious strategic impacts.

A recent case demonstrated the dangers of Canadian security agencies continuing to address these issues in *ad hoc* ways. In 2016 the Federal Court of Canada convened a rare "*en banc*" hearing to review a CSIS intelligence collection and retention program whose existence had not been previously disclosed to the court.[195] After a lengthy review, involving the direct testimony of several high ranking senior CSIS officials, the court found that CSIS had "breached its duty of candour towards the Court by failing to inform it clearly and transparently of its retention program…."[196] At the core of this proceeding was the retention of third party data that was electronically embedded in otherwise lawfully obtained information. The privacy implications for the retention of this data was considered extremely important by the Federal Court. The judges described themselves as "gatekeepers" balancing private interests with the states need to intrude upon privacy for a collective good.[197] This case ended with the judges suggesting that it "…may be time for Canadians to renew a debate regarding the mandate and functions of our domestic intelligence agency."[198] This serious challenge to CSIS's core mandate and credibility could have been avoided through understanding the deep-seated privacy concerns their operational procedures raised, and acting to proactively address them.

---

[195] X (RE) (2016) FC 1105. An "*en banc*" hearing is one in which the entire Federal Court bench is invited to sit on the case. This is a rare occurrence in Canada.
[196] *Ibid.,* para. 7.
[197] *Ibid.,* para. 100.
[198] *Ibid.,*para. 264.

Recognize important privacy issues in security cyber operations and effectively managing them can be done through a pragmatic approach. Solove proposed a pragmatic approach to conceptualizing privacy that focussed on particular contexts of privacy, instead of abstract unifying privacy theories.[199] This pragmatic approach focusses on practices that are deserving of legal protection, with the degree of protection contingent on its social importance.[200] Solove pragmatically organized privacy issues into a "taxonomy" of: information collection, information processing, information dissemination and invasion.[201] These are a collection of practical situations where privacy values can be evaluated in the context of the actual factors impacting that situation.

Utilizing the taxonomy as a starting point, the different practical aspects of various privacy situations encountered by defence and security agencies can be analysed in a pragmatic way. Using the privacy surrounding ISP subscriber information is one example of information collection. The analysis would hinge on what aspects of subscriber information are impacted by privacy protections. [202] The analysis focusses on a concrete practice, as opposed to abstract notions of privacy.[203] Pragmatically, how is the practice of ISPs obtaining contract information impacted by increased or decreased expectations of privacy. [204] Looking at this issue pragmatically would focus on the purpose of the ISP collecting subscriber information. Relying on a technical understanding of cyberspace, an ISP provides its customers some physical network equipment and logical network access through an IP address. To obtain the equipment

---

[199] Solove, *Conceptualizing Privacy*…, 1092.
[200] *Ibid*., 1093.
[201] Daniel Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154 No. 3 (2006): 488.
[202] *Ibid*., 1143.
[203] *Ibid*., 1127.
[204] *Ibid*.,

and services the ISP requires standard contract information from the purchaser to know who to bill for its services and where to provide the services. The identity of the ISP is normally available to anyone on the internet through the IP address, along with a reasonably close geographic location. The subscriber information does not include the person using the IP address, but instead the person who contracted with the ISP for the provision of that IP address. This information can be used to pragmatically evaluate the specific values in conflict, namely those of the person using the IP address, and compared to those of defence and security agencies in pursuit of their mandates. Very little analogy or metaphor is required to understand the nature of the issue and come to a fair evaluation of the competing interests.

Canadian defence and security agencies could benefit from a pragmatic approach to privacy. Developing a Canadian pragmatic approach could put security agencies in a unique position to provide sensible input to the discussion. All Canadian security agencies are comprised of people who engage in years of training to perform espionage, warfare or law enforcement operations that are well outside the everyday norms of most Canadians. In all forms of review, whether judicial, political or otherwise, Canadian security agencies are in the role of presenting evidence to decision makers. Taking a pragmatic approach would see security agencies evaluating the means and methods of cyber operations against a Canadian version of Solove's taxonomy of privacy. For example, using this approach could challenge the propensity towards physical space metaphors and analogies that simply do not translate to the cyber domain.[205] Putting Canadian security agencies in a position to provide the best information about cyber operational techniques including responsible and balanced approaches to civil rights

[205] Solove, *Conceptualizing Privacy*…, 1131.

would positively impact operations. Instilling public, political and judicial confidence through professionalism can only enhance operations. Practical benefits could be realized through considered input into the many difficult future decisions related to balancing privacy and security interests. However, these benefits will be difficult or impossible to realize if each Canadian defence and security agency takes a different position on these issues. In terms of privacy, Canadians can be reasonably expected to scale their expectations with the degree of threat involved.[206] Privacy though is only one consideration in a complex operational environment.

The Canadian cyber security policy has not recognized that before any agency can mount an effective and lawful response to a hostile cyber operation, a legal context needs to be determined. Is the hostile cyber operation a domestic or international crime that ought to be responded to by criminal prosecution? Is it an internationally wrongful act that could be responded to with expulsion of diplomats, economic sanctions or a destructive attack on the command and control systems for the malware? Or, could the seemingly minor hostile cyber operation be the beginning of an armed attack once proper attribution and effects are understood? The Horizontal Evaluation has demonstrated that this approach has created problems that prevent effectively dealing with these situations.

Canada and specifically the institutions responsible for protection of Canadians, do not possess unlimited means and methods to execute on their responsibilities. Canadian security objectives can be achieved once the technical realities of cyberspace are understood in the context of the three potential legal regimes. Operations in the cyber domain will be conducted utilizing similar technologies and adapting to similar adversary

---

[206] Daniel Solove, "*'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*," *San Diego Law Review* 44 (2007): 748.

behaviour from lone child predators to state actors. It is only through analysing effect, attribution and applying political will in a comprehensive approach that Canadian security agencies can hope to navigate successfully through these issues. Going it alone, as evident in the CSIS case and the CCSS Horizontal Evaluation will only serve to de-legitimize otherwise legitimate cyber operations.

The best way to accomplish these objectives with limited national capabilities is through the comprehensive approach. A comprehensive approach can best integrate the range of security based cyber operations and afford the best chance to maximize Canadian resources in this area. More importantly, a comprehensive approach can also address issues of oversight and public trust to ensure that cyber security operations do not sacrifice the very values that they are put in place to protect. The question remains, how can the comprehensive approach meet all these needs?

CHAPTER 3 - THE COMPREHENSIVE APPROACH

The comprehensive approach represents one effective way to determine attribution, measure effect and combine it with political will. Essentially, this approach combines civilian and military efforts to best manage a situation.[207] In a security context, comprehensive security has been described as the coordinated application of both government and non-government capabilities.[208] The CAF has embraced this concept to engage complex situations effectively. Known in CAF doctrine as JIMP Operations, the concept of Joint, Inter-agency, Multi-national, Public makes the point to commanders that other elements of national and allied power can be brought to bear on complex situations.[209] The comprehensive approach has been utilized in both foreign and domestic operations, including Afghanistan and the 2010 Vancouver Olympics.

An important distinction exists between the comprehensive approach and the whole of government approach. The latter means interagency or inter-departmental coordination and cooperation within government.[210] Taking a comprehensive approach means integration beyond government. In the cyber domain both the logical network and physical network are largely out of the control of governments. Private companies like Shaw, Bell, Rogers, Telus and others own most physical networks in Canada. Logical networks are mostly the domain of large multi-national corporations like Apple, Microsoft and Google who manage software "ecosystems" that enable most electronic

---

[207] Dr. Cécile Wendling, *The Comprehensive Approach to civil-military crisis management. A critical Analysis and perspective* (Paris: Institut de Recherche Stratégique de l'Ecole Militaire 2010), 10.
[208] Ann Fitz-Gerald and Don Macnamara, "Comprehensive Security Requires Comprehensive Structures – How Comprehensive Can We Get?" *Strategic Studies Working Group Papers* (Ottawa: Canadian Defence & Foreign Affairs Institute, 2012), 4.
[209] Department of National Defence, B-GL-300-003/FP-001, *Command In Land Operations* (Ottawa: DND Canada, 1996), 2-23.
[210] Gjert Lage Dyndal and Cornelia Vikan "NATO's Comprehensive Approach: Still Something for the Future?" Paper presented at the *Norwegian Defence Command and Staff College Doctrine Conference*, Oslo, 25-26 June 2014, 4.

devices. The protocols that allow the internet to operate are managed by public international bodies. Envisioning a national cyber security strategy without the engagement of key public and private stakeholders would be doomed to failure from the start as government is only one participant. These public and private stakeholders rely on government regulation and facilitation to conduct business in Canada, presenting a motivation for collaboration. The wide collaboration envisioned in the Canadian Cyber Security Strategy is what we seek to operationalize through a comprehensive approach.[211]

Unfortunately, the comprehensive approach has historically been much easier to talk about than implement. Basic issues like compete or cooperate are at the heart of many complex issues that make a comprehensive approach difficult to operationalize.[212] Recognizing recent Canadian challenges experienced in comprehensive operations provides guidance for how Canadian security agencies could be coordinated for cyber operations.

Recent Canadian Challenges with the Comprehensive Approach

Two significant Canadian operations that took a comprehensive approach were the decade long deployment to Afghanistan and the Vancouver 2010 Olympic domestic security operation. The North Atlantic Treaty Organization (NATO) has also adopted the comprehensive approach to operations as a standard. Valuable guidance reveals that challenges with the comprehensive approach can be broken down into two broad categories of potential shortfalls: coordination challenges and capability gaps.[213]

---

[211] Government of Canada, *Cyber Security Strategy*…, 1.
[212] Christian Leuprecht. "Conclusion," in *Security Operations in the 21st Century: Canadian Perspectives on the Comprehensive Approach,* 165-176, ed. Michael Rosteck and Peter Gizewski (Kingston and Montreal: McGill-Queen's University Press, 2011), 237.
[213] Philipp Rotmann, *Built on shaky ground: the Comprehensive Approach in Practice*, NATO Research Paper No. 63 (Rome: NATO Defense College December 2010), 2.

Reviewing the guidance can identify historically challenging areas for operationalizing the comprehensive approach for Canadian cyber operations.

Identifying past areas of difficulty implementing the comprehensive approach allows planners to mitigate these issues for cyber operations integration. In the case of the Vancouver Olympic security operation, a lack of a central coordination mechanism was the main criticism, with emphasis on a lack of classified information sharing.[214] This coordination failure was arguably never corrected.[215] Although information sharing issue has been blamed on "tribalism" law governing police obligations for disclosure may provide a different perspective.[216] Since classified information sharing is a significant facet of integrated cyber operations capabilities, this issue requires planning attention.

Some aspects of the information sharing issue can be explained by the legal context police are required to operate. A significant issue faced by all police criminal operations is the disclosure requirements imposed in cases such as *R. v. Stinchcombe* and *R. v. Jordan*.[217] Working together with the *Canada Evidence Act,* these cases impose a very robust obligation on police and Crown Counsel to disclose all information in its possession or control that is not clearly irrelevant.[218] The recent *Jordan* ruling imposed further temporal pressures to the existing disclosure obligations. These disclosure requirements pose a significant and ongoing impediment to the sharing of information between security agencies. Regardless of government attempts at legislating information sharing between security agencies, the robust disclosure requirements imposed on police

---

[214] Bernard Brister, "Family Relations: A Preliminary Analysis of the Use of the Comprehensive Approach at the Vancouver 2010 Winter Olympics," in *Security Operations in the 21st Century: Canadian Perspectives on the Comprehensive Approach*, edited by Michael Rostek and Peter Gizewski (Kingston and Montreal: McGill-Queen's University Press, 2011), 176.
[215] *Ibid.*, 175.
[216] *Ibid*., 171.
[217] *R.* v. *Stinchcombe* [1991] 3 SCR 326; *R.* v. *Jordan* [2016] 1 SCR 631.
[218] R.S.C., 1985, c. C-5.

are very difficult for other security agencies to deal with.[219] Given the nature of cyber operations, free exchange of information is a significant requirement for any comprehensive attribution and effects analysis to be successful. Seamless information sharing is but one of several coordination challenges that can be forecasted.

In the military-led mission to Afghanistan, coordination problems abounded. Some particularly applicable to the Canadian cyber security situation include the requirement for well trained, equipped and experienced task force participants. Areas of improvement included clearly defined political and operational objectives and the ability for senior government and operational leadership to receive and understand input on changing tactical, operational and strategic contexts.[220] These Afghanistan coordination issues are similar to those experience more broadly in NATO.

NATO has employed a comprehensive approach to operations for many years. This experience has identified consistent challenges, like those experienced by Canada in the Vancouver Olympics and Afghanistan. The first was fragmentation of participants from common objectives to pursue parochial interests.[221] In the Canadian context fragmentation could occur for several reasons including personnel shortages or other competing agency priorities. The second challenge was organizational cultures. In the NATO context culture issues are largely seen as military culture and values clashing with various civilian agencies, both governmental and non-governmental. Domestically, this type of organizational friction reportedly occurred during the Olympic security operation and would be a foreseeable challenge integrating various security agencies cyber

---

[219] *Security of Canada Information Sharing Act*, SC 2015, c.20, s.2
[220] David J. Bercuson and J.L. Granatstein, *Lessons Learned? What Canada Should Learn from Afghanistan* (Ottawa: Canadian Defence & Foreign Affairs Institute, 2012), 26.
[221] Rotman, *Shaky Ground*…, 4.

operations.[222] The final challenge NATO identified related to questions of strategy and policy. This strategy-policy dynamic has attracted Canadian academic interest related to domestic security operations. These commentators recommended identifying clear national interests in policy direction to agencies that can then be translated into strategy by operational commanders.[223] Overall, the coordination challenges are well documented and have produced credible academic and practitioner analysis that can serve to guide the way forward.

Common themes are identifiable for capability related challenges as well. From the Vancouver Olympics operation, observations related to the different agencies strengths and weaknesses were evident. Olympic security was RCMP led. In this role, the RCMP demonstrated a lack of capability with respect to strategic planning and coordination that caused friction with other agencies, particularly the CAF who excel in these areas.[224] Not being accustomed to sharing information in intelligence handling impacted the ability of civil emergency agencies to work with both the RCMP and CAF, who had highly refined capabilities in this area.[225] Overall, practical concerns can impact resource allocation. Canada is not a nation of unlimited security resources, meaning that to staff a highly functioning cyber operations unit would mean resources would be re-allocated from the various agency's primary responsibilities.[226] These capability related challenges will likely manifest themselves while trying to integrate cyber operations in a number of practical ways.

---

[222] Brister, *Family Relations*..., 170.
[223] Brad Gladman and Peter Archambault, "A Role for Effects-Based Planning in a National Security Framework," *Journal of Military and Strategic Studies* 13 No. 2 (Winter 2011): 9.
[224] Brister, *Family Relations*..., 167.
[225] *Ibid.*, 169.
[226] Fitz-Gerald, *Comprehensive Security*…, 7.

Even if new funding and supplemental human resources are added to defence and security agencies, the transformation to operational capability is often measured in years. Bringing in existing capabilities needs to be realistically balanced with each agency's primary responsibilities.[227] Reallocating key resources increases agency pressure to show results and prove value for the reallocation. Clear rules of agency engagement would be necessary to avoid undermining the legitimate independence of the agencies and corresponding Ministers. On balance, managing practical challenges far outweighs the operational benefits of a comprehensive approach.

A Comprehensive Approach to Cyber Operations

Operationalizing a comprehensive approach in Canadian cyber operations leverages prior experience and recommendations to avoid and manage anticipated challenges. The process of operationalizing can be approached in three broad areas: coordination, capabilities and facilitating factors. Efforts in these areas serve to constructively address the common and recurring challenges experienced by Canadian and international operations. The coordination and capabilities areas speak to the comprehensive approach to ascertaining attribution, effects and political will that determines what legal regime ought to apply, but also what Canadian defence or security agency ought to assert jurisdiction. Facilitating factors are those areas that support and allow for effective cyber operations in a comprehensive environment. In each of these areas, recommendations are made to successfully integrate a comprehensive approach to cyber operations.

Coordination

[227] Leuprecht, *Conclusions*…, 245.

Based on lessons from both the Vancouver Olympic security operation and Afghanistan, coordinating political direction with operational effect in a way that can evolve with the situation is imperative to achieve desired objectives. Since some cyber operations may require direction up to and including the Prime Minister, modeling after the Afghanistan Task Force and Cabinet Committee on Afghanistan may offer an effective way forward.[228] A cyber task force could be created under the Privy Council Office (PCO). Its purpose would be to bring together authoritatively high level multi-agency bureaucrats that would be responsible to produce effective strategic policy and meaningful coordination of government activities in cyber space. The cyber task force would be responsible for informing Canadians about cyber security operations and capabilities. The cyber task force would be linked closely with a Cabinet committee that would have the key ministerial representation including Public Safety and Defence. This committee would be the link between the bureaucratic and political organizations.[229] Unlike the National Security and Intelligence Committee of Parliamentarians, the cabinet committee would be operationally focused instead of review focussed.[230] PCO leadership also provides interface between operations and the bureaucracy.

Operational coordination could come in the formation of some type of office of cyber operations, overseen by a senior civilian bureaucrat that was directly responsive to the PCO cyber task force. Since the nature of comprehensive cyber security operations is very different than that of Afghanistan operations, this level is where caution would need to be exercised. Specifically, this office would be designed as a long standing

---

[228] Nicholas Gammer, "The Afghanistan Task Force and Prime Ministerial Leadership: Tactical Retreat or a New Direction in Managing Canadian Foreign Policy?" *American Review of Canadian Studies* 43 No. 4 (2013): 468.
[229] Gammer, *New Direction*…, 469.
[230] *National Security and Intelligence Committee of Parliamentarians Act*, SC 2017, c. 15.

governmental structure that oversees a wide range of security related cyber operations.[231] These cyber operations would be conducted across the spectrum of security agencies, some of whom like the police, have long standing common law authorities to act independent of political interference. The senior bureaucrat leader would need to have experience and understanding of operations in the Public Safety sector where these types of considerations are routine.

Underneath the civilian public servant would be senior operational leaders representing the security agencies that form a command council. It is at this leadership level where operational decisions would be made, and the flow of information would be determined in a collaborative way. A command council would link the independent operations of the individual security agencies with the collective operations of the cyber operations teams, and vice versa. This collection of operational leaders would also collaboratively make determinations of attribution and effect which could be sent through the office of cyber operations to the cyber operations task force and up to the Cabinet Committee and Prime Minister where required, for the application of political will.

This proposed structure seeks to incorporate lessons from past comprehensive operations to mitigate previously identified challenges. The operational-bureaucratic-political interface has had reasonable success and ultimately improved operational effects in managing Afghanistan operations.[232] The model is also credited for reducing departmental "tussle" that was widely cited as negatively impacting operations.[233] Once mature, this model could also serve to push operational decision down to the lowest most

[231] Leuprecht, *Conclusions*…,, 245.
[232] Gammer, *New Direction*…, 471.
[233] Bercuson, *Lessons Learned*…, 34.

responsive level, another key lesson learned internationally.[234] Lowest level decision making could develop further as stable expressions of political will were established through practice and experience allowing predictability of response options. Below this operational leadership level could exist the actual capabilities of the cyber operations teams.

Capabilities

Questions of attribution and effect consistently come up throughout any legal analysis of cyber operations both domestically and internationally. Attribution and effect analysis are not conducted the same or necessarily require the same skill sets. For this reason, two separate multi-disciplinary teams could be organized to accomplish each critical task.

The attribution team would have as its main effort knowing who is doing what and where it is taking place in cyberspace. Intelligence and investigation would be the main purpose of this multi-disciplinary team's existence. The team could rely on a fusion of CSIS and RCMP investigators and analysts, supported by CAF, CSE and Global Affairs lines of information, perspective and experience. Their essential responsibility would be to ensure the best possible attribution for both proactive or offensive operations as well as defensive operations, including intelligence, law enforcement, espionage and warfare. The key to success for the team would be effective blending of technical specialists with operational investigators to achieve maximum capability to attribute. Attribution capability requires the ability to conduct real world operations in coordination with operations in cyber space. Real world capability to support attribution would be the

[234] Rotmann, *Shakey Ground*…, 7.

strength of the multi-agency "reach back" to home agency capability. This team would require a close liaison capacity with corporate, private and public bodies responsible for internet security and protocols. Liaison would allow the exchange of information with respect to security threats to these bodies, as well as awareness of what security measures are being taken in the private sector.

An effects analysis team would require similar blended multi-agency capabilities to the attribution team, but the focus would be on the damage or potential damage from either offensive or defensive cyber operations and the impacts from hostile cyber operations. It is with this team that software engineering, forensic evidence specialists and systems specialists in conjunction with appropriate analytical resources to provide assessments of cyber operations impacts. CSE and CAF would likely be the main contributors to this team, with support from CSIS and RCMP forensic specialists. This capability would be required to understand complex impacts from sometimes subtle and wide-ranging hostile cyber operations. This specialization would be instrumental in informing the legal assessment of cyber weapons, used across the full spectrum of cyber operations from intelligence to warfare. The team would also provide expert opinions on reasonably expected effects from employing cyber operational techniques across the full range of cyber operations. Implicit is also the technical expertise to provide cogent explanations for Canadian cyber capabilities to courts, the political and bureaucratic leadership and the Canadian public as required. Like the attribution team, this team would require close liaison with corporate, private and public bodies. The difference is that the effects team would be more interested in issues of infrastructure, design and vulnerabilities. The team would also engage with ongoing integrated critical

infrastructure security measures.[235] Together the effects and attribution teams would provide key analysis that would facilitate operational and political decision making.

Coordinating the effects and attribution teams would be needed to provide a point for integrating the two streams of analysis. An operations coordination center would be responsible for the fusion of the effects and attribution products into a cohesive analytical product. The command council would utilize the analytical product for decision making and obtaining direction on political will as required. Rarely will there be perfect clarity on these issues. The coordination center could also provide advice to the command council to assist in turning the political will, effects and attribution information into viable cyber operational directions. Once jurisdiction has been decided, the coordination center can ensure the information is tasked to the appropriate defence or security agency for intelligence or follow-up action. The operations coordination center would continue to liaise with the responsible agency to monitor progress and engage either the attributions or effects analysis teams for specialized support as required. Conversely, when real world capabilities are required in support of attribution or effects analysis, the coordination center could be responsible for arranging those capabilities. The final responsibility of the operational coordination center would be to monitor all cyber operations teams for legal compliance. Legal compliance would also include ensuring that each team had appropriate judicial authorizations in place for activities violating expectations of privacy and other *Charter* provisions. The coordination center could also provide similar advice to each defence and security agency to assist in ensuring all agency cyber operations conformed to the appropriate legal regime.

---

[235] Public Safety Canada, *Action Plan for Critical Infrastructure,* (Ottawa: Her Majesty the Queen in Right of Canada, 2017), 5.

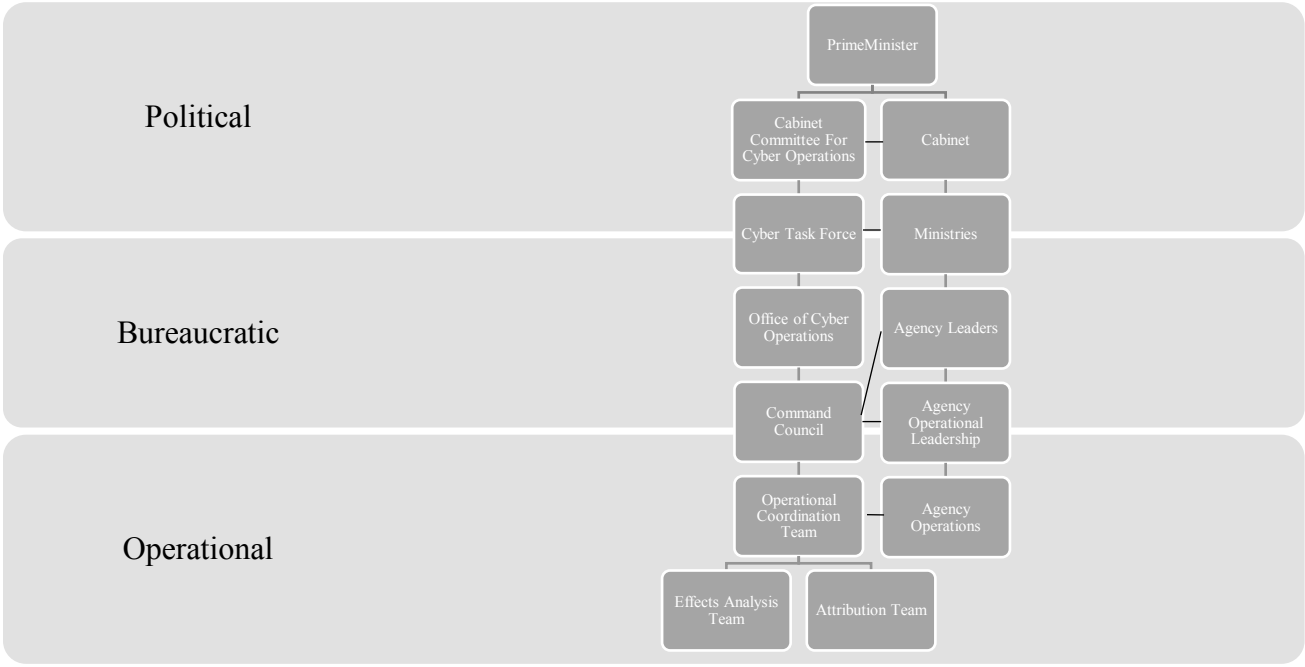


Figure 3 – Proposed Coordination Structure

Facilitating Factors

Independent of both coordination and capabilities are three other important factors that would be critical to the success of a comprehensive approach to cyber operations: communication, training and trust. Each factor is itself important, but the importance to integrating each factor with each other and then throughout the coordination and capabilities aspects of the comprehensive approach cannot be overstated.

Communication is an intentionally broad term that includes multiple aspects of information sharing. Full information sharing internally from task force to operational leadership to operations teams would be critical in areas of attribution and effects analysis. Understanding the anonymizing nature of cyber space technology means small nuanced bits of information would be critical to successful accomplishment of these tasks. The integration of information and intelligence from across the spectrum of government agencies as outlined in the CCSS and Table 1 earlier is another critical

enabler. Finding ways to pass security information effectively between government and private sector actors is another challenging but critical task. Yet there are still significant legal and organizational barriers that would have to be navigated to obtain this level of communication. These barriers become increasingly complicated when elevated to the international level. The rewards for overcoming these challenges are great. All countries face similar challenges given the global nature of cyberspace. It would be extremely limiting and ultimately self-defeating to not find a way to coordinate cyber operations with international partners, both governmental and non-governmental. Perhaps the most critical area of communication is between this collection of government security agencies and the public. Wide public communication can attain transparency of goals and efforts. The goal of these communications would be to enhance public trust. Achieving that goal requires significant effort and engagement by a wide range of interested parties who are also operational enablers, including privacy agencies, judiciary, bar associations and the public at large.

The second important factor is training. Training in this context means much more than just having qualified personnel occupy key jobs. A consistent challenge highlighted in comprehensive approach reviews has been lack of formal training given to civilian government personnel that compares to the rigours and depth of military staff colleges, particularly in areas like command and leadership.[236] In recent years, military staff colleges have opened to other government departments loading students into higher level programs, usually strategically focused. This type of cross-training would likely need to expand in different ways for comprehensive cyber operations. Inter-agency cross

[236] Chris Madsen, "Military Responses and Capabilities in Canada's Domestic Context Post 9/11," *Journal of Military and Strategic Studies* 13 No. 3 (Spring, 2011): 8.

training in technical as well as investigative areas would allow for the development of common understanding and perhaps even standardization of terminology, often the acronym bane of inter-agency operations.[237] Closely aligned with standard language is the ability of engaging in effective multi-agency after action or lessons learned processes. Particularly in the early states of operationalizing this comprehensive approach, the ability for every participant to learn from mistakes made allows greater opportunity for faster success and unit cohesion. Learning together as multi-disciplinary teams and being free to discuss and learn from mistakes made also enhances inter-team trust.

The final factor is trust. Already mentioned in both communication and training, trust has been recognized as a critical component in operations hoping to employ the comprehensive approach.[238] Like using the terms communication and training, trust also encompasses a wide range of relationships. By their nature, security agencies employ skeptical people, who have learned through years of hard experience that trust is more often earned than given. Large multi-national corporations also have significant self-interest in guarding information and protecting proprietary information. Interpersonal trust is often the key enabler by which government security operators and corporate employees can move forward with constructive operations. Trust often takes significant time to build and can be destroyed quickly.

Canadian security agencies engaged in cyber operations are already facing significant questions of trust. These questions come from the public, as revealed through media attention and demonstrations, and the courts revealed through a path of seemingly more restrictive views on governmental cyber operations. If a comprehensive approach to

---

[237] Christopher M. Schnaubelt, "Complex Operations and Interagency Operational Art," *Prism* 1 No. 1 (2009), 48.
[238] Dyndal, *NATO's Comprehensive Approach*…, 8.

cyber security operations is undertaken, it would be wise for leaders to devote considerable attention to issues of trust, both internally and externally. Some considerations for how these goals could be accomplished include Canadian cyber security policy that limits the most intrusive forms of cyber operations to only the most serious threats, both technical and human. Precedent resides in the way police are only allowed the use of wiretap for the most serious criminal offences.[239] Utilizing judicial oversight is another practical means of obtaining public trust. The benefit of judicial oversight is evidenced in comments from the Federal Court of Appeal tying CSIS credibility to judicial oversight of their operations.[240] Proactively designing a judicial oversight regime for all Canadian security agencies would likely be preferable than waiting for public outcry that has preceded past growth in this area. The way CSIS utilizes Federal Court oversight seems to be an effective way forward. It is conceivable that many peacetime cyber operations could use a combination of existing *Criminal Code* and *CSIS Act* provisions to obtain judicial authorization.

Each of these three enabling factors are intertwined in their practical application, and if done well, would likely result in cross-support for each. Multi-agency training fosters and enables better communication and enhanced trust for example. Overall, emphasizing these three factors in conjunction with the development of coordination and capability elements would be the backbone of the comprehensive approach to cyber operations by Canadian security agencies. Utilizing this approach would maximize Canadian operational capabilities and bring together currently isolated cyber operations. An effective comprehensive approach would directly address the shortcomings identified

---

[239] *Criminal Code*, s. 183.
[240] *Canadian Security Intelligence Service Act (Re)(TD)*…, 10.

by the Horizontal Evaluation and provide the best chance that Canadian cyber operations would comply with the rule of law across the spectrum of security agencies. Legal compliance would be accomplished by a central cyber security structure that could apply the best information of attribution, effects with political will to make operational decisions that started with what legal regime or regimes thought best to be applied. The central cyber security structure would also be able to coordinate real world operations in support of cyber operations, or vice versa, through jurisdiction of the security agencies depending on the legal regime applied. This level of effective central coordination would bring meaning to the Parliamentary intent written into the legislated mandates of each security organization to work in support of each other for the common security interests of Canada.

CONCLUSION

Fundamental principles that have served us well ought not be abandoned or set aside. As the cyber domain is an artificial system carrying out the day to day informational needs of billions of people, international and domestic law have an enormous impact on how it operates. This domain, unlike air, land and water, is not solely dependant on geography to organize agency jurisdictions. The comprehensive approach has the potential to most effectively manage cyber operations in Canada. Utilizing effective collaboration, Canadian security agencies will together manage cyber operations while reflecting and safeguarding Canadian values they were created to protect.

Basic understanding of how the cyber domain is organized and operates provided context for why attribution is among the most difficult challenges facing security agencies tasked with developing cyber operations capabilities. To manage these challenges, Canada developed the *Canadian Cyber Security Strategy* that engaged a wide array of government agencies with a stake in cyber operations. This policy took an effects-base approach to determining which defence or security agency had jurisdiction over any given cyber operation. Specifically, if the effect of the cyber operation impacted defence, then the CAF would have jurisdiction. If it impacted government infrastructure the CSE would have jurisdiction. If it involved a threat to national security, then CSIS would have jurisdiction and if a cyber crime, then the RCMP or other law enforcement agency would engage. A Horizontal Evaluation was conducted which evaluated the strategy and found that despite the best intentions, it suffered shortcomings. The shortcomings included poor communication, redundant capability development and

confused mandates for security agencies trying to conduct cyber operations. One explanation for these shortcomings was the legal basis upon which the various security agencies were required to operate, combined with a lack of recognition that three separate legal regimes may apply to Canadian cyber operations.

The law is generally slow to transform in the face of rapid technological change, however concerted efforts by international scholars have made tremendous progress in a few short years. The Tallinn Manual 2.0 set out operationally sound international law principles that found more agreement than disagreement. Wide consensus that traditional international legal frameworks can be modified to accommodate the explosive growth in cyber operations exists. Two international legal regimes possibly impact cyber operations. Peacetime international law governs most state interactions and most international cyber operations. LOAC engages upon the existence of an armed conflict to which at least one state is involved. The international law governing cyber operations utilizes thresholds reached mostly through effects-based analysis.

Despite wide consensus on basic international rules that govern cyber operations, significant uncertainty remains. Largely this uncertainty exists in state practice and application of the international law governing cyber operations. In the past several years cyber operations attributed to both state and non-state actors have created significant effects. State practice is still coming to terms with the scope and impact that these cyber operation effects are having. Canada is not excepted from these struggles to assess the impact of hostile cyber operations, what appropriate response options are available and conformity to international law.

To date, Canada has taken a largely defensive and domestically-focused response to hostile cyber operations. Publicly, available reports cite successive Canadian governments of different political parties consistently allowing hostile cyber operations to default to law enforcement jurisdiction. Recently, the current government has through policy statements expressed its intent to engage the CAF and CSE in "active" cyber operations that include both offensive cyber operations and active defence. CSIS has also recently been given new authorities to take tangible action, transforming the security agency from a purely intelligence function. The four main security agency's enabling legislation revealed that jurisdiction amongst Canadian security agencies is legally based on attribution analysis. Specifically, where geographically the operation took place, who was involved in the operation and why they were conducting it are key factors in what defence or security agency has jurisdiction.

Implicit in both the international and domestic legal analysis was the concept of political will. Evident in the executive political determinations required in both peacetime international law and LOAC, the concept of political will remains critical to a determination of the appropriate legal regime. Less overt, but equally important is political will applied in the domestic context. Through direction to defence and security agencies as well as through legislation and policy, political will has an important part to play in determining domestic jurisdiction for cyber operations. Privacy issues in cyberspace have both political and legal dimensions that are critical for Canadian security agencies to understand.

Recent Supreme Court of Canada privacy cases revealed a lack of technical evidence and understanding in leading decisions. Instead, questionable metaphors and

analogies are substituted for actual understanding of how cyberspace operates. In addition, disparate privacy concepts have been conflated to apply the *Charter* to cyberspace. The utilization of these techniques has led to arguably a failure to achieve the privacy protections sought by the judiciary while placing unnecessarily restrictive approaches to legitimate government cyber security operations. While the specific cases are undoubtedly of interest to any defence or security agency engaging in cyber operations, a broader point can be discerned from these decisions. Specifically, Canadian courts are taking a particularly broad application of *Charter* privacy protections in cyberspace. The broader point and one specific case serve to remind leaders in the cyber security field that privacy issues are ignored at the peril of effective cyber operations.

A proposed American pragmatic approach to privacy provides a more rational context for application of privacy law to cyber operations. Canadian security agencies should understand and adopt this approach because through it, specific cyber operation circumstances could be contemplated rationally and contextually. Broad circumstances such as information collection, information processing, information dissemination and invasion accommodate Canadian privacy jurisprudence and legislation. Security agencies analysing privacy issues in this way could bring appropriate information to the responsible decision maker, whether that be political or judicial, to encourage an informed decision. This pragmatic approach recognized that Canadian security agencies in day-to-day jobs are unique and beyond the everyday experience of most Canadians, including judges and politicians. Operating in the cyber domain is essentially a unifying circumstance for Canadian security agencies who face very similar challenges in this artificial environment.

The comprehensive approach offers the best way for Canadian security agencies to meet the various challenges presented in the cyber domain and specifically address the shortcomings identified in the Horizontal Evaluation. The comprehensive approach was recognized as nothing new, and Canada has recently employed this approach both domestically and internationally with reasonable success. The comprehensive approach allows a wide array of government agencies and non-government bodies to work together towards achieving common objectives.

Recent Canadian experience with the 2010 Vancouver Olympic domestic security operation and the counter-insurgency war in Afghanistan provided valuable lessons learned. Common challenges experienced with past attempts to operationalize a comprehensive approach informs understanding of cyber operations and how they might be collectively conducted and managed. Coordination and capability challenges were commonly reported. Issues around operational leaders receiving effective political and bureaucratic support and fragmentation of capabilities due to home agency priorities were identified as significant challenges.

Despite these challenges, the comprehensive approach is the best way to achieve the goals of the *Canadian Cyber Security Strategy* and to do so in accordance with the rule of law. Under a proposed theoretical structure, a cyber operations cabinet committee working in concert with a cyber operations task force based in the PCO provide the critical political interface with senior bureaucrats. The structure provides an effective conduit for the input of political will to determine the appropriate legal regime for specific cyber operations in a timely way. The PCO task force would possess the capacity to coordinate varied government departments. A PCO task force connected to operational

leadership through an office of cyber operations would provide the requisite level of bureaucratic authority to mitigate fragmentation from competing agency priorities. The task force model would also allow a variety of government departments to communicate at a strategic level. The office of cyber operations would also provide the bureaucratic to operational interface.

The command council would be responsible for evaluations of effect and attribution pertaining to cyber operations impacting Canada or proposed to be launched by Canadian security agencies. This structure would provide currently lacking operational communication, consistent cyber operational approaches and complementary capability development amongst agencies. Enabling the command council is an operational coordination team supported by an effects analysis team and attribution team. These teams would leverage the real-world operational capabilities of the contributing agencies and provide a pool of varied operational expertise. The pool of expertise would provide the basis for expert-to-expert consultation with provincial and municipal cyber operators, industry, business and other necessary collaborators. The integrated pool of expertise would also provide credible security-related information to political and judicial decision makers, as well as the public.

The comprehensive approach would be operationalized using this structure underscored by three key principles of communication, joint training and trust. All three principles have been recognized through experience as being critical to operationalizing a comprehensive approach successfully. Uniquely important to enabling effective cyber operations is the principle of trust. As demonstrated in both the political and judicial feedback to government efforts to promote cyber security, trust is the factor that underlies

most critiques of Canadian cyber security operations. Suggestions on how to advance trust included clear statements that intrusive cyber operations would only be used to pursue the most serious threats to Canadians and subject those cyber operations to proactive judicial review. Under this structure, judicial review could be obtained through existing CSIS and RCMP structures for most peacetime cyber operations.

Overall, the proposed organizational structure envisioned the effective operationalization of the comprehensive approach applied to Canadian security agencies. The structure was patterned after feedback from other Canadian operations that employed a similar approach. Based solidly on the way in which the cyber domain functions, this integrated approach leverages the strengths of existing security agencies. Foundationally, the structure supports government cyber operators effectively interacting with critical non-government enablers, such as ISP and multi-national companies. This interaction could be done with meaningful operational and political oversight. The goal of the *Canadian Cyber Security Strategy* was to meet the overall cyber threat to Canadians. Considering the legal and operational realities facing Canadian security agencies mandated to address that threat, the comprehensive approach offers a good chance for success.

BIBLIOGRAPHY

Adamson, Liisi. "Sovereignty in Cyberspace: Organized Hypocrisy?" Master's thesis, University of Tartu School of Law, 2016.

American Registry for Internet Numbers. "Regional Internet Registries," last accessed 28 March 2018, https://www.arin.net/knowledge/rirs.html.

Bailey, Christopher E. "Cyber Civilians as Combatants." *International and Comparative Law Journal* 8, no. 1 (2017): 4-22.

Bercuson, David J. and J.L. Granatstein, *Lessons Learned? What Canada Should Learn from Afghanistan*. Ottawa: Canadian Defence & Foreign Affairs Institute, 2012.

Bergman, Michael K. "White Paper: The Deep Web: Surfacing Hidden Value." *Journal of Electronic Publishing* 7(1) (August 2001): 1-27.

Bou-harb, Elias, Mourad Debbabi, and Chadi Assi. "Cyber Scanning: A Comprehensive Survey." *IEEE Communciations Surveys & Tutorials* 16, no. 3 (Third Quarter 2014): 1496-1519.

BrightPlanet. "Clearing Up Confusion – Deep Web s. Dark Web." last modified 27 March 2014, https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.

Brister, Bernard. "Family Relations: A Preliminary Analysis of the Use of the Comprehensive Approach at the Vancouver 2010 Winter Olympics." In *Security Operations in the 21st Century: Canadian Perspectives on the Comprehensive Approach*, 165-176. Edited by Michael Rostek and Peter Gizewski. Kingston and Montreal: McGill-Queen's University Press, 2011.

Buchan, Russell. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict & Security Law* 17 No. 2 (2012): 211-227.

Brown, Gary. "Spying and Fighting in Cyberspace: What is Which?" *Journal of National Security Law Policy* 8 (2016): 1-22.

Canada. Canadian Security Intelligence Agency. "CSIS-RCMP Framework for Cooperation One Vision 2.0, 10 November 2015." Access to Information Request Number 117-2015-645 – Documents Related to Frameworks for Cooperation with Key Government Partners. July 2016.

Canada. Canadian Security Intelligence Agency. *Who Said What? The Security Challenges of Modern Disinformation*. Ottawa: Canadian Security Intelligence Service, 2017.

Canada. Canadian Security Establishment Canada. "Briefing Binder C-59 November 29, 2017." Access to Information Request Number A-2017-00077 – CSE Briefing Binder Bill C-59. March 2018.

Canada. Communications Security Establishment Canada. "Foreign Signals Intelligence." last modified 2017-06-22 https://www.cse-cst.gc.ca/en/inside-interieur/signals-renseignement.

Canada. Department of National Defence, B-GJ-005-000/FP-001, *Canadian Military Doctrine*. Ottawa: DND Canada, 2009.

Canada. Department of National Defence, B-GL-300-003/FP-001, *Command In Land Operations*. Ottawa: DND Canada, 1996.

Canada. Department of National Defence, *Strong, Secure, Engaged Canada's Defence Policy*, Ottawa: Her Majesty the Queen in Right of Canada, 2017.

Canada. Government of Canada. *Canada's Cyber Security Strategy*. Ottawa: Her Majesty the Queen in Right of Canada, 2010.

Canada. Joint Doctrine Branch, Canadian Forces Warfare Centre. *Joint Doctrine Note - Cyber Operations*. Ottawa: Department of National Defence, 2017.

Canada. Public Safety Canada. *Horizontal Evaluation of Canada's Cyber Security Strategy Final Report*. Ottawa: Public Safety Canada, 2017.

Canada. Public Safety Canada. *Action Plan for Critical Infrastructure.* Ottawa: Her Majesty the Queen in Right of Canada, 2017.

Canada. Royal Canadian Mounted Police. *Cybercrime: An Overview of Incidents and Issues in Canada*. Ottawa: Her Majesty the Queen in Right of Canada, 2014.

Canada. Royal Canadian Mounted Police. *Royal Canadian Mounted Police Cyber Security Strategy*. Ottawa: Her Majesty the Queen in Right of Canada, 2015.

Combe II, Peter C. "Traditional Military Activities in Cyberspace: The Scope of Conventional Military Authorities in the Unconventional Battlespace." *Harvard National Security Journal* 7 (2016): 526-576.

Diab, Robert "Canada," In *Comparative Counter-Terrorism Law*, edited by Kent Roach, 78-114. New York: Cambridge University Press, 2015.

Dunlap Jr., Charles J. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* (Spring 2011): 81-99.

Dyndal, Gjert Lage. and Cornelia Vikan. "NATO's Comprehensive Approach: Still Something for the Future?" Paper presented at the *Norwegian Defence Command and Staff College Doctrine Conference*, Oslo, 25-26 June 2014.

Eichensehr, Kristen E. "The Cyber-Law of Nations." *The Georgetown Law Journal* 103, (2015): 317-380.

Firecompass. "Understanding Surface Web, Dark Web, Deep Web and Darknet." last modified 5 October 2017, https://www.firecompass.com/blog/darkweb-deepweb-darknet-browsers/.

Fitz-Gerald, Ann and Don Macnamara. "Comprehensive Security Requires Comprehensive Structures – How Comprehensive Can We Get?" *Strategic Studies Working Group Papers*. Ottawa: Canadian Defence & Foreign Affairs Institute, 2012.

Gammer, Nicholas. "The Afghanistan Task Force and Prime Ministerial Leadership: Tactical Retreat or a New Direction in Managing Canadian Foreign Policy?" *American Review of Canadian Studies* 43 No. 4 (2013): 462-476.

Gendron, Angela and Martin Rudner, *Assessing Cyber Threats to Canadian Infrastructure*. Ottawa: Canadian Security Intelligence Service, 2012.

Gladman, Brad and Peter Archambault. "A Role for Effects-Based Planning in a National Security Framework." *Journal of Military and Strategic Studies* 13 No. 2 (Winter 2011): 1-26.

Government of Canada. "Government of Canada Cyber Security Event Management Plan." last modified 11 December 2015, https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

Hathaway, Oona A. *et al,* "The Law of Cyber-Attack." *California Law Review* 100, (2012): 817-885.

Hogg, Peter. *Constitutional Law of Canada*. Toronto: The Carswell Company Limited, 1985.

Holzer, Corey T. "The Ethics of Hacking Back." *The Center for Education and Research in Information Assurance and Security* 1 (2016): 1-7.

International Corporation for Assigned Names and Numbers. "Domain Name Registration Process," last updated July 2017, https://whois.icann.org/en/domain-name-registration-process.

International Corporation for Assigned Names and Numbers. "Information for Registrars," last accessed 28 March 2018, https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en.

International Corporation for Assigned Names and Numbers. "International Domain Names," last accessed 28 March 2018, https://www.icann.org/resources/pages/idn-2012-02-25-en.

Int'l Grp. Of Experts at The Invitation of The NATO Coop. Cyber Def. Ctr. Of Excellence. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2017.

Kilovaty, Ido. "Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under International Humanitaran Law." Michigan Telecommunications and Technology Law Review 23 (2016): 113-151.

Leuprecht. Christian. "Conclusion." In *Security Operations in the 21st Century: Canadian Perspectives on the Comprehensive Approach,* edited by Michael Rosteck and Peter Gizewski, 237-247. Kingston and Montreal: McGill-Queen's University Press, 2011.

Madsen, Chris. *Military Law and Operations*. Toronto: Carswell, 2017.

Madsen, Chris. "Military Responses and Capabilities in Canada's Domestic Context Post 9/11." *Journal of Military and Strategic Studies* 13 No. 3 (Spring, 2011): 1-18.

Payne, Thomas. "Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations." *Lewis & Clark Law Review* 20, no. 2, (2016): 683-715.

Reed, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014.

Rotmann, Philipp. *Built on shaky ground: the Comprehensive Approach in practice*. NATO Research Paper No. 63. Rome: NATO Defense College, 2010.

Schmitt, Michael N. "Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework." *Institute for Information Technology Applications*, Research Publication 1 (June 1999): 1-41.

Schmitt, Michael N. "Cyber Operations and the Jus Ad Bellum Revisited." *Villanova Law Review* 56, no. 3 (2011): 569-606.

Schmitt, Michael N. "International Law and Cyber Attacks: Sony v. North Korea." *Just Security* (2014): 1-6.

Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal* 54, (December 2012): 13-37.

Schmitt, Michael N. "The Law of Cyber Warfare: *Quo Vadis*?" *Stanford Law & Policy Review* 25, (2014): 269-299.

Schmitt, Michael N. "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Anallytical *Vade Mecum*." *Harvard National Security Journal* Vol. 8 (2017): 239-280.

Schnaubelt, Christopher M. "Complex Operations and Interagency Operational Art." *Prism* 1 No. 1 (2009): 37-50.

Sharma, Dilip Kumar and A.K. Sharm. "Deep Web Information Retrieval Process: A Technical Survey." *International Journal of Information Technology and Web Engineering* 5(1) (January-March 2010): 1-22.

Sher, Jake B. "Anonymous Armies: Modern 'Cyber-Combatants' and Their Prospective Rights Under International Humanitarian Law." *Pace International Law Review* 28 (2016): 233-275.

Solove, Daniel. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 No. 3 (2006): 477-560.

Solove, Daniel J. "Conceptualizing Privacy." *California Law Review* 90, No. 4 (July 2002): 1087-1156.

Solove, Daniel. "*'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*." *San Diego Law Review* 44 (2007): 745-772.

Steiner, Hrafn. "Cyber Operations, Legal Rules and State Practice – Authority and Control in International Humanitarian Law," Master's thesis, Stockholm University Faculty of Law, 2017.

Tsagourias, Nicholas. "Cyber attacks, self-defence and the problem of attribution." *Journal of Conflict & Security Law* 17, no. 2 (2012): 229-244.

United Nations General Assembly. *Responsibility of States for Internationally Wrongful Acts*. New York: UN, 2002.

United Nations, *International Covenant of Civil and Political Rights*. New York: UN, 1976.

United Nations General Assembly. *Universal Declaration of Human Rights* New York: UN, 1948.

United Nations General Assembly. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN, 2013.

Wendling, Dr. Cécile. *The Comprehensive Approach to Civil-military Crisis Management. A Critical Analysis and Perspective.* Paris: Institut de Recherche Stratégique de l'Ecole Militaire, 2010.