National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Ethics in a Dangerous Cyberspace Time

Lieutenant-Colonel Melany Lepage

JCSP 47

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 47

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 47 – PCEMI 47

2020 – 2021

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

ETHICS IN A DANGEROUS CYBERSPACE TIME

By Lieutenant-Colonel Melany Lepage

TABLE OF CONTENTS

ABSTRACT

This paper sets out to answer if Canada can ethically conduct offensive cyber operations. It first describes case studies of cyber events through history. They are followed by a review of existing international laws and treaties and the ambiguities that exist as they apply to the cyber domain. The last chapter examines the difference between passive and active cyber defence, Canada′s current policies, the impacts of Canada conducting offensive cyber operations and concludes with ethical considerations. This paper argues that in order for Canada to conduct offensive cyber operations ethically, Canada, and more specifically, the Canadian Armed Forces (CAF) must build upon the existing codes of conduct and ethics already institutionalized within the CAF. This framework will augment the guidelines that already exist for decision-makers and cyber operators, such as the Tallinn Manual, and provide a Canadian-specific guide to improve decision-makers and cyber operators ethical guidelines.

INTRODUCTION

Cyber security and cyber attacks have become a prevalent topic in modern popular culture as seen in the news, books and movies. The media depict a Tom Clancy-like exciting story that dramatically results in a cyber attack yielding spectacular results, either through effects or massive data breaches. While the consequences of a cyber attack can be devastating to the victim, the sensationalized version of events gives the impression that cyber is a swift, accurate and weapon of choice for decision makers. The reality of cyber warfare diverges from the sensationalized version in many ways. Cyber operations are slow and deliberate, requiring the gathering of information and intelligence in order to develop an effective attack. The damage caused by a cyber attack is seldom permanent, and the outcomes do not usually result in physical damage.

Cyber is the wild west; cyber operators must navigate a grey space as the relevance of international laws and United Nations resolutions in the cyber domain are still being contemplated. With the recent assent of Bill C-59, which permitted Canada to adopt a more aggressive cyber posture, and the lack of clear guidance provided through international law, this leads to a debate of whether Canada should be conducting offensive cyber operations.

This paper will first provide an overview of some general cyber concepts and terminology commonly used. It will then examine six significant case studies that uniquely shaped the cyber domain. The following chapter will then review current policies, laws and frameworks including the Law of Armed Conflict and United Nations resolutions. The third chapter will also review the challenges and advantages as well as the difficulties of attribution in the cyber domain which in turn has implications on the

use of force concept when conducting cyber operations. Then, the chapter will explore the Just War Theory as it is applies to actions in the cyber domain, followed by an overview of the Schmitt Analysis criteria. The Schmitt Analysis criteria was a first attempt at framing the ethics of this new domain and defining how the principle of Use of Force applies to cyber attacks. The Schmitt Analysis criteria were later used as the foundation for the Tallinn Manual. That manual provides lawmakers, cyber planners and decision makers with a framework to guide them through the decision-making process when considering cyber actions. Finally, the fourth chapter will examine Canada's current policies and evaluate the impacts to Canada in operating in the offensive cyber operations space. The chapter will end with some considerations of how ethical guidelines may be developed for cyber operators. This paper will provide the background with a view to set out to answer the question: Should Canada be conducting offensive cyber operations? This paper will demonstrate that despite the uncertainties of the international laws in the cyber domain, Canada can operate ethically in the offensive cyber domain.

CHAPTER 1 — REVIEW OF GENERAL CYBER TERMINOLOGY

According to Canada's National Cyber Security Strategy, cyberspace is defined as "The electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 3 billion people are linked together to exchange ideas, services, and friendship."[1] Canadian Joint Doctrine Note defines the cyber domain as "All infrastructure, entities, users and activities related to, or affecting cyberspace."[2] On the other hand, the Department of Defense (DoD) Joint Publication 1-02 defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors."[3]

The Canadian National Cyber Security Strategy defines cybersecurity as "the protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information."[4] The safeguarding of digital information is not limited to equipment. It also includes process, best practices and mitigations measures. The Canadian Armed Forces (CAF) define cybersecurity as "the ongoing provision of service and support for the day-to-day use of cyberspace for day-to-day business such as sending emails, using network-based applications and collaborating."[5]

---

[1] Public Safety Canada, "National Cyber Security Strategy," ed. Public Safety Canada (Canada: Government of Canada, 2018), 34.

[2] Department of National Defence, "Joint Doctrine Note Cyber Operations," ed. Department of National Defence (Ottawa2017), 2-1.

[3] Department of Defense, "Joint Publication 1-02," in Department of Defense Dictionary of Military and Associated Terms (2016), 58.

[4] Canada, "National Cyber Security Strategy," 33.

[5] Defence, "Joint Doctrine Note Cyber Operations," 1-4.

A Denial of Service (DoS) attack is launched with the aim to degrade or deny the access to web based services or information available to legitimate users. “Threat actors design DoS attacks to exhaust a network′s resources such as its bandwidth, computing power and/or operating systems.”[6] Distributed Denial of Service (DDoS) is a denial of service attack executed through the installation of malicious code across many computers. “Multiple computers used to target one system simultaneously. This is achieved through the use of botnets.”[7] DDoS is a more sophisticated attack than a DoS as it may require more coordination as thousands of computers, controlled by several threat actors, is needed to carry out the attacks. The pay off could be significant for the threat actors as “DDoS incursions are deceptive in origin as they implicate the compromised hosts and not the actual threat actor.”[8]

Cyber warfare is described as the act of “employ[ing] computer network attacks as a use of force to disrupt an opponent’s physical infrastructure for political gain. This includes military cyber operations that degrade enemy data processing to facilitate an integrated assault during wartime.”[9] Canada’s Communications Security Establishment (CSE) provides some advice for Canadian Business and Government departments as to how to protect themselves against DoS attacks. Measures such as properly configured firewalls, router access controls, and procuring an Internet Service Provider (ISP) who

---

[6] Communication Security Establishment (CSE), "Cyber Journal," https://www.cse-cst.gc.ca/en/node/1493/html/25199#a2.

[7] Samuli Haataja, Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics, 1 ed. (Abingdon, Oxon;New York, N.Y;: Routledge, 2019), 114.

[8] (CSE), "Cyber Journal".

[9] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," Security Studies 22, no. 3 (2013): 372.

offers sufficient bandwidth to resist a DoS attack, are all ways CSE suggests Canadians can protect themselves.[10]

The United States DoD has categorized Computer Network Operations (CNO) into three sub-elements. Computer Network Defence (CND), which includes measures to protect their computer networks. Computer Network Attack (CNA) is considered the most aggressive sub-element under CNO. This element is set out to devastate or damage the target. The third element is Computer Network Exploitation (CNE) which refers to exploiting data on computer networks.[11] Canadian Joint Doctrine Note 02-2017 states that terms like CNO and CNA are now obsolete terminology, and they are replaced with concepts such as Offensive Cyber Operations (OCO) and Defensive Cyber Operations (DCO).[12] OCO is defined as "an offensive operation intended to project power in or through cyberspace to achieve effects in support of military objectives."[13] DCO is defined as "a defensive operation conducted in or through cyberspace to detect, defeat and/or mitigate offensive and exploitive actions to maintain freedom of action."[14] Of note, the doctrinal definition also elaborates to specify that DCO can include both passive defensive measures and as well as include actions in response to an event. These forms of cyber defence are also described as active and passive cyber defence.

Cyber attacks generally follow a typical cycle of three phases. The first phase of executing an attack in the cyber domain is preparation. This stage includes target identification, reconnaissance and intelligence gathering. The first phase is arguably the

---

[10] (CSE), "Cyber Journal".
[11] Kevin A. Elliott, "Active Cyber Defense and Attribution in Cyber Attacks" (ProQuest Dissertations Publishing, 2018), 10.
[12] Defence, "Joint Doctrine Note Cyber Operations," 7-3.
[13] Ibid., GL6.
[14] Ibid., GL4.

most important of the three. Stuxnet has proven the value of the combination of cyber planning conducted in conjunction with the application of accurate intelligence gathered against the target. While errors were still present in the Stuxnet code that allowed it to spread beyond the target. Mitigation measures were in place to ensure the code was only executable on the intended target. After the initial phase, a cyber attack will move into execution. In this phase, the target of the cyber attack is engaged by delivering the payload and the required installation procedures are initiated. The final phase of a cyber attack is the result phase. This is after the payload that was delivered by the malicious code initiates its execution, and the effects of the cyber attack are realized. [15]

[15] Nicholas Tsagourias and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges," European journal of international law 31, no. 3 (2020): 947.

CHAPTER 2 — REVIEW OF SIGNIFICANT CYBER EVENTS

The first section of this paper laid the foundation of basic understanding of some cyber concepts required for the remainder of the paper. This was achieved through the review of basic terminology and concepts relevant to the cyber domain. The understanding of the cyber domain will be further built upon in the upcoming section through the examination of significant cyber events through recent history.

Cybersecurity culture was starting to emerge as early as mid-20th century. In 1945, Rear Admiral Grace Murray Hopper used the term 'bug' when he discovered a moth was interfering with the Navy computer.[16] Jumping to the 1970s, the emergence of phone 'phreaking' started taking place. Phreaking is the term used to describe when hackers create a tone that allows them to make phone calls for free from pay-phones, as the technique allowed them to circumvent the billing system the telephone companies had in place.[17] Phone 'phreaking' became more accessible in 1972 when John Draper discovered the cereal Cap'n Crunch offered a toy whistle prize which emitted the exact frequency needed to phreak AT&T's pay-phone system, making this early cyber attack more accessible and mainstream.[18] This event could be considered the first step that started to shape what is thought of as a cyber event in the 21st century.

This section will examine six case studies:

- Morris Worm, which occurred in the early days of the Internet in 1988;

---

[16] Jason Andress and Steve Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 2nd ed. ed. (Elsevier, 2014), 291.

[17] James Adams, The Next World War: Computers Are the Weapons and the Front Door Is Everywhere (New York: Simon and Schuster, 1998), 172.

[18] Ibid., 173.

- 2007 cyber attacks on Estonia. Those attacks were a crucial catalyst to the development of frameworks specific to the cyber domain;
- Georgia in 2008 followed by Stuxnet in 2010, which was the first demonstration of cyber offensive action transitioning from the cyber domain, causing physical damage;
- The 2014 National Research Council spear-phishing attack; and
- The most recent high-profile cyber attack, the 2020 SolarWinds attack.

Morris Worm (1988)

The Morris Worm emerged on 2 November 1988 and was created by Robert Morris, a Cornell University student. [19] The Morris Worm highlighted the importance of cybersecurity and acted as a catalyst and wakeup call for the United States (US).

The Morris Worm had been designed to attack computers running a specific version of Unix operating system, but the worm quickly became out of control.[20] There were undetected errors in the code prior to initiation that had the unintended consequence of an increased rate of infection, infecting the same computer multiple times.[21] In total, the worm infected approximately 6,000 computers.[22] The mistake in the code resulted in slowing the internet down to unusable speeds.[23] The estimated damages the Morris worm caused vary dramatically, from $100,000 to $10 million.[24] In 1988, the internet was

[19] "The Morris Worm, the First Indictment under the Cfaa and Wake up Call of a New Age," (Santa Monica: Newstex, 2020).
[20] No publisher, "The Morris Worm," (Washington: Newstex, 2018).
[21] Jon Thompson, "The Morris Worm," Personal computer world (2009).
[22] publisher, "The Morris Worm."
[23] Steven Furnell and Eugene H. Spafford, "The Morris Worm at 30," ITNow 61, no. 1 (2019).
[24] "The Morris Worm, the First Indictment under the Cfaa and Wake up Call of a New Age."

estimated to have 60,000 devices connected, most of which were believed to be located in the United States.[25]

The Morris Worm resulted in many firsts and highlighted capability gaps in cybersecurity. Robert Morris was convicted under the Computer Fraud and Abuse Act, being the first person convicted under the Act. It forced the creation of the United States' first Computer Emergency Response Team (CERT). As well, developers sought out to create intrusion detection software.[26]

The Morris Worm demonstrated the vulnerability of the internet, the power of intrusion detection software and the impact of user education. It highlighted the need for enhanced cybersecurity, protection, education and network monitoring.

Estonia (2007)

Estonia has the reputation of being Europes most tech savvy country.[27] This reputation is in no small part due to their Tiger Leap program, which was launched in 1997. The program was aimed to foster the understanding and the appreciation of technology education in the school system.[28] Estonia has been described as "the most wired or connected country in the world."[29] By 2002, Estonia had issued electronic identification cards to all of its citizens. It was through these cards that Estonians could access government services online, everything from voting to social security services, and it was used to file taxes. The electronic identification card enabled the people of

---

[25] Furnell and Spafford, "The Morris Worm at 30."

[26] publisher, "The Morris Worm."

[27] Stephen Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity," Georgetown journal of international affairs 18, no. 3 (2017): 2.

[28] George Dewey Davis, III, "The Digital Fog of Cyber: Case Study of the 2007 Cyber Attack on Estonia" (ProQuest Dissertations Publishing, 2017).

[29] Ibid., 14.

Estonia to access several e-services from multiple government institutions.[30] By 2007, 97% of Estonians were using online banking services, and 60% were using the Internet on a daily basis.[31]

In April 2007, Estonia *poked the bear* when they decided to relocate a statue dedicated to Soviet soldiers who died in the Second World War.[32] For the Estonians, this statue represented their oppression under Soviet rule, and the monument was to be relocated two kilometres southeast.[33] These events unfolded in an unprecedented manner and were described by the president of Estonia as being "Web War One."[34] The cyber attacks lasted three weeks, in April - May 2007. While they were initially simple Denial of Service (DoS) attacks, they quickly evolved into Distributed Denial of Service attacks (DDoS). The DoS attacks occurred from 26 April until 29 April 2007, immediately following the removal of the Bronze Soldier memorial, and they were considered technically simplistic.[35] Many government websites and civilian services, such as banks and news sites, experienced DoS attacks. This attack rendered the services unusable by the citizens of Estonia due to the high volume of traffic experienced. [36] As the conflict developed, so did the techniques the cyber attackers used. They moved to DDoS, which involved the using a botnet that was estimated to include thousands of computers from

---

[30] Haataja, Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics, chapter 5, p 2.

[31] Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity," 2.

[32] Alex Rodriguez, "'Cyber Attack' Strikes Estonia; Ominous Denial-of-Service Campaign Wreaks Havoc: Final Edition," The Ottawa citizen (1986) 2007.

[33] Haataja, Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics, 112.

[34] Ibid., chapter 5, p1.

[35] Ibid., 113.

[36] Andress and Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 12.

178 countries.[37] The DDoS attacks reached their peak on 9 May 2007, where the traffic volume experienced in Estonia reached as high as 90 Mbps, a departure from their usual traffic levels of just under 10 Mbps. It is speculated that the abrupt reduction in volume on 10 May 2007 was due to the expiry of the botnet rental contract.[38]

While the cyber attacks on Estonia have not officially been attributed to Russia, many organizations, including industry, governments and Estonia themselves, believe they were behind the events. US Intelligence and Cyber Law & Business Report have attributed the actions on Estonia to Russia.[39]

Fortunately, Estonia had a well-established CERT which was able to mitigate the attacks by implementing a two-pronged approach. They first increased the bandwidth to servers hosting government services under attack, which enabled them to accommodate the increased traffic. Secondly, they were able to filter out traffic that was suspected of contributing to the DDoS attacks.[40] Shortly after the cyber events, the Estonian Minister of Defence attended a meeting with fellow European Union defence ministers. At that meeting it was agreed that future cyber attacks must be responded to in a swift manner. The Estonian Minister of Defence described the events in that forum as the "scale of damage and the way these cyber attacks have been organized, we can compare them to terrorist activities."[41]

---

[37] Haataja, Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics, 114.

[38] Ibid., 115.

[39] Davis, "The Digital Fog of Cyber: Case Study of the 2007 Cyber Attack on Estonia," 50.

[40] Haataja, Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics, 115.

[41] Ibid., 117.

The impact of the cyber attacks on Estonia were not insignificant. The economic impact of the attacks were estimated to be up to USD 40.5 million.[42] The attacks highlighted an institutional gap and the realization of the increased threats that exist in the cyber domain. This conclusion led to the formal accreditation of the Cooperative Cyber-Defense Center of Excellence (CCDCOE) by NATO on 14 May 2008. At that time CCDCOE was created through Estonia's initiative and they were joined by Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain.[43] The pinnacle accomplishment to date of CCDCOE is the creation of the Tallinn Manual, and in 2017 CCDCOE expanded upon their first iteration and released an updated version, "Tallinn Manual 2.0 on international Law Applicable to Cyber Operations".[44]

Georgia (2008)

The cyber conflict against Georgia in 2008 is an interesting case study where the attacks occurred concurrently with conventional warfare. This was the first time cyber attacks were used in conjunction with kinetic actions.[45] As with events in Estonia, Russia is believed to be involved in this cyber conflict. Both Georgia and Russia are suspected of having conducted information operations during the battle.[46] Unlike Estonia, this cyber conflict was met with information operation countermeasures from Georgia through the use of international media. However, Georgia was not believed to be technologically

---

[42] Ibid., 115.

[43] CCDCOE, "Ccdcoe," https://ccdcoe.org/about-us/.

[44] Ibid.

[45] Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," Parameters (Carlisle, Pa.) 47, no. 2 (2017): 52.

[46] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," Security dialogue 43, no. 1 (2012): 43.

advanced to position them to conduct cyber counter attacks nor cyber defence during the operations.[47]

Despite the wide belief that the Georgian attacks have originated from Russia they have not been formally attributed to the Russian government or military.[48] However, some experts have observed that the timing of the attacks relative to conventional military actions is noteworthy. This correlation may be significant as the experts continue to argue that if these attacks originated from the Russian government, it would be an important indicator as to the significance of the cyber domain as it relates to Russian declared assets in military conflicts.[49] Some researchers have observed a link between state actors and cyber activities as the timing of both kinetic and cyber actions seemed to be coordinated. The conventional phases of operations seemed to be synchronized with cyber events. A report pointed out this evidence in a publicly available unclassified summary of a Top Secret document written by the U.S. Cyber Consequences Unit (US-CCU). In the summary of the report, it states that: "The organizers of the cyber attacks had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out."[50] While the URL to the report summary is now broken, these claims are corroborated by an article released by CNN.[51] Additionally, the North Atlantic Treaty

---

[47] Ellada Gamreklidze, "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia," Journal of international communication 20, no. 2 (2014): 211.

[48] Andress and Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 12.

[49] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," 13.

[50] Nart Villeneuve, "Ru-Ge Skepticism," http://www.nartv.org/2009/08/25/ru-ge-skepticism/.

[51] Jeanne Meserve, "Study Warns of Cyberwarfare During Military Conflicts," CNN, http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html.

Organization (NATO) Review magazine website makes brief mention of the coordination on their website.[52]

Contrary to Estonia, Georgia is not considered as technologically advanced and unable to maintain sufficient cyber security.[53] This observation has led some experts to conclude that nations who are developing their digital footprint are at an increased level of cyber vulnerability regardless of the size of their dependence on technology.[54]

In response to the attack, Georgia authorities started to filter internet traffic originating from Russia.[55] However, this action became a self-censorship action. Much of the internet infrastructure in Georgia was routed through the Russian Business Network (RBN), which the hackers also used during the cyber attacks.[56]

The impacts of the cyber attacks were widely felt across the country, impacting many of the services available to the citizens. “The attacks successfully denied citizen access to 54 websites related to communications, finance and government.”[57] As a result of the cyber attacks, banks closed their ATMs and no longer offered online services. These actions created panic across the population as Georgians attempted to withdraw funds, ultimately resulting in the closure of all financial institutions until the cyber attacks were resolved as described below.[58] The cyber attackers defaced Georgian government websites.The government did not have an effective means to communicate with their

---

[52] "Nato Review Magazine," https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm.

[53] Gamreklidze, "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia," 201.

[54] Ibid.

[55] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," 6.

[56] Ibid., 4.

[57] Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," 52.

[58] Gamreklidze, "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia," 211.

citizens as the DDoS attacks impacted not only the government websites but also the media outlets. This lack of information and communication internally within Georgia, caused either by the cyber attacks or the unintended self-censorship, created panic across the population.[59] The cyber attacks executed by Russia and the "unintended consequences of Georgia's self-imposed censorship helped amplify the success of Russian military strikes against Georgia's communications infrastructure and may have strengthened Russia's narrative in the CIS region."[60]

Weeks after the conflict began, Georgia was able to gain the upper hand in the information war and regain control over its information technology. This was accomplished through Georgia turning for help from other nations through the use of web hosting services distributed to other countries, such as the USA.[61] Concurrently, while the conventional military actions and cyber attacks were ongoing, both Russian and Georgian agencies "appreciated the importance of strategic communication, and targeted domestic and international media in order to narrate the intent and desired outcome of the conflict."[62]

During the conflict, sites the United States, as well as other countries that offered hosting services for Georgia's websites, also became targets of the DDoS attacks.[63] One example is the company TSHot, based in Atlanta, offered to host some of Georgia's online services. This well-intended act had severe consequences. The CEO of the

---

[59] Ibid.

[60] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," 12.

[61] Peter Svensson, "Georgian President's Web Site Moves to Atlanta," USA Today, 11 August 2008.

[62] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," 4.

[63] Ibid., 11.

company, an expatriate from Georgia, did not inform the authorities in the United States about their offer to provide these services.[64] Georgia's government also moved other online services to Estonia, France and Poland, which mitigated the impacts of the immediate damage the cyber attacks caused. Despite the mitigating stopgap measures that were put in place thanks to allies, "they nevertheless assess the consequences of the cyber attacks as strategically important and related to the country's communication infrastructure, cyber and political capabilities."[65] While it is believed that Russia won the kinetic conflict with Georgia, the victor of the information operations portion of the campaign and hearts and minds of the international community was Georgia.[66] Their victory over the information operations domain can be observed through media reports praising Georgia over the public relations posture throughout the conflict.[67]

The cyber conflict between Georgia and Russia is a significant incident in cyber warfare history. The events demonstrated correlations between conventional military actions in traditional domains, such as land warfare, and the relationships between the conventional domains and cyber. The events also showcase how non-state actors can have dramatic impacts on kinetic operations. It demonstrated the consequence cyber effects could have on a country during conventional military warfare and how the cyber domain can be used to win the conventional war.

The impacts of cyber actions during the conflict can be demonstrated in two ways. The first is the sequencing or timing of cyber attacks relative to the timing of kinetic

---

[64] Ibid.

[65] Gamreklidze, "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia," 212.

[66] Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," 54.

[67] Peter Wilby, "Georgia Has Won the Pr War," The Guardian, 18 August 2008.

effects. On 9 August 2008, Georgia news agency Novosti-Gurzija experienced a DDoS account and the website of the Georgian Ministry of Foreign Affairs was defaced. The same day, Russia conducted an airstrike on Gori and sank a Georgian missile boat. This is just one of several examples throughout the conflict of cyber attacks coinciding with kinetic effects. The second way the cyber attacks had an impact on the kinetic mission was that it hindered the military's ability to communicate. "Georgian tactical communications failed, and Russian kinetic strikes against key communication facilities severely restricted communication with the national common authority."[68] The events exemplified the importance of cyber security and the inverse relationship between the importance of cyber security relative to the size and dependence of a nation's digital footprint. The events also exemplified the impact of operations in the cyber domain and the impact of information denial on a population.

Stuxnet (2010)

The Stuxnet cyber attack was an incredibly sophisticated demonstration of the strategic effects the cyber domain can have on an adversary. It is considered the first cyber attack that their effects were observed outside the cyber domain as the attack directly resulted in physical damage.

As a result of increasing concerns throughout many parts of the world regarding Iran's nuclear program, several United Nations Security Council Resolutions were put in place between 2006 and 2008. The resolutions stipulated Iran's uranium enrichment program was to be halted until Iran implemented safeguards.[69] The concerns surrounding

[68] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," 10.

[69] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 379.

Iran's nuclear program go back as far as 1984. On 19 January 1984, the US Department of State began imposing sanctions against Iran in response to their morning concerns. In September 2003, the International Atomic Energy Agency (IAEA) board of governors approved a resolution for the suspension of Iran's nuclear program. A condition of this resolution was to establish regular inspections conducted by IAEA in all Iranian nuclear facilities, set to comment in October 2003.[70] During these inspections it was observed Iran did not fully cooperate with the Security Council resolutions. Iran had claimed their nuclear research and development were required to meet the national energy demands. However, the resistance to cooperation fuelled suspicions that Iran was in violation of the Nuclear Non-Proliferation Treaty. During the investigation, the IAEA could not determine if a nuclear weapons program was underway.[71]

The Stuxnet program was initiated under the George W. Bush administration. It was known as Olympic Games. The initiative accelerated once Barrack Obama took office. It became a joint initiative between the United States (US) and Israel as the US used the cyber domain as a strategic and political tool to influence Israel. Israel was prepared to conduct airstrikes against Iran, and the possibilities Stuxnet presented persuaded Israel to partner with the US. Not only was this partnership advantageous as the US was able to conduct an attack against Iran in the domain of their choosing, but in order to execute their plan and deliver the payload as they envisioned it, they needed access to the Iranian networks. Israel's covert intelligence network provided the cyber

---

[70] Julia Masterson, "Timeline of Nuclear Diplomacy with Iran," Arms Control Association, https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran.

[71] Clare Stevens, "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet," Contemporary security policy 41, no. 1 (2020): 142.

planners with the details required to develop the malware. Ultimately, Stuxnet proved to be effective and less costly as it did result in physical damage to Iran's centrifuges, as described later in this paper.[72]

Stuxnet displayed the powerful combination of carefully gathered intelligence and programming. The meticulous precision that was considered when programming Stuxnet was astonishing. The success of Stuxnet was in no small part due to the attention to detail, as the program was able to navigate the Industrial Control System (ICS) network undetected to deliver its payload. The features of the code paralleled the details known about the Natanz nuclear facility.[73] "Cyber planners must gather intelligence on the mechanical and organizational dimensions of their target, gain access to the targets computer network, exploit vulnerabilities to navigate through the network to the ICS."[74] The Stuxnet program code demonstrated the importance of effective and accurate intelligence gathering and how cyber planners and code writers can leverage those details to produce successful malware.

It is estimated that Stuxnet was able to infect anywhere from 50,000 to 100,000 computers, 58% of which were located in Iran. It is believed that other countries that were infected with Stuxnet include, but are not limited to, Azerbaijan, India and Indonesia.[75] Since the malware was searching for specific features found in the Iranian facilities, the payload was dormant. However, some collateral damage did occur. For example, India reports that the attack affected a satellite.[76]

---

[72] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 385.
[73] Ibid., 383.
[74] Ibid., 378.
[75] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," Computer (Long Beach, Calif.) 44, no. 4 (2011): 92.
[76] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," Survival (London) 53, no. 1 (2011): 34.

As the centrifuges were controlled through an air-gaped system, the malware had to go through many steps in order to start executing. It is suspected that the worm was first introduced through the use of a USB memory stick which was left on the ground surrounding the facility. The centrifuges are controlled by Programmable Logic Controllers (PLCs), which are "special computers that are optimized for control tasks and the industrial environment."[77] The PLCs were the brains of the centrifuges; they controlled all aspects, including the rotation speed. One of the methods used to deliver the Stuxnet payload to the centrifuges was through the use of removable media or email attachments. The hope was the worm would eventually make its way to an engineer or programmer who was responsible for the configuration of the PLCs.[78] Once Stuxnet made its way to the PLC, the conditions would be set to activate the once dormant code.[79]

The cyber planners behind the Stuxnet code were able to conceptualize a plan to deliver a payload in the cyber domain that would result, over time, in physical damage to equipment through the override of rotation speed. "Stuxnet alternated the frequency of the electrical current that powers the centrifuges causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed for."[80] While the centrifuges were experiencing changes in rotating speeds, the operators were receiving altered data stating the rate of rotation was consistent.[81] This deception prevented the sounding of alarms and the detection of Stuxnet. Stuxnet demonstrated to

---

[77] Samuli Haataja, "Stuxnet," (Routledge, 2019), 141.
[78] Ibid.
[79] Stevens, "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet," 145.
[80] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 24.
[81] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 384.

the world that malware could expand beyond the cyber domain and cause physical damage to infrastructure.[82]

Stuxnet was able to demonstrate unprecedented capabilities. “The genius of the worm is that it can strike and reprogram a computer target.”[83] The composition of Stuxnet was unique compared to malware that was typically discovered at the time. It exploited four zero-day vulnerabilities; malware usually exploits one zero-day vulnerability. Unlike common malware, the Stuxnet code had a specific target and was extremely selective. Despite the attention to detail and research performed by the team who created Stuxnet, collateral damage was observed on unintended targets. Malware is commonly passed through the internet and networks; Stuxnet first had to be propagated through the use of external memory devices to bridge the air gap problem. The last distinctive characteristic that set Stuxnet apart from common malware was its size. Stuxnet was about 500 Kilobytes which was almost half the size of typical malware.[84] These unique features enabled Stuxnet to evade antivirus detection programs and steal digital certificates. These features permitted Stuxnet to present a facade of a legitimate program.[85]

The final result of Stuxnet is up for debate. The Americans believe the repeated acceleration of the centrifuge past the operating limits resulted in damage of 948 out of approximately 9,000 centrifuges at Natanz.[86] Supported by the reports by IAEA, who

---

[82] Chen and Abu-Nimeh, "Lessons from Stuxnet."
[83] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 24.
[84] Chen and Abu-Nimeh, "Lessons from Stuxnet."
[85] Stevens, "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet," 139.
[86] Haataja, "Stuxnet," 145.

observed through security camera footage located around the perimeter where the centrifuges are housed, that approximately 10% of the centrifuges at Natanz were dismantled. This was observed within the timeframe Stuxnet was believed to have occurred.[87]

The Iranians claim that Stuxnet did not damage the system, but they do admit the malware had infected some computers at the facility.[88] While the Iranians claim no damage to the centrifuges occurred through the execution of Stuxnet, the confidence in the equipment dwindled. The Iranians had assigned employees at the Natanz facility to monitor the equipment and report their observations through a radio net.[89] When deliberating if the Stuxnet malware is considered to have exceeded the threshold of use of force, it depends from which perspective or version of the truth the impact of Stuxnet is being examined. Consider for a moment, the American's assessment of the damage Stuxnet had caused is accurate. In that case, the events could be assessed as exceeding the threshold due to the assumption that the malware caused permanent damage to the centrifuges at the Natanz facility.[90] When examining the use of force exerted when considering the Iranian account of the damage Stuxnet caused, a different conclusion can be deduced: "only weak grounds for arguing that it represented the use of force, armed attack or aggression under the UN Charter."[91] This conclusion was drawn by James P. Farwell and Rafal Rohozinski, after evaluating the circumstances surround Suxnet, use of force and UN Article 2(4) and Article 51.

---

[87] *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics, 145.*
[88] Chen and Abu-Nimeh, "Lessons from Stuxnet," 92.
[89] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 392.
[90] Haataja, "Stuxnet," 137.
[91] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 29.

Stuxnet showcased the power that can be harnessed within the cyber domain when cyber planners leverage intelligence gathered on a target. The intelligence-gathering enabled the creation of unique characteristics to penetrate the network and evade detection. When combined with the execution of four zero-day exploits, it contributed to the unprecedented success of Stuxnet, at least in the short term. The unparalleled transition of an attack in the cyber domain to kinetic effects illustrated to the world the power of deliberately planned and executed cyber warfare.

National Research Council (2014)

In July 2014, Canada, more specifically the National Research Council (NRC), became the victim of a state-sponsored spear-phishing attack originating from China.[92] The Communications Security Establishment detected the attack.[93] The Canadian Cyber Incident Response Centre describes the attack as "textbook moves commonly seen in state-sponsored digital assaults."[94] It is unknown exactly what intellectual property China was able to secure; however, the NRC had been working on many exciting projects at the time, including highly secure quantum communications, as well as DNA sequencing.[95] Original estimates of the financial implications of the attack were estimated to be around $32 million,[96] but years later, estimates grew to hundreds of millions of dollars.[97] These

---

[92] Jim Bronskill, "Chinese Hackers Attacked National Research Council Computers," The Canadian Press, https://www.ctvnews.ca/mobile/canada/chinese-hackers-attacked-national-research-council-computers-1.2146400.

[93] The Canadian Press, "Canadian Spies Say Chinese Hacked National Research Council," Maclean's 2021, no. 28 April (2014).

[94] Bronskill, "Chinese Hackers Attacked National Research Council Computers".

[95] Press, "Canadian Spies Say Chinese Hacked National Research Council."

[96] Janice Dickson, "Chinese Hackers Trigger Government Request to Spend $32.5 Million," iPolitics, https://ipolitics.ca/2015/02/19/chinese-hackers-trigger-government-request-to-spend-32-5-million/.

[97] Colin Freeze, "China Hack Cost Ottawa 'Hundreds of Millions,' Documents Show," The Globe and Mail, https://www.google.ca/amp/s/www.theglobeandmail.com/amp/news/national/federal-documents-say-2014-china-hack-cost-hundreds-of-millions-of-dollars/article34485219/.

actions on the NRC are only significant for the cost ensured by the government of Canada but also the potential loss of intellectual property. “The research agency had hoped that such technology would position Canada as a global leader in [the] field of quantum cyber security.”[98]

When iPolitics asked Deepa Kundar, a computer engineer and cyber security expert, about the plan to clean up the cyber attack and incorporate new secure communications, they said: “I think there’s a long-term response that’s needed. In the short term it’s definitely needed but in the long term I think there needs to be great investment in training and developing individuals in the field of cyber security.”[99]

In addition to financial and intellectual property implications, the cyber attack also created political strains. At the time of the attack, “Foreign Affairs Minister John Baird [was] in China laying a path for a visit there [that] fall by Prime Minister Stephen Harper.”[100] The attack had further strained relations between Canada and China as “[g]overnment officials publicly […] took the unusual step of openly blaming the intrusion on a highly sophisticated, Chinese state-sponsored player. Beijing has denied involvement, accusing Canada of making irresponsible charges.”[101]

This attack was significant for Canada, it resulted in financial loss, intellectual property compromise, and strained political relationships.

SolarWinds (2020)

The SolarWinds cyber attack is one of the most recent high-profile cyber prolonged infiltration, being reported on 17 December 2020 by Microsoft. The attack

---

[98] Press, "Canadian Spies Say Chinese Hacked National Research Council."
[99] Dickson, "Chinese Hackers Trigger Government Request to Spend $32.5 Million".
[100] Press, "Canadian Spies Say Chinese Hacked National Research Council."
[101] Bronskill, "Chinese Hackers Attacked National Research Council Computers".

capitalized on a back door that was discovered in the SolarWinds software, a systems management software. Through this backdoor, malicious software was able to be installed, eventually reaching more than 18,000 companies and US government departments.[102] The Cybersecurity and Infrastructure Security Agency (CSIA) stated that the SolarWinds cyber attack "*poses a grave risk* to the federal government along with state and local governments and critical infrastructure."[103] While the malware was able to reach the US Department of Energy, it was unable to compromise the computer systems, fortunately avoiding adversely affecting "mission essential national security functions."[104] Microsoft was able to quickly patch the vulnerability once discovered.[105] In the alert bulletin that was released advising the public against the malware, the CISA described the adversary as: "This is a patient, well-resourced, and focused adversary that has sustained long duration activity on victim networks."[106] Although not officially attributed, the US government believes Russian intelligence organizations are the perpetrators of the attack.[107] Examining the problem set, the experts recognize the importance of information sharing, not only between government agencies monitoring the cyber domain but also between partners in industry.[108]

---

[102] Barbara Kollmeyer, "'Effectively, an Attack on the United States.' Microsoft Gets Caught up in Solarwinds Cyberattack," no. Journal, Electronic (2020).

[103] Robert Walton, "Doe Confirms Its Systems Were Compromised by Solarwinds Hack," (Washington: Industry Dive, 2020).

[104] Ibid.

[105] Kollmeyer, "'Effectively, an Attack on the United States.' Microsoft Gets Caught up in Solarwinds Cyberattack".

[106] Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," Cybersecurity and Infrastructure Security Agency, https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[107] Walton, "Doe Confirms Its Systems Were Compromised by Solarwinds Hack."

[108] "Russia's Solarwinds Hack Was Espionage, Not an Act of War: Technology Companies Are Incensed, but the Federal Government Is More Sanguine," (Washington, D.C: WP Company LLC d/b/a The Washington Post, 2020).

Impact of the Cyber Events

The six events described above provide significant insights into key aspects of cyber attacks. The Morris Worm demonstrated early on the unintended reach, and collateral damage cyber attacks may inflict due to errors made by the cyber attackers. The attacks on Estonia resulted in the acknowledgement that more policy and legal frameworks need to be developed in order to effectively and lawfully navigate within the cyber domain. Thanks to the conflict in Estonia, the Tallinn Manual was created, which law makers and cyber planners use to ethically guide them through the cyber domain as cyber action is considered. The conflict within Georgia was the first conflict that gave indications of how powerful cyber operations could be when used in conjunction with kinetic effects. Stuxnet, considered the first cyber action to cross domain from cyber activities to physical damage, demonstrated the power of intelligence gathering as it relates to cyber planning. Had the cyber planning team not taken time to understand the problem space, and they did, the malware may not have been as effective. The Canadian NRC example demonstrated the power of China's ability to gather information and the political strain that may result Finally, SolarWinds highlighted the importance of collaboration and intelligence sharing between industrial partners and government organizations. The more recent cases have demonstrated the lack of international legal mechanisms to deal with cyber attacks across National boundaries.

CHAPTER 3 — CYBER AND THE LAW

Some argue it is still early days in the cyber domain, and the regulations and laws will develop as familiarity with the technology in the domain increases.[109] However, the cyber domain is considered vital to many nations with respect to national security.[110] Can vital ground wait for time to resolve the critical gaps in international law, policy and frameworks in the cyber domain? There are several areas where more information is required, and advancement needs to occur to improve the regulation of the cyber domain. This chapter will examine some of the legal and ethical frameworks, laws and concepts that are available to cyber law makers, planners and decision makers – first, an examination of the Law of Armed Conflict and how it applies to the cyber domain. Then there will be an examination of the United Nations and how some of the resolutions may help or hinder regulating actions within the cyber domain. The challenges surrounding attribution and the importance of attribution in the cyber domain will then be addressed. A brief discussion of the use of force and the debates surrounding its applicability to cyber warfare and the cyber domain will follow. Furthermore, there will be a discussion of Just War Theory as it applies to the cyber domain.

An overview of the Schmitt Criteria is next. The Schmitt Criteria was one of the first tools available to the cyber community intended to contextualize laws put in place before the prevalence of information technologies. The Tallinn Manual is then examined, the ground breaking role it fulfills as it attempts to bridge the gaps of the above

---

[109] George Lucas, Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare (Oxford University Press, 2017), 42.

[110] Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," European Conference on Information Warfare and Security (2010): 177.

mentioned laws, policies and frameworks in place to serve cyber planners and law makers better as they navigate cyber conflicts in the cyber domain.

Law of Armed Conflict

The first aspect that should be considered when analyzing cyber warfare is the Law of Armed Conflict (LOAC) and how it applies to the cyber domain. James P. Farwell and Rafal Rohozinski state in their article that "[t]he Law of Armed Conflict and UN Article 51 effectively condition self-defence upon proving the attacker's identity. It is not clear what degree of certainty in identification is required to justify a response."[111] This interpretation is not uniformly accepted in the world of cyber warfare, as article 51 plainly states "if an armed attack occurs."[112]

Much of the infrastructure in the cyber domain is considered dual-use. Meaning the infrastructure and equipment are used for both civilian and military operations. At some point, it is reasonable to assume that most cyber attacks will transit through, reside or be prepositioned on telecommunications infrastructure used by the civilian population, either through the communication lines, data centres, etc. While cyber attacks may be permitted on these dual use systems according to LOAC, cyber attack's secondary effects must be considered. These effects are difficult to determine when attacking through dual use systems or equipment. This has an impact on the proportionality factor as it is difficult for the commander to anticipate the degree to which collateral damage is expected to be due to the vast degree of dual-use equipment contained in the cyber domain. The LOAC does not permit an attack if the collateral damage on the civilian population exceeds the military advantage gained for the attack to be successful. It is also

[111] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 35.
[112] United Nations, "UN Article 51," (United Nations).

expected that a commander must anticipate through reasonable means the degree of collateral damage. Therefore, it could be argued that since the degree of interdependencies between dual use and civilian infrastructure is so extensive, it is not reasonably feasible for a commander to accurately anticipate all the possible secondary effects of a cyber attack, so such attacks could be considered illegal under LOAC.

Consequently, there are two areas of responsibilities expected of a commander when considering a cyber counter attack as it applies to proportionality under LOAC. The first is determining the target or actor, to include if it is a state or non-state actor. The second is to determine what type of attack, armed or unarmed, was initially executed.[113]

United Nations

One of the several debates in the cyber domain is surrounding United Nations (UN) Article 2(4). "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[114] The wording 'use of force against the territorial integrity' in Article 2(4) some have argued does not apply in the cyber domain as the act of cyber attack and cyber warfare, generally speaking, does not involve entering adversarial land and crossing borders into their territory.[115] Under this interpretation, the victim of a cyber attack may have little recourse in the context of Article 2(4).

---

[113] Eric F. Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework," Strategic studies quarterly : SSQ 8, no. 1 (2014): 114-17.

[114] "Charter of the United Nations Chapter I," United Nations, https://www.un.org/en/sections/un-charter/chapter-i/index.html.

[115] James A. Green, Cyber Warfare: A Multidisciplinary Analysis, 1 ed., Routledge Studies in Conflict, Security and Technology (Routledge, 2015), 99.

Three conditions are required to be met in order for Article 2(4) to be applicable to operations in the cyber domain. The first is that the cyber attack must be attributed to state actors. The second condition is "the cyber operation must amount to either a 'threat' or a 'use of force'"[116] The last condition is that the use of force or threat must be exercised on the international stage and impact international relations.[117]

An additional UN article that may apply is Article 51, which permits acts of self defence.[118] UN Article 51 states,

> "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."[119]

Note that "under the traditional standard, most cyber attacks will not violate Article 2(4), and thus do not enable Article 51 self-defence."[120] UN articles also permit authorization of use of force by the UN Security Council. These circumstances are outlined under UN Articles 39–42.[121]

Article 8 under United Nations General Assembly Resolution 56/83 outlines the Responsibility of States for internationally wrongful acts states: "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[122] This resolution may provide an

---

[116] Carlo Focarelli, "Self-Defence in Cyberspace," (Edward Elgar Publishing, 2015), 234.
[117] Ibid.
[118] United Nations, "Charter of the United Nations Chapter Vii," https://www.un.org/en/sections/un-charter/chapter-vii/index.html.
[119] "UN Article 51," 429.
[120] William C. Banks and Evan J. Criddle, "Customary Constraints on the Use of Force: Article 51 with an American Accent," Leiden journal of international law 29, no. 1 (2016): 88.
[121] Nations, "Charter of the United Nations Chapter Vii".
[122] "UN Doc a/Res/56/83," (United Nations, 2002).

avenue for recourse under international law for victims of cyber attacks carried out by companies or people hired by the State. While this article offers some framework for recourse under international law, some questions remain unanswered as it relates to cyber warfare, including the problem with attribution and the standard of attribution required in order to pursue the alleged attacker lawfully.[123] Attribution and issues associated with attribution will be discussed in greater detail later in this chapter.

Use of Force

UN article 2(4) has an additional aspect that is contested in the international law community as it applies to cyber warfare and conflict. That is the concept of use of force in that domain. Many argue that the act of cyber attack does not constitute a use of force in the traditional sense, as the intent of the term *force* is to describe an armed force. A counter argument to this point is that if the objective were to cover specific acts of armed forces, that language would have been used to include the word *armed* rather than the general term: use of force.[124] There are other experts who have opposing views and believe the intent of use of force was to be all-encompassing and defined under general terms. Green states that"[t]he prohibition of the use of force was always meant to be comprehensive in nature, in the sense that any and all uses of force fall under its purview."[125]

Another approach used to consider if a cyber attack should be regarded as an act of use of force is proposed to consider the target of the cyber attack. This approach

---

[123] Kubo Macak, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors," Journal of conflict & security law 21, no. 3 (2016): 407-08.

[124] Green, Cyber Warfare: A Multidisciplinary Analysis, 100.

[125] Ibid., 99.

argues that a cyber attack could exceed the use of force threshold if the target of a cyber attack is considered part of national critical infrastructure (NCI).[126] Under this method, any cyber attack against NCI, regardless of the severity, would be considered a use of force. This generated concerns as some argue this approach is too inclusive "it would also qualify as a use of force those cyber operations that only cause inconvenience or merely aim to collect information as long as they target a NCI."[127]

The Stuxnet attack is believed to be a cyber attack that could fit the use of force criteria due to the damage that is believed to have occurred on the centrifuges.[128] Up until the Stuxnet attack, physical damage resulting from a cyber attack had occurred less than a handful of times.[129] While Use of Force is a significant issue requiring concessions across the international community, attribution may be the most significant challenge present in cyber warfare.

Attribution

This section will examine the significance of attribution in the cyber domain and the complications analysis encounter when attempting to solve the attribution problem. Significant hurdles include the anonymity and complexity of the Internet, which is used in favour of the cyber attacker or hacker. This section will also explore some tools hackers could use to conceal their identity, as well as the tools analysts can use to counter the concealment and attribute the cyber attacks. The section will conclude with a discussion of the importance of attribution, the significant impact of misattribution on the accuser and accused, and the proportionally increased importance of attribution as the

[126] Focarelli, "Self-Defence in Cyberspace," 236.
[127] Ibid.
[128] Haataja, "Stuxnet," 136.
[129] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 373.

intended consequences of a cyber attack increase. Although a considerable amount of discussion and analysis regarding attribution has occurred, much work remains to ensure consensus is reached. Debates within the community regarding how much control is required to appropriately attribute a cyber attack to an organization or State.[130] Until this concurrence is reached, the already difficult task of attribution remains increasingly challenging.

James P. Farwell and Rafal Rohozinski argue that under the Law of Armed Conflict section and Article 51 of UN Charter set the conditions that attribution must be established prior to conducting a counter attack. If attribution is not correctly realized and a cyber attack is launched on an organization or state perceived to have caused the initial attack, it may, in fact, reduce the credibility of the defender as they have now themselves become an attacker. The cyber attack that may have once been described as cyber defence becomes an act of aggression as attribution was not adequately established. The counter attack was unintentionally directed at an innocent organization or state.[131]

Attribution in the cyber domain faces many challenges, including the anonymity of the internet and lack of regulation regarding identification, as opposed to telecommunications companies, that require users to register prior to accessing the telephone network. These challenges increase in severity when the attribution of State actions is being examined. “State attribution has been even more challenging […] because of the serious political and legal consequences that attribution or misattribution may trigger.”[132]

---

[130] Green, Cyber Warfare: A Multidisciplinary Analysis, 113.
[131] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 35.
[132] Tsagourias and Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges," 944.

Attribution is difficult because attackers mask their true identity by routing the attacks through various locations that can make it look like an attack came from somewhere else.[133] In the early days of the Internet, the Tor project was created by the US Government to provide an anonymous way of collecting intelligence.[134] While the system is now well known for being compromised by the government itself and therefore not offering much privacy to civilians, state sponsored attackers will often replicate the principles behind the Tor network via paid online hosted traffic relay services or through hacked hosts acting as bots and relaying traffic unknowingly.[135] These attackers can quickly establish a new means of transmission for their attack before dismantling it to hide their tracks through these methods.[136] Therefore, unless a government has the ability to capture and store a significant amount of traffic across the internet to determine where a malicious packet has travelled through and originated from, it becomes very difficult to determine the true origin of an attack,[137] especially when using hacked hosts as relays.[138]

The challenge with attribution is related to the complexities of the telecommunication infrastructure and technologies. It is not uncommon that an IP address is known and the physical location of the attacker is not. In an interview with the chief scientist at the Computer Science and Telecommunications Board part of the US National Research Council, Herbert Lin contextualized this attribution problem with an illustration

---

[133] Robert Koch, Mario Golling, and Gabi Dreo Rodosek, "How Anonymous Is the Tor Network? A Long-Term Black-Box Investigation," Computer (Long Beach, Calif.) 49, no. 3 (2016): 43.

[134] S. Benmeziane, N. Badache, and S. Bensimessaoud, "Tor Network Limits" (2011).

[135] Scott J. Shackelford and Richard B. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," Georgetown journal of international law 42, no. 4 (2011): 981-82.

[136] Benmeziane, Badache, and Bensimessaoud, "Tor Network Limits," 1.

[137] Shackelford and Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," 983.

[138] "Tor (Anynoymity Network)," https://en.wikipedia.org/wiki/Tor_(anonymity_network).

of the challenges this information gap may present: “Assume a computer controls an adversary’s air defence network and you cannot physically locate it. If you go after it with a cyber attack, what if it’s located in a neutral nation? Or your own territory?”[139] The example Herbert Lin presented demonstrates the problem with engaging a cyber target without appropriate attribution. It shows the possibility of a country unknowingly engaging in a war with a nation they otherwise would not have or with their own citizens. “Cyber war complicates matters and challenges traditional notions of neutrality and sovereignty.”[140]

Attribution is made more difficult due to the broad access to the cyber domain.[141] “Third parties currently working in concert with a state may or may not be held under tight control. Criminal groups are mercenary. They may well sell their services twice.”[142] This poses not only a problem with attribution but also the ethics of warfare as the lines can quickly blur, from military action, to state and non-state actors, hactivist for hire, or someone who simply wants to prove they can do it. The challenges surrounding attribution are significant. To highlight how complicated this problem can be, the US White House cyber security advisor, Richard Clarke, openly confessed in 2002 that they still had not been able to attribute a cyber attack against America to a State actor.[143] Recently, the US indicted six Russians part of the Russian Main Intelligence Directorate (GRU) with computer attacks and intrusions with the view to strengthen Russia’s strategic objectives. The work towards exposing the GRU agents was not insignificant.

---

[139] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 31.
[140] Ibid.
[141] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 179.
[142] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 35.
[143] Macak, "Decoding Article 8 of the International Law Commission’s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors," 409.

The FBI had been working towards attributing the attacks to the GRU for more than two years. When the FBI agent in charge of one of the attribution teams, Michael A. Christman, was asked what contributed to the successful attribution, they stated: "[t]hese criminals underestimated the power of shared intelligence, resources and expertise through law enforcement, private sector and international partnerships."[144] The United States Department of Justice reports that "[t]he FBI's investigation was assisted by a parallel, independent Royal Canadian Mounted Police investigation."[145]

While hactivist for hire and state sponsored actors is a severe concern for many nations, theories exist that outline why state-sponsored actors may be less common than initially believed. One idea outlines that there are several factors that must be considered when evaluating the likelihood of a state-sponsored cyber attack. The criteria include three elements "(1) the alignment between state and the hacker goals, (2) the degree of support needed relative to the difficulty of achieving a given operational aim, and (3) the value of a state's objectives relative to the expected consequence."[146] These criteria display the values of the hacker must be in line with the state and the desired effects. This avenue may not be the one stop shop it was once believed to be. Therefore cyber incidents that appear to be politically motivated and traced back to what looks while non-state hackers are most likely committed by that state's internal resources regardless of

---

[144] The United States Department of Justice (DoJ), "Six Russian Gru Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[145] "U.S. Charges Russian Gru Officers with International Hacking and Related Influence and Disinformation Operations," https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

[146] Justin Key Canfil, "Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity," Journal of international affairs (New York) 70, no. 1 (2016): 222.

their denials. The reach of the internet through the cyber domain "partially levels the playing field between states and individuals in the cyber domain, means the threat of patriotic (or otherwise non-state) CNA will no doubt increase should no developments intercede to alter our current trajectory."[147] Nations still must be concerned about non-state actors, but they may be acting on their own accord rather than acting as a proxy for other countries.

The process to attribute a cyber attack is a significant undertaking that could take years to complete.[148] "Technical means of identifying attackers are necessary but largely insufficient due to the ability to spoof, delete, obfuscate, or call into question the interpretation or legitimacy of evidence used to assert a claim of attribution."[149] There are several ways to increase the successful attribution, including adjusting internet protocols that would decrease the success of spoofing and "traffic that is difficult to attribute could be filtered by routers."[150] However, privacy concerns have been raised in the past when these solutions were considered to increase the likelihood of attribution.

The inability to definitively attribute actions in the cyber domain can diminish the relevancy and effectiveness of proportionally in Just War Theory.[151] Without attribution, it is difficult to appropriately determine the correct target of a counter attack, let alone the proportional response. This lack of accurate attribution could lead to an escalation of the conflict. The escalation in conflict could take the form of increased political tensions, sanctions, kinetic or non-kinetic actions. "In some circumstances mistaken attribution can

---

[147] Ibid., 224.
[148] Henrik Karlzén, "Usefulness of Cyber Attribution Indicators" (Reading, 2020), 173.
[149] Elliott, "Active Cyber Defense and Attribution in Cyber Attacks," 1.
[150] Karlzén, "Usefulness of Cyber Attribution Indicators," 173.
[151] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 180.

lead to an unlawful response even if the victimized State made a reasonable determination of attribution and implemented countermeasures."[152] More on Just War Theory will be discussed later in this Chapter.

Key indicators believed to be useful towards attribution include tradecraft, infrastructure, malware, intent and external sources. Tradecraft refers to patterns and habits that can be observed over time by cyber attackers. "This is arguably the most important indicator category, because human habits are more difficult to change than technical tools."[153] The infrastructure used to create and execute a cyber attack and provide clues to the analyst as to the attribution of the cyber attack. Factors such as IP addresses and domain names can contribute to the aggregate knowledge of attribution. The code itself can also provide critical information for the analysis. While the malware can be analyzed, this should be done cautiously as the malware can be later modified by another actor or organization. Finally, intent and external sources refer to the influence factors such as geopolitics may have on the cyber attackers. These factors can provide clues to the analyst as to the attribution of the cyber attack.[154]

One theory states the attribution criteria can be broken down into three elements: instructions, direction, and control.[155] The theory argues that while the three terms are used interchangeably in everyday English language. "For example, the respected Oxford Dictionary uses 'instruction' to define 'direction' and 'directing' to define 'control'."[156] However, when examining Article 8 under the International Law Commission from

---

[152] William Banks, "State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0," Texas law review 95, no. 7 (2017): 10.

[153] Tsagourias and Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges," 947.

[154] Ibid., 946-50.

[155] Macak, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors," 414-25.

[156] Ibid., 411.

United Nations General Assembly 56/83, they have distinct meanings as applied to attribution.

To be attributable, the actions by non-state actors must be instructed, directed and controlled by a State. Where the challenge lies is that for each of these criteria, the level to which the state is engaged has to be met. "However, a general ′rallying call by the State encouraging like minded but unspecified ′patriotic hackers to engage in offensive action would not suffice for the purposes of attribution."[157] The fact that the state supports a non-states actor's position or platform does not mean that their actions are attributable to the state.[158] This link to instructions delivered by the State and, by extension, the cyber attack attributed to the Sate could connect the actions to Article 2(4) and satisfy the first requirements: the activities must be attributed to the State.[159]

In summary, in the case of proxy actors or state hired cyber attackers, the theory explains that it creates a subordinate relationship between the state and non-state actors due to instructions being delivered by the state. The instructions being given to the non-state actors keeps the responsibility of the cyber attack and results with the state. The challenge then becomes less about debating if the state should be held responsible for the attack, but rather can the attribution of the attack be proven to the state. "While shared goals may indicate political alignment and may thus suffice for the purposes of political attribution, the same can not be said for the establishment of legal liability."[160]

---

[157] Ibid., 415.
[158] Ibid., 421-22.
[159] Elliott, "Active Cyber Defense and Attribution in Cyber Attacks," 234.
[160] Macak, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors," 415.

Additionally, as the intended consequences of the planned counter-cyber attack increase in severity, so does the importance of attribution and the requirement for increased accuracy.[161] Conversely, the same can be said when considering the severity of the outcomes experienced by the victim as a result of the attack. The level of effort to be put towards solving the attribution problem is observed to be relative to the scale of the offence. The more grand the act is, the more effort will be exerted to attribute the cyber attack.[162]

Attribution is not only a seemingly insurmountable technical challenge, but it is made increasingly difficult due to the lack of consensus across the international community as to what standard of attribution is acceptable. Many theories such as those highlighted above attempt to guide the conversation towards concurrence and acceptance of desperately needed attribution standard. The need for an internally accepted standard of attribution will only increase as technology evolves and the political risk of misattribution increases. Attribution is an important factor in cyber warfare, especially when decision-makers are evaluating options regarding countermeasures. Just War Theory can be equally important when considering the ethics of courses of actions and developing the plan.

Just War Theory

Just War Theory is considered by some as the pinnacle of ethical guidance for waging a justified conflict. It is viewed as the framework of ethical doctrine to base decisions in conflict. “In general, just war theories attempt to conceive of how the use of

[161] Elliott, "Active Cyber Defense and Attribution in Cyber Attacks," 15.
[162] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 401.

arms might be restrained, made more humane, and ultimately directed towards the time of establishing lasting peace and justice."[163] While it has been taken from a traditional theory that is now common knowledge, many experts believe the Just War Theory holds true in modern times. It is still a vital tool to measure military actions against.[164]

Just War Theory can be divided into three categories. The first, jus ad bellem, outlines criteria for war, the transition from peace to war. The second, jus in bello, theorizes justifiable use of force during a conflict. The last, most recent category, just post bellem, defines the transition from war to peace and the termination of war.[165]

There are many variations of the subcategories held within the three main categories of Just War Theory. Generally speaking, the subcategories can be listed as follows: Within Jus ad bellum: just cause, right authority to wage war, last resort, net benefit, and the right motivation. Within Jus in bello: protection of non-combatants, proportionality, discrimination, more good than harm. The third and final category had the most variation amongst theorists and scholars. The most commonly summarized subcategories of Jus post bellum are as follows: the establishment of peace, take responsibility for a share of actions, participate in forgiveness.[166]

There are three schools of thought as to the applicability of Just War Theory as it relates to the cyber domain. The first is that although Just War Theory was developed long before cyber warfare conflicts existed, the theory still applies to the conflict in the cyber domain. The second group believes Just War Theory provides the framework under

---

[163] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 178.
[164] Tamar Meisels, Contemporary Just War Theory and Practice, 1 ed., vol. 1 (Abingdon, Oxon;New York, NY;: Routledge, 2017), 151.
[165] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 178.
[166] Mark Evans, Just War Theory: A Reappraisal (New York: Palgrave Macmillan, 2005), 12-13.

which another set of guidance can be built to provide a robust policy to guide conflict in the cyber domain. The last group believes the cyber domain is new, and unlike any other domain where war is waged. Therefore, this new domain requires new theories under which morals must be measured against.[167] The argument commonly made is that Just War Theory was conceived prior to the development of digital technology, so it would not have been considered when Just War Theory was created. Some have argued that "the advent of cyber weapons surely represents a revolutionary development in our security environment and hence we should not expect ethical frameworks such as Just War Theory, developed in and for a pre-digital world, to apply in this new context."[168] It is the belief under this group that the current set of regulations are insufficient to regulate operations in the cyber domain, and an opportunity exists to establish the treaties required proactively.[169]

A counter point to the relevancy of Just War Theory as it applies to the cyber domain: it may not be applicable because Just War Theory was not created to include non-physical, non-human and non-violent actions.[170] These attributes are characteristic of operations conducted within cyber warfare. Generally, the overall results of cyber attacks are non-physical, against equipment, not humans, and the impact of cyber attacks is, for the most part, considered non-violent. Considering Just War Theory has withstood the test of time, this should point to the need to enhance it to be applicable to characteristics

---

[167] Matt Sleat, "Just Cyber War?: Casus Belli, Information Ethics, and the Human Perspective," Review of international studies 44, no. 2 (2018): 325.

[168] Ibid.

[169] Neil Rowe Patrick Lin, and Fritz Allhoff, "Is It Possible to Wage a Just Cyberwar?," The Atlantic, 5 June 2012 2012.

[170] Sleat, "Just Cyber War?: Casus Belli, Information Ethics, and the Human Perspective," 328.

that are unique to the cyber domain, instead of finding arguments why it should be discarded.

The following section will discuss Just War Theory as it applies to conflict in the cyber domain. It will explore whether Just War Theory is applicable to conflicts in the cyber domain or if the absence of international law within the cyber domain is insurmountable. The following five elements of Just War Theory will be examined: just cause, last resort, and proportionality.[171] Additionally, the protection of non-combatants and will be examined concluding with prevention.

Just cause. UN Charter Article 51, states that all nations have a right to self defence. So, in theory, and at first glance, performing countermeasures in the cyber domain could be considered self-defence, therefore just cause. However, there are other factors such as use of force and attribution that complicate the initial straightforward claim to self defence. When the use of force is considered, the analysis of just cause becomes more difficult. As the impact of many cyber attacks is temporary and does not cause physical damage, the attacks do not cross the use of force threshold. Although, if we were to consider the term use of force as an all-encompassing term, then a case could be made that a cyber attack represents a use of force, and counter measures could fall under the category of just cause. “The prohibition of the use of force was always meant to be comprehensive in nature, in the sense that any and all uses of force fall under its purview.”[172]

An additional hurdle that must be overcome in order to make a claim of self defence is attribution. Attribution must be determined to understand who carried out the

[171] Eliav Lieblich, "Internal Jus Ad Bellum," The Hastings law journal 67, no. 3 (2016): 697.
[172] Green, Cyber Warfare: A Multidisciplinary Analysis, 99.

initial attack in order to launch justifiable offensive countermeasures. A case for just cause can be made to conduct countermeasures in the cyber domain under claims of self defence as long as use of force is demonstrated in the first attack and attribution is determined.

Last resort. It can be argued that the Stuxnet cyber attack was an act of last resort. For years the UN had imposed sanctions against Iran due to growing concerns surrounding its nuclear program. Failed diplomatic discussion and inspections conducted by the IAEA yielded inconclusive results. The US had imposed sanction on Iran over concerns of its nuclear program since 1984.[173] After years of diplomatic dialogue, inspections and sanctions, concerns grew and culminated in considerations of an Israeli airstrike against Iran. Taking action in the cyber domain can be considered an act of last resort. Sanctions, inspections, regulations and diplomatic discussions did not quell international concerns surrounding Iran's nuclear program. In 2006, Israel collaborated with the Americans to establish Operation Olympic Games with the aim to conduct a cyber attack against the Iranian Nuclear facility rather than conducting an airstrike. Considering the alternate course of action was the possibility of an airstrike, Stuxnet was not only the last resort but also preserved the protection of non-combatants, was proportional to the threat and prevented the use and further development of perceived nuclear weapons program.[174]

Proportionality. There are concerns that a conflict in the cyber domain could escalate into a gruesome battle in the form of conventional kinetic effects.[175] Rule 23 -

---

[173] Masterson, "Timeline of Nuclear Diplomacy with Iran".

[174] Kim Zetter, Inc OverDrive, and ebook OverDrive, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, 1st ed. (New York: Crown Publishers, 2014), 36-86.

[175] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 180.

Proportionality of Countermeasures of the Tallinn Manual 2.0 states that according to UN Article 51, countermeasures are appropriate as long as they are proportionate. It is the State's responsibility to ensure all counter measures set in place for self defence are proportionate.[176] A response or countermeasure is considered proportionate if the force is being "applied in a manner that avoids excessive use."[177] The debate as to whether a cyber attack can constitute a use of force is a contentious issue. Currently, there is no consensus that cyber attacks do not cross the use of force threshold, as the end result of a cyber attack does not usually cause permanent physical damage to equipment or infrastructure. Therefore, it would be difficult to justify a countermeasure to an attack in the cyber domain. A proportional cyber countermeasure may almost be limited to a cyber response to a kinetic attack.[178]

Protection of non-combatants. The protection of non-combatants is a crucial factor when considering if a war is just. The fact that much of the information technology infrastructure could be categorized as dual use means the protection of non-combatants must be at the forefront of cyber planners thoughts. Disregarding this could mean that a cyber attack on infrastructure could be seen as an attack against non-combatants. Depending on the infrastructure that was targeted during the cyber conflict, the attack could impact NCI which could be considered a use of force.

Prevention. Like in any type of conflict, when considering taking any action, it should always be with the intent to prevent further escalation, prevent the start of a much

---

[176] Michael N. Schmitt and Nato Cooperative Cyber Defence Centre of Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, ed. Michael N. Schmitt and Liis Vihul, 2nd ed. (Cambridge;New York, NY;: Cambridge University Press, 2017), 127.

[177] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 178.

[178] Banks and Criddle, "Customary Constraints on the Use of Force: Article 51 with an American Accent," 88-89.

more dangerous situation, pre-emptive self defence, or put an end to the conflict by overwhelming the enemy. With this in mind, the cyber domain offers many valuable assets which can be used for those purposes. As in the example of Stuxnet, cyber may be used to prevent the proliferation of nuclear weapons or weapons of mass destruction, even if the effects were only temporary.[179] It could be argued that Stuxnet demonstrated how carefully constructed and executed cyber attacks may have prevented kinetic attacks that could have caused serious injury to many people.

Schmitt Analysis Criteria

Some scholars and experts have attempted to reframe some of the existing laws and articles through the creation of criteria and frameworks in order to effectively apply rules that were put in place before the conception or establishment of the cyber domain and cyber warfare. One of those experts is Michael N. Schmitt, who created the Schmitt Analysis Criteria in 1999. Schmitt's framework has generally been believed to have stood the test of time since and considered "the most refined theory to date for addressing the legality of cyber attacks under jus ad bellum."[180]

The Schmitt criteria were created as a framework to be used to determine the likelihood of a State to determine if cyber actions are to be categorized as a use of force. Schmitt created the criteria because he recognized "traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by Computer Network Attack, the Article proposes an alternative normative framework

[179] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 180.
[180] Green, Cyber Warfare: A Multidisciplinary Analysis, 107.

based on scrutiny of the consequences caused by such operations."[181] The Tallinn Manual 2.0 agrees with Michael Schmitt's assessment, as they refer to the criteria in "Rule 69 - Definition of the use of force."[182] The Schmitt criteria are broken down into six elements: Severity, Immediacy, Directness, Invasiveness, Measurability, and Presumptive Legitimacy.[183] Severity is the degree to which destruction or injury is expected. Immediacy describes the materialization of action, the more quickly the attack culminates the less chances are for peaceful resolution. Directness refers to the harm caused and whether the action taken is the only contributing factor to the results. If the harm is only attributable to cyber action it is more likely to be considered a use of force. Invasiveness considers the origin of the attack and if it was initiated outside of the borders of the targeted state. Measurability refers to the damage caused by the attack. If the effects can be quickly quantified, the odds of it being considered a use of force increases. Presumptive Legitimacy criteria evaluates if the actions were legitimate and undertaken by a state actor.[184] Severity is considered to be the most significant among the Schmitt criteria.[185]

Tallinn Manual

The Tallinn Manual has developed eight criteria to be used when determining if the prohibition of Article 2(4) was broken. Six of the eight criteria were proposed by

---

[181] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," The Columbia journal of transnational law 37, no. 3 (1999): 885.

[182] Schmitt and Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 333.

[183] Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 914.

[184] Ibid., 914-15.

[185] R. Ottis C. Czosseck, K. Ziolkowski, "Ius Ad Bellum in Cyberspace – Some Thoughts on the "Schmitt- Criteria" for Use of Force," International Conference on Cyber Conflict 4th (2012): 301.

Michael Schmitt.[186] The original manual was published in 2013 which contained 95 rules that were designed by committee. The committee considered these rules relevant to cyber warfare and in line with international laws. The committee "provided commentary that included noting any disagreements among the committee members as to the application or interpretation of these 95 laws."[187] The comments were included as the aim of the manual was to advise and provide planners and decision-makers with options to consider. The Tallinn manual was not intended to be a definitive guide. The first version of the Tallinn manual, Tallinn Manual 1.0, was centred around cyber war. Tallinn manual 2.0 was released three years later and expanded to "focus on activities below the level of war, which include cyber terror, cyber espionage, and cyber crime."[188]

The Tallinn Manual attempts to bring the international community together and reach common ground towards the impact of a cyber attack. It attempts to quell the debate as to if a cyber attack could constitute a use of force and takes a different approach. A cyber attack may not surpass the threshold of use of force, however it could constitute "a violation of the principle of non-intervention in the international affairs of another State."[189] As explained in Tallinn Manual 2.0 Rule 68 - Prohibition of threat or use of force and UN Article 2(4), "All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity

[186] L. J. M. Boer, "'Restating the Law "as It Is"': On the Tallinn Manual and the Use of Force in Cyberspace," Amsterdam law forum 5, no. 3 (2013): 11.

[187] Paul J. Springer, Ebscohost, and Ebsco ebook, Encyclopedia of Cyber Warfare (Santa Barbara, Calif: ABC-CLIO, 2017), 287.

[188] Ibid., 288.

[189] Focarelli, "Self-Defence in Cyberspace," 250.

or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[190]

Experts are divided when examining the 2007 cyber attacks against Estonia next to the criteria described in the Tallinn Manual. Michael Schmitt argues that the events could be viewed as a use of force when measured against the criteria set out in the Tallinn Manual. However, "these criteria only suggest the probable direction in which the law will develop in the future; the position in existing law remains intact."[191] – Meaning, due to the laws currently in place, while it should be considered a use of force act when measured against the Tallinn Manual criteria, it is not. Additionally, experts argue that while the cyber attacks were disruptive, they would not exceed the use of force threshold because there was no permanent damage after the DDoS attacks stopped. After careful evaluation of the laws and frameworks in place, Michael Schmitt believes "the cyber attacks constituted a violation of Estonia's sovereignty and breached the non-intervention principle."[192]

Other Nations' Cyber Posture

Now that a summary of ethical and legal tools relating to the cyber domain has been reviewed, this chapter will now conclude with an examination of what is commonly considered the two adversarial cyber powers to the west, Russia and China.

Both the Estonia and Georgia cyber attacks have demonstrated that Russia's "cyber methodology was relatively crude, in that it involved a brute-force DDoS

---

[190] Schmitt and Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 329.

[191] Haataja, Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics, 120.

[192] Ibid.

approach that required enormous botnets to continually evolve and continue their attacks."[193] While the approach may have been crude and temporary, they were practical. They displayed the Russian government's willingness to operate in the cyber domain and "use cyber attacks as a major force enabler to complement physical violence."[194] The 2014 Crimea annexation can also note similarities in Russian cyber methodology. Russia used a similar approach as with the conflict in Estonia and Georgia. It relied upon DDoS attacks to disrupt the flow of information through overwhelming social media with misinformation, government websites and servers shut down due to DDoS and the disruption of media transmitters.

Russian doctrine only uses the phrase *cyber warfare* when discussing foreign activities. Russian documents describe the cyber domain as "separating out computer network operations from other activities is the division between the information-technological and information-psychological domains."[195] These two categories that Russia divides information warfare into is a significant shift from western countries' cyber doctrine approach to technical solutions to technical threats. This doctrinal position can explain their focus on misinformation and the effectiveness of these campaigns."The country claims that information warfare is the basis of all cyber campaigns. Obtaining information through the use of cyber proxies allows Russia to deter and disorient adversaries."[196] The use of proxies allows Russia to remain anonymous while achieving its desired effect. The misinformation jeopardizes and sabotages the national security of

---

[193] Springer, Ebscohost, and ebook, Encyclopedia of Cyber Warfare, 257.

[194] Ibid.

[195] Valeriy Akimenko and Keir Giles, "Russia's Cyber and Information Warfare," Asia policy 15, no. 2 (2020): 68.

[196] Jennifer Pomeroy et al., "Russia's Search for Stability: Cyber Capabilities and Military Buildup," Current politics and economics of Russia, Eastern and Central Europe 33, no. 1/2 (2018): 103.

Russia's adversaries. Jeremy Fleming from Britain's intelligence services would agree with this sentiment as he told the Telegraph, "The Russian Government is widely using its cyber capability. They′re not playing to the same rules… they're blurring the boundaries between criminal and state activity."[197] Another recent focus of the Russian cyber methodology has been the tampering of election results, as demonstrated during the 2016 hacking of the US Democratic National Convention. "Direct political obstruction has of late become a major asset of Russian cyber interference and poses a threat to democratic societies."[198]

Mainstream media consistently portrays China as a hacker state. This section will examine what are the realities of China's cyber capabilities. "China's military strategists describe cyber capabilities as a powerful *asymmetric* opportunity in a *deterrence* strategy."[199] Computer network operations, specifically computer network attack, is considered an essential deterrent by Chinese analysts due to the increased costs incurred by the enemy when engaged in warfare. "This could, for example, leave China with the potential ability to deter the United States from intervening in a scenario concerning Taiwan."[200] In the 2020 Military and Security Developments Involving the Peoples Republic of China (PRC) Annual Report to Congress, it states that the People's Liberation Army (PLA) believes that cyber operations are a low-cost method to manage escalating conflict.

---

[197] "Uk Can Degrade Russia's Cyber Capabilities in the Same It Dismantled Isil's, Gchq Director Says," Telegraph.co.uk 2018.

[198] Pomeroy et al., "Russia's Search for Stability: Cyber Capabilities and Military Buildup," 104.

[199] Hjortdal Magnus, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," Journal of strategic security 4, no. 2 (2011): 5.

[200] Ibid., 6.

Furthermore, the PLA believes attaining cyber superiority is a significant objective that must be realized in order to "deter or degrade an adversary's ability to conduct military operations against China."[201] The PLA targets both military and civilian cyber objects. Cyberspace is increasingly a decisive tool for China for three reasons "deterrence through infiltration of critical infrastructure; military technological espionage to gain military knowledge; and industrial espionage to gain economic advantage."[202] In the annual report to congress, analysts have determined that there are significant PRC intrusions worldwide. The report focused on what this could mean for the US and, more specifically, the DoD:

> "These and past intrusions focus on accessing networks and extracting information. China uses its cyber capabilities to not only support intelligence collection against U.S. diplomatic, economic, academic, and defense industrial base sectors, but also to exfiltrate sensitive information from the defense industrial base to gain military advantage. The targeted information could enable PLA cyber forces to build an operational picture of the U.S. defense networks, military disposition, logistics, and related military capabilities that could be exploited prior to or during a crisis"[203]

This exploitation can assist China in their diplomatic negotiations to complete their powerful and sought-after One Belt One Road (OBOR) initiative. Additionally, this information gathered could help the PLA exploit adversarial computer networks and other military and industrial capabilities. Due to the PRC's extensive industrial and military cyber espionage capabilities, they are considered the most significant cyber threat to the US and those they are aligned with. As mentioned previously, China views

---

[201] Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," (2020), 74.

[202] Magnus, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 1.

[203] Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," 84.

cyber attacks as a valuable deterrent from external involvement. Concerning China's strategy, they have a "doctrine of first strike, but suffers from a degree of chaos in its cyber security efforts. On this evidence, it would seem that a war fighting approach would serve the interests of the US well."[204] Bearing in mind the PRC's controlled information flow, even to the extent that their cyber security law requires all information technology to originate from China and further restricts the sale of foreign technologies to be implemented in the country, including data storage.[205] Considering the contrast between the western and eastern values of information flow, it would behoove western nations to evaluate their information flow with a view of protection against cyber espionage.

While Russia and China can be considered great cyber adversaries, they both have dramatically different approaches and goals. Russia aims to spread misinformation through the cyber domain, and China aims to gather as much information as possible to further their economic, industrial or military power.

[204] David J. Lonsdale, "Warfighting for Cyber Deterrence: A Strategic and Moral Imperative," Philosophy & technology 31, no. 3 (2017): 420.

[205] Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," 16.

CHAPTER 4 — CYBER OPERATIONS

The previous sections provided the background required to examine if Canada should participate in offensive cyber operations. The case studies highlighted in the earlier chapters demonstrate how offensive cyber operations can be a powerful strategic tool. The cyber domain can be considered the "wild west" since international law has yet to provide clear guidance on the legality of cyber attacks and where exactly is the use of force threshold. Despite the untamed nature of the cyber domain, stakeholders can not underestimate its value. Cyber operations can be a strategic political tool complete with deniability should that be the desire.Operating ethically in the cyber domain is very important should Canada want to continue to hold its international reputation as a contributing ally to alliances such as NATO and NORAD.

This section will examine the differences between passive cyber defence and active cyber defence, which were the only forms of cyber operations Canada was permitted to conduct until 2019. Next will be a review of the current Canadian cyber policies. The final section will examine the impacts of Canada performing offensive cyber operations and conclude with the recommendation to either continue to develop offensive cyber operations or cease the capability building and revert to a posture of exclusively passive and active cyber defence.

Cyber Defence

Cyber defence can be broken down into two categories, passive cyber defence and active cyber defence. The definition of *defensive* cyber operations according to Department of Defense (DoD) Joint Publication 1-02 is "Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and

protect data, networks, net-centric capabilities, and other designated systems."[206] Passive cyber defence uses tools such as anti-virus software, firewalls and user education, intending to increase the cyber security education and practice of all who use the networks.[207] The goal of passive cyber defence is to reduce the probability of becoming a victim of a cyber attack as well as minimizing the impact of a cyber attack if one were to occur. Passive defence can be defined under American doctrine as "measures taken to reduce the probability of, and to minimize the effects of damage caused by hostile action without the intention of taking the initiative."[208] Passive cyber defence aims to reduce the impact of a cyber attack and decrease the time required to restore the network should the attack be successful. [209]

Active cyber defence is defined as "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[210] In other words, active cyber defence encompasses cyber countermeasures and counter attacks directed at a hostile cyber actor. These counter attacks are a defensive response to a cyber attack executed by a hostile actor. Defensive cyber attacks can be further broken down into two subcategories: mitigation counterstrike and retributive counterstrike. Mitigation counterstrike is aimed at protecting the network and reducing the damage of a cyber attack."The purpose of a mitigative counterstrike must be to mitigate damage from an immediate threat."[211]By contrast, a retributive counterstrike is aimed at punishing the

[206] Defense, "Joint Publication 1-02," 63.
[207] Elliott, "Active Cyber Defense and Attribution in Cyber Attacks," 26.
[208] Defense, "Joint Publication 1-02," 181.
[209] Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework," 120.
[210] Defense, "Joint Publication 1-02," 1.
[211] Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework," 121.

cyber attacker. The retributive counter attack is a controversial element of cyber defence and not universally agreed upon as to what constitutes an active cyber defence. One theory states that retributive counterstrikes can be further broken down into four categories: observation, access, disruption, and destruction.[212] Colonel Eric F. Mejia from the United States Air Force (USAF) summarized that "[u]nder International law, only the mitigative counterstrike is truly defensive, because its purpose is to defend against an immediate threat."[213] This summary was derived from a Harvard Journal of Law and Technology article[214] where the authors made this determination based on the analysis of UN Article 51, US Common Law, the US Computer Fraud and Abuse Act (CFAA) and the US Electronic Communication Privacy Act (ECPA).

Canada's Current Cyber Policy

Bill C-59, the National Security Act, 2017, was introduced in 2017 and received royal assent two years later, 21 June 2019. The bill permits Canada to conduct offensive cyber operations.[215] However, Canada does not use the term *offensive* nor did they use that language in the bill. The term *active* cyber operations is used in its place.

The Communications Security Establishment (CSE) states it is permitted to conduct foreign defensive and active cyber operations. The authorities to conduct these cyber operations "provide the Government of Canada with important tools to help protect Canadians and Canada's interests."[216] CSE describes two categories of cyber activities are authorized to conduct, defensive cyber operations and active cyber operations.

---

[212] Elliott, "Active Cyber Defense and Attribution in Cyber Attacks," 5.

[213] Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework," 121.

[214] Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," Harvard Journal of Law & Technology 25, no. 2 (2021).

[215] *An Act Respecting National Security Matters, C-59.*

[216] Communications Security Establishment (CSE), "Foreign Cyber Operations," https://www.cse-cst.gc.ca/en/inside-interieur/cyberoperations-cyberoperations.

Defensive cyber operations as defined by CSE are comparable to active cyber defence as described above. CSE is authorized to defend the government of Canada's and Canadian commercial systems against foreign threats. This can be done by taking action proactively against foreign cyber actors prior to the attack reaching Canada's systems. The CSE explains the mandate: "Under a Defensive Cyber Operations Authorization, CSE could disable a foreign server used by cyber actors attempting to steal information about Canadians from a Government of Canada Network, or to disrupt elections infrastructure."[217]

Thanks to Bill C-59 being assented, CSE is now able to conduct Active cyber operations. More commonly referred to as offensive cyber operations. "Under an Active Cyber Operations Authorization, CSE could use its capabilities to disable communication devices used by a foreign terrorist network to communicate or plan attacks."[218] The authorization is not limited to disabling communication devices. CSE can also degrade, disrupt, influence or interfere with communication capabilities or activities related to international affairs, security or defence. CSE is authorized to target not only States but also foreign terrorist organizations. It is important to note that in accordance with Rule 66 - Intervention by states of the Tallinn manual 2.0. "A State may not intervene, including by cyber means, in the internal or external affairs of another State."[219] Therefore, any of Canada's active cyber operations must not intervene in a State's internal affairs.

[217] Ibid.
[218] Ibid.
[219] Schmitt and Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 312.

Although CSE is authorized to conduct active cyber defence or active cyber operations, the proper approval mechanism must be realized before performing operations in the cyber domain.

> "The CSE Act sets out additional conditions for these Authorizations, including that activities must not cause death or bodily harm to an individual, or willfully attempt to obstruct, pervert or defeat the course of justice or democracy."[220]

Furthermore, CSE must seek approval from the Minister of National Defence before the execution of all defensive and active cyber operations. The Minister of Foreign Affairs must also grant authorization for active cyber operations and must be consulted during defensive cyber operations. It may be noticed that there was no mention of passive cyber defence, this area of cyber operations is under the responsibility of Shared Services Canada (SSC). Passive cyber defence is critical to all operations in the cyber domain. SSC has established a Critical Incident Response Team (CIRT) "to coordinate the identification, mitigation, recovery, and post-analysis of IT incident within the GC."[221] Passive cyber defence is critical to security and maintaining operations.

The Canadian National Cyber Security Strategy was first released in 2010. The strategy underwent revision in 2018. The strategy was aimed to be "designed as the mainstay of the Governments continuous efforts to enhance cyber security in Canada. The Government's actions will evolve alongside the ground-breaking technological developments and resulting paradigm shifts"[222]

Canada's National Cyber Security Strategy focuses on improving the state of cyber security for Canadians and industry. The Strategy recognizes the importance of

---

[220] (CSE), "Foreign Cyber Operations".
[221] Defence, "Joint Doctrine Note Cyber Operations," 1-5.
[222] Canada, "National Cyber Security Strategy," 5.

collaboration with industry to further initiatives in the cyber domain, in particular those innovations related to cyber security. The strategy also recognized the importance of collaborating with academic institutions to further develop cyber skills and enhance cyber security across Canada.[223] The importance of Canadians' trust in the cyber domain is acknowledged in the report recognizing that poor cyber security would likely result in the loss of faith in the Internet. A cyber domain where Canadians place little to no trust would have adverse secondary effects. "Cyber incidents can also be profoundly destabilizing. They can erode trust in e-commerce and government institutions and can lead people to question their continued use of digital technologies if they feel their safety or privacy is at risk."[224]

The strategy recognizes the importance of strong cyber defence not only across our governmental institutions but also throughout industry and across the Canadian population. As the digital age evolves and Canada's reliance on technology increases, the importance of cyber security will grow. "Some cyber systems — such as electricity grids, communications networks or financial institutions — are so important that any disruption could have serious consequences for public safety and national security."[225]

Although the importance of a cyber foreign policy was acknowledged in the implementing strategy of the National Cyber Security Strategy, "two years later, Canada still lacks a cyber foreign policy. This is unlike Canada's allies and adversaries, which

[223] Ibid., 11-29.
[224] Ibid., 14.
[225] Ibid., 18.

have released strategies outlining their interests and values in cyberspace — and how they plan to promote and defend them."[226]

When examining Article 51 and LOAC from the Canadian context, in particular the CAF, it has been determined that the term cyber attack is not an appropriate catch-all term for cyber actions across the domain. The CAF recognizes the debate as to whether a cyber attack constitutes an armed conflict as well as the legal and doctrinal issues that are associated with the lack of clarity and agreement across the international community. According to the CAF Joint Doctrine Note, a cyber attack is defined 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."[227] As an interim solution, the CAF has implemented a classification system aimed at resolving some of the confusion. These terms are also aligned with the definitions used within Public Safety Canada.

The classification system spans four levels, with the first being the least severe. The first level of the four groups is *Cyber security event*. It describes the actions that could be categorized as passive cyber defence. A cyber security event describes vulnerabilities that exist and may be exposed. These vulnerabilities are typically resolved once discovered, or a mitigation plan is put in place. The second level, *cyber security incident*, describes the compromise of information technology systems within the government of Canada. Depending on its nature, a cyber security incident could also be considered as part of passive cyber defence. The third level, *significant cyber incident*, is the first level where the incident transitions from a cyber security incident to a defence

[226] Christopher Parsons and Irene Poetranto Josh Gold, "Canada's Scattered and Uncoordinated Cyber Foreign Policy: A Call for Clarity," (New York: Just Security, 2020).
[227] Defence, "Joint Doctrine Note Cyber Operations," 3-2.

incident The final level, *cyber attack*, describes events that would fall under LOAC. "Cyber events or incidents that can impact or have the potential to impact military operations, therefore making them a defence matter."[228] These actions are considered a matter of national defence.[229]

Canadian Offensive Operations

Up until now, this paper has laid the foundation required to examine if Canada should be conducting active cyber operations. By reviewing significant cyber events in history, the impact of actions in the cyber domain can be powerful if properly executed. The effect of a DDoS attack can be severe when conducted on a population heavily reliant on services hosted in the cyber domain. The power of cyber operations overlaid with kinetic conventional military operations can be significant. The strategic power cyber operations can have on the international community, and the power malware can have when it is paired with accurate and through intelligence information should not be underestimated. The following examples demonstrate the strategic power of cyber operations and their impact on international relations.

With the assent of bill C-59 in 2019, Canada is late to implement active cyber operations to its legislature relative to the significant actors in the cyber domain. While there is a capability gap to overcome compared to our allies and opponents, who have been navigating the offensive cyber operation space for much longer than Canada has, bridging the capability gap is not insurmountable.

---

[228] Ibid., 3-9.
[229] Ibid., 3-1 - 3-9.

The CAF cyber capability, Cyber Task Force (Cyber TF), was established 1 September 2010.[230] The task force was established with a view to "strengthen the government's capability to detect, deter and defend against cyber attacks while deploying cyber technology to advance Canada's economic and national security interests."[231] The Cyber TF directive acknowledged that the establishment of cyber capabilities was uncharted territory for the CAF, recognizing the need to procure equipment and design the concepts and capabilities.[232] The directive called upon CAF leadership to assist with the establishment of the capability, with the view to present a decision brief to the Commander responsible for the management and establishment of Cyber TF Director General Information Management Operations (DGIMO) by 15 July 2011.[233] The Cyber TF directive was followed up with a Chief of the Defence Staff (CDS) initiative directive for defensive cyber operations, released 2 February 2015, where the Commander Canadian Joint Operations Command (CJOC) was tasked to optimize and operationalize defensive cyber operations.[234] The directive stressed the importance of cyber to military operations stating "[t]he increasing reliance of modern militaries on the Digital infrastructure increases the risk of compromise and potentially undermines DND/CAF's ability to meet its defence mandate."[235] The directive outlined seven DND/CAF strategic

---

[230] DGIMO, "Cyber Task Force (Cyber Tf) - Vcds Establishment Directive," ed. Department of National Defence (Ottawa2010).

[231] John Adams, "2016 Policy Review Series," in Canada and Cyber (Calgary AB: Canadian Global Affairs Institute, 2016), 2.

[232] DGIMO, "Cyber Task Force (Cyber Tf) - Vcds Establishment Directive," 3.

[233] Ibid., 5.

[234] Chief of the Defence Staff, "Cds Initiating Directive for Defensive Cyber Operations," ed. Department of National Defence (Ottawa2015), 2.

[235] Ibid., 5.

objectives, including: the ability to respond to cyber threats, ensure freedom of maneuver and establish a responsive capability.[236]

Shortly after the release of the CDS directive, the CAF cyber operator trade was created. According to the CAF recruiting website, the CAF cyber operator trade "conduct defensive cyber operations, and when required and where feasible, active cyber operations."[237]

Some have argued that a country's perceived cyber power and capabilities have a direct correlation to their influence on international relations [238] "What really matters to political leaders is the political consequence of a cyber attack, not the mere fact of a cyber attack."[239] The responsibilities of the CAF cyber operator can include: analyze network data, identify vulnerabilities and "conduct defensive and active cyber operations."[240]

There are many anecdotes of self-inflicted cyber attacks carried out through human error, selecting an insecure password or not taking the time to download the latest software update, to name a few simple cases. However, it is possible that human error can be a form of cyber defence. "In fact, the complexity heterogeneity, and interdependence between technical and human processes can provide a degree of resilience for the defence as attacks scale up."[241] To execute a complex cyber attack, the circumstances around the attack must be carefully researched and implemented flawlessly into malware code.

---

[236] Ibid., 9.

[237] Canadian Armed Forces, "Cyber Operator," Department of National Defence, https://forces.ca.en/en/career/cyber-operator/.

[238] Gamreklidze, "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia," 214.

[239] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 398.

[240] Forces, "Cyber Operator".

[241] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 402.

Humans make mistakes; these can lead to a procedural misstep that the malware is relying on to deliver the payload to the target. As the complexities of the cyber attack increase so do the dependencies of the human procedure and the risk that human error could be a form of cyber defence. In other words, a complex cyber attack also relies on the fact that the humans are acting in accordance with the procedures expected, without deviation. This highlights the fact that as the technical complexities of a cyber attack increase, so do the significance of other external elements, such as the human factor, as it relates to the intelligence gathered required to enable the cyber planners to create the malware.

It is natural to assume cyber deterrence would be useful in cyber operations because of the use of armed forces. Armed forces are created and used to conduct deterrence operations. "Massive retaliatory threat may be the only credible deterrent that a potential victim of cyber-conflict may have."[242] Based on this logic, it can be reasonable to assume an armed force capable of effective offensive cyber operations creates deterrence. It is still unclear if it is a reality because there is not enough data established through attribution.

The cyber strategy at the Pentagon reaffirms many topics already discussed in this paper. William J, Lynn III, US Deputy Secretary of Defense stated "Pentagon cyber strategy: (1) cyber warfare is asymmetric (2) the offence has the upper hand (3) deterrence models of assured retaliation do not apply to cyberspace where it is difficult and time consuming to identify an attack's perpetrator"[243] Attribution is difficult to ascertain, and offensive cyber operations are proactive and have the upper hand. As

[242] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 180.
[243] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 374.

opposed to the general deference previously mentioned, targeted deterrence is not a significant factor in the cyber domain as long as attribution is ambiguous.

Offensive cyber operations can be used to penetrate and disable an adversary before they execute their attack capabilities. In some cases, it is more effective to conduct offensive operations rather than defensive operations as adversaries could quickly disable and disarm defensive measures put in place. On the other hand, offensive action may not be wise because the attack may be targeted and affect the wrong enemy. In cyber operations, it is unknown that the attack will stop at the target, the collateral damage may be extensive.

The cyber domain can act as a valuable strategic and diplomatic tool, as illustrated in the Stuxnet worm and the NRC attack. As described earlier, the United States used the cyber domain as a compromise with Israel, which wanted to use air power to act on their concerns related to Iran's nuclear program. The United States was able to counter with a proposed cyber war rather than a kinetic airstrike.[244] This course of action was less costly,[245] safer for the troops, and afforded the United States and Israel the diplomatic cover of the difficulties of attribution.

Generally speaking, the consensus across the cyber community is that a defensive posture is reactive as the threats will quickly determine the defensive strategies and overcome them. "Offensive capabilities improve quickly while network defence improves slowly because technology takes time to develop and defenders lack incentives

[244] Ibid., 399.
[245] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 35.

to cooperate."[246] Estonia demonstrated the importance of cooperation to further goals in the cyber domain.

The aftermath of the 2007 cyber attack on Estonia resulted in several lessons learned for the nation. They recognized the issue to resolve cyber defence did not rest solely with the technical experts nor the lawmakers. Estonia recognized the need to harden their military defences in the cyber domain in order to deter attacks. They also recognized the importance of a legal framework to prevent cyber attacks and the importance of attribution and punishment when deterrence is not successful. "The revised penal code includes a number of sections dealing with cyber attacks and cyber crime."[247] Estonia's approach to deterrence, and punishment when deterrence is not successful highlights a theme throughout this paper, the importance of deterrence as it relates to cyber defence and collaboration.

The following are considerations that must be weighed against the argument that Canada should be conducting offensive cyber operations. Factors such as escalation, reputation, legality and normality must be considered when evaluating if Canada should take this course of action.

Deterrence operations through offensive cyber action could lead to an escalation of force. The conflict could grow rapidly out of proportion. Just because the adversary acted offensively, should a counter attack be launched? Will the attacks remain proportional? Tallinn manual 2.0 states, "States must act as reasonable States would in

[246] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 376.
[247] Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity," 71.

the same or similar circumstances when considering responses to them."[248] Fear of escalation, uncertainty and complexity of the cyber domain could deter political leaders from navigating in the cyber domain "uncertainty about collateral damage will affect decisions by political leaders, who may be unwilling to incur the risk of a cyber attack that could widen or escalate a conflict."[249]

Generally speaking, the sentiment across the Canadian population regarding our international reputation would be considered as *the nice guys*. Canada is known as a law abiding country and a peacekeeping country.[250] Would Canada's increase of offensive cyber capabilities damage Canada's reputation across the international community? Some would argue that Canada is delusional when thinking we have a reputation of do-gooders. Since the days of the Harper administration, Canada's reputation as do-gooders has fallen into disrepair through the government's "inept handling of international relations."[251] There are arguments made that Trudeau is starting to make gains to repair Canada's reputation; the real impact of the repair could be debated. "While addressing the UN General Assembly is certainly preferable to opting for a photo-op at Tim Horton's the earnest (if ineptly chosen) declaration that 'Canada is here to help' has yet to be convincingly demonstrated."[252] The Reid Institute conducted a survey of approximately 1500 Canadians regarding their perceived reputation of Canada. The results climbed from

---

[248] Schmitt and Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 81.

[249] Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," 179.

[250] Dave Korzinski, "Five Years after Trudeau Promised Canada Was 'Back' on the World Stage, Many Canadians Say We're in the Same Place," Angus Reid Institute, https://angusreid.org/canada-international-reputation-un-security-council/.

[251] Nicholas J. Cull and Michael K. Hawes, Canada's Public Diplomacy (Palgrave Macmillan, 2020), 36.

[252] Ibid., 45.

79% in September 2016 to 84% in July 2018, only to drop significantly to 71% in June 2020.[253] "The Trudeau government's record has at best been mixed, with the initial encouraging signs compromised by the hoisting of contradictory red flags and a painful lack of serious international policy reinvestment, not least in public or science diplomacy."[254]

As discussed in the previous chapter, the legality of offensive cyber operations is a great debate across the international stage. "International law currently is silent on whether a cyber attack can be considered an armed attack."[255] Canada has demonstrated due diligence in the cyber domain when it comes to the debate about the ethics and legality of active cyber operations. The implementation of the doctrinal level system across the government departments is used to determine the appropriate proportional response or countermeasure to a cyber event or attack. This tool can be used by cyber planners to ensure their plans are proportionate and in accordance with Article 51 and LOAC and can be valuable when navigating the contentious and contested issue.

If a significant number of countries adopt the position that offensive cyber operations are required, the normality of cyber warfare should be considered. Will offensive cyber operations become the societal norm where cyber attacks are expected, and defensive cyber or no action is a rarity? Is that the right mentality for society to adopt? The execution of warfare in the cyber domain by state actors can establish a precedent and normalizes cyber attacks. Barrack Obama recognized this when he was debating the implementation of operation Olympic Games. "Any American

---

[253] Korzinski, "Five Years after Trudeau Promised Canada Was 'Back' on the World Stage, Many Canadians Say We're in the Same Place".

[254] Cull and Hawes, Canada's Public Diplomacy, 46.

[255] Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework," 119.

acknowledgement that it was using cyber weapons - even under the most careful and limited circumstances - could enable other countries terrorists or hackers to justify their own attacks."[256] Cyber warfare can be a risky tool that can lead to political fallout. Barrack Obama also recognized this when considering moving forward with Stuxnet. "If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work."[257]

Additionally, another factor that must be considered when evaluating if Canada's offensive cyber operation posture is required is the fact that Canada is a member of several alliances, including NATO, five eyes, and NORAD. As observed during the evaluation of China's cyber capabilities, their clear demonstration of offensive cyber posture acted as a deterrent. While their approach, including espionage and targeting civilian nodes, may be considered ethical, it is believed by the PRC to have been a significant deterrent of other conflicts. "[O]ne of NATO's strengths is the interoperability of the different national forces, […] cyber vulnerability at the national level could mean that neither the NATO command authorities nor other nations could safely interoperate with a vulnerable entity."[258]

Ethical Offensive Cyber Operations

Through the evaluation of the Just War theory in the previous chapter, to the acknowledgement that as a member of an alliance, the chain is only as strong as its weakest link. The question is not whether *should* Canada conduct offensive cyber actions, but rather *can* Canada conduct cyber operations ethically?

---

[256] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 399.
[257] Ibid.
[258] ROBERT J. BUTLER FRANKLIN D. KRAMER and AND CATHERINE LOTRIONTE, "Cyber, Extended Deterrence, and Nato," (Washington D.C.: Atlantic Council, 2016), 4.

In a journal article discussing ethics and cyber security, the argument was made that an organization requires a clear statement of ethical principles and behaviours that can be adapted to conduct in the cyber domain. The article explains the adaptation of a generic code of conduct "can be utilized to create a specifically tailored code of conduct for any individual application. The code of conduct can then serve as a starting point for the direct implementation and assurance of ethical practice for cyber security."[259] Cyber actions in the government of Canada is a team sport comprising of CSE, RCMP and others. Evaluating this concept as it applies to the CAF can be the basis for a favourable argument. The CAF has a robust code of conduct, a justice system and a code of ethics. These elements combined with the Tallinn manual, LOAC and Just War form the basis of an ethical framework that can be developed specifically to meet the need of CAF offensive cyber operations.

As with most ethical conundrums, the morality of cyber warfare is not clear cut. "It offers the promise of non-violent, proportionate and discriminating threats and use of force. However, this promise may be undone by the unpredictability of cyber attack, new forms of harm, and the fact that it potentially lowers the threshold of conflict."[260] Ultimately the author David J. Lonsdale reached the following conclusion to the ethical debate of the use of offensive cyber warfare "A failure of deterrence is likely to lead to even greater levels of unpredictability and harm."[261] This illustrates the theory that ethically, possessing an offensive cyber capability may protect Canadian citizens from conflict more than if Canada did not have these capabilities.

---

[259] Dan Shoemaker, Anne Kohnke, and Greg Laidlaw, "Ethics and Cybersecurity Are Not Mutually Exclusive," EDPACS 60, no. 1 (2019): 9.

[260] Lonsdale, "Warfighting for Cyber Deterrence: A Strategic and Moral Imperative," 423.

[261] Ibid., 424.

It has been established that a code of conduct specific to cyber operations would be in place to guide cyber operators through their ethical dilemmas. It is also established that deterrence is required to reduce harm and unpredictability. But what is ethical cyber warfare? Are there tools that can be implemented to increase the ethical tendencies of Canadian cyber operators?

"According to the *Tallinn Manual*, damaging code and data on computers does not qualify as an attack in the law of armed conflict and is not subject to rules protecting civilian objects from attack."[262]As the Tallinn Manual is a guide that presents varying views that planners and decision-makers can use to evaluate the legality and ethics of cyber actions that are being considered, grey zones still do exist. These grey zones will continue to be a factor for planning cyber operations for the foreseeable future. The integration of a CAF cyber operator code of cyber ethics will reduce the ambiguities that exist within cyber operations and improve the ethics of Canada's cyber actions.

Throughout this paper, the use of force threshold was often described as a barrier when it came to just war theory. In an article written by the Atlantic Council in which NATO cyber capabilities were evaluated, an approach was presented that could resolve the threshold problem."Thresholds should operate on an adaptive basis. To cope with the proliferation of intrusions, thresholds should be somewhat ambiguous at lower levels of threat, with the ability to harden as risk develop."[263] While not directly related to thresholds of use of force, Canada has already demonstrated an acknowledgement of the usefulness of an adaptive threshold evaluation system through the CAFs incorporation of

[262] David P. Fidler, "Just & Unjust War, Use of Force & Coercion: An Ethical Inquiry with Cyber Illustrations," Daedalus (Cambridge, Mass.) 145, no. 4 (2016): 42.

[263] Lonsdale, "Warfighting for Cyber Deterrence: A Strategic and Moral Imperative," 426.

a levelling response system to a cyber action, as outline in the CAF Joint Doctrine Note. This system demonstrates that the CAF recognizes that actions in the cyber domain are not a one size fits all solution, and the actions and response actions must be carefully considered. Should the international community agree to adaptive thresholds based on the incorporation of the CAF cyber response system, it could be assumed the CAF would adopt this system. This would increase the tools available to CAF cyber operators to ensure ethical avenues are pursued when considering offensive cyber operations.

Some authors have argued that "cyber weapons do not create the stark ethical dilemmas that the militarization of other technologies has. Ever more destructive weaponry has strained ethical strictures in *jus in bello*, but cyber technologies do not follow this pattern."[264] Provided that the pattern holds true, with refined organizational-specific ethical frameworks to augment the Tallinn Manual, as well as adaptive thresholds, a case could be made that ethical offensive cyber operations are possible.

The decision to use offensive cyber operations is not one to be taken lightly. The Government of Canada would arguably agree with this statement as bill C-59, permitting offensive, or active, cyber operations, assented in 2019. This has resulted in a relativity nascent offensive cyber capability relative to our allies and adversaries. While being significantly behind our peers in the development of the capability is cause for concern, Canada is displaying the intent to operate ethically in the cyber domain. Until international law can reach a consensus as to how to approach actions in the cyber domain as it applies to LOAC, CAF has created a level system to rely upon. The level system is used as a guide to determine the escalation of cyber action. Although

[264] Fidler, "Just & Unjust War, Use of Force & Coercion: An Ethical Inquiry with Cyber Illustrations," 42.

escalation, normality and legality are all significant considerations to be applied to the development of courses of action when evaluating the option to execute offensive cyber actions, it does not negate the ethical consideration of offensive cyber action. Offensive cyber demonstrates relevance on the International stage, is more responsive than defence cyber actions, and can be an important political and strategic tool. Canada should continue to develop its offensive cyber capabilities.

CONCLUSION

Through the examination of six significant cyber events in history, a few important conclusions can be drawn. Collateral damage and intended consequences are a serious consideration when operating in the cyber domain. Mistakes in the programming code can have a significant impact. A legal and ethical framework is critical for operating the cyber domain. The safeguard of information is critical to preserving intellectual property and national interests.While there is still debate across the international community, the Tallinn Manual provides one framework for lawmakers and cyber planners to evaluate their actions and ensure they are ethical and legal. Cyber operations, when overlaid with conventional kinetic operations, can prove advantageous, especially when synchronized. The importance of intelligence and cyber planning can not be overstated. The closer these two functions work together, the more influential the cyber defence or offence. Operations can be used as a powerful strategic tool for political leaders. Finally, the examples in history demonstrated the importance of collaboration, not only between government departments but also with industry partners and allies. Collaboration improves the probability of discovering a cyber attack and swift resolution.

An examination of the legal and ethical frameworks as well as policies and concepts currently in place for cyber planners, lawmakers and decisions makers followed. The cyber domain has been described as a vital ground to national security. Yet when confronted with the questions regarding the developing laws and frameworks in place, some experts simply offer the advice that with time our comfort with the new cyber domain will be increasing, bringing with it robust and improved laws and policies.[265]

---

[265] Lucas, Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare, 42.

With more than 32 years since the first arrest of an American who conducted a cyber crime, how much more time will have to pass before the cyber domain is not considered new and the appropriate laws are in place?

The challenge with cyber conflict as it applies to LOAC is the fact that much of the information technology infrastructure is dual use. The impact of the dual use equipment is understanding the secondary effects and possibility of collateral damage of the cyber attack. This was demonstrated through the Morris Worm case study; this can be difficult for the commander to ascertain. The United Nations has several articles that were created with a view to protect and enable their member states to act ethically. There are several UN articles that may apply to the cyber domain. Article 2(4), enabling the use of force. Article 51 permits states to the right to self-defence. However, these Articles become a hindrance due to the language and the debate about whether actions in the cyber domain can be considered a use of force or an armed attack. As most damage created by a cyber attack is not permanent, this is widely debated if the United Nations articles apply. Examining Article 2(4) a little closer, the debate becomes more complex when considering the theory that an attack on national critical infrastructure could be considered a threat, by extension, a use of force. This situation may have applied to the SolarWinds case study.

Attribution can be both a hindrance and an asset in the cyber domain. The difficulties surrounding attribution not only as it relates to the technical complexities but also the ambiguous standards of attribution that call into question the legality of launching a cyber counter measure. Therefore making these actions challenging to justify. Attribution may be an asset if deniability is essential when launching a cyber

attack. The problematic and unclear standards of attribution give politicians and decisions makers plausible deniability should they not wish to be attributed to a cyber attack.

Just war theory, as well as the Tallinn Manual, are two frameworks available to decision makers and cyber planners to guide them through the cyber domain as they ensure their plans are ethical, lawful and just.

The last section examined the forms of cyber actions that Canada was previously restricted to conduct as well as passive cyber defence and active cyber defence. The policies Canada has in place to operate in the cyber domain display a concern for the security of Canadians, industry and government. The policies also attempt to bring a better understanding of the ambiguous legal and policy space the international community and international law have yet to develop and ratify.

Internationally it is still debated as to the importance of offensive cyber actions relative to defensive cyber. "Offence-defence theory has focused on whether it is possible to measure the offence-defence balance at all, to include whether it should encompass just technology or also some combinations of doctrine, manpower, resources, territory and even diplomacy."[266] It is clear that cyber is not the easy button solution to all conflict. Still, through the examination of the case studies, current policies and laws in place, offensive cyber actions are a crucial capability for nations to develop.

Although Canada is nascent in its offensive cyber capabilities, this paper has demonstrated the importance of a capable offensive cyber force as it applies to international relations, Canada's alliances, and the speed and impact of offensive cyber operations relative to a defensive posture. The CAF must build on already existing codes

[266] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 395.

of conduct and ethics and develop an ethical framework that cyber operators can use to ensure offensive cyber operations are conducted ethically. The framework would augment the Tallinn manual and provide Canadian cyber operators with additional guidelines, specific to Canadian morals, to assist in ethical cyber operations. As with traditional warfare the fog of war is present in cyber domain. Leaders and cyber operators must embrace the grey space and navigate within it. The Canadian specific ethical guidelines will enable CAF members to navigate the grey space. While there are still some areas for development across the community regarding the legalities and ethics of offensive cyber warfare, it is in Canada's best interest to develop offensive cyber capabilities. Canada is well positioned to responsibly and ethically move forward to develop offensive cyber capabilities.

BIBLIOGRAPHY

(CSE), Communication Security Establishment. "Cyber Journal." https://www.cse-cst.gc.ca/en/node/1493/html/25199#a2.

(CSE), Communications Security Establishment. "Foreign Cyber Operations." https://www.cse-cst.gc.ca/en/inside-interieur/cyberoperations-cyberoperations.

(DoJ), The United States Department of Justice. "Six Russian Gru Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

———. "U.S. Charges Russian Gru Officers with International Hacking and Related Influence and Disinformation Operations." https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

An Act Respecting National Security Matters. C-59.

Adams, James. The Next World War: Computers Are the Weapons and the Front Door Is Everywhere. New York: Simon and Schuster, 1998.

Adams, John. "2016 Policy Review Series." In *Canada and Cyber*, 6. Calgary AB: Canadian Global Affairs Institute, 2016.

Agency, Cybersecurity and Infrastructure Security. "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." Cybersecurity and Infrastructure Security Agency, https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

Akimenko, Valeriy, and Keir Giles. "Russia's Cyber and Information Warfare." *Asia policy* 15, no. 2 (2020): 67-75.

Andress, Jason, and Steve Winterfeld. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. 2nd ed. ed.: Elsevier, 2014.

Banks, William. "State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0." *Texas law review* 95, no. 7 (2017): 1487-513.

Banks, William C., and Evan J. Criddle. "Customary Constraints on the Use of Force: Article 51 with an American Accent." *Leiden journal of international law* 29, no. 1 (2016): 67-93.

Benmeziane, S., N. Badache, and S. Bensimessaoud. "Tor Network Limits." 2011.

Boer, L. J. M. "'Restating the Law "as It Is"': On the Tallinn Manual and the Use of Force in Cyberspace." *Amsterdam law forum* 5, no. 3 (2013): 4-18.

Bronskill, Jim. "Chinese Hackers Attacked National Research Council Computers." The Canadian Press, https://www.ctvnews.ca/mobile/canada/chinese-hackers-attacked-national-research-council-computers-1.2146400.

C. Czosseck, R. Ottis, K. Ziolkowski. "Ius Ad Bellum in Cyberspace – Some Thoughts on the ″Schmitt- Criteria" for Use of Force." *International Conference on Cyber Conflict* 4th (2012): 14.

Canada, Public Safety. "National Cyber Security Strategy." edited by Public Safety Canada, 35. Canada: Government of Canada, 2018.

Canfil, Justin Key. "Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity." *Journal of international affairs (New York)* 70, no. 1 (2016): 217-26.

CCDCOE. "Ccdcoe." https://ccdcoe.org/about-us/.

"Charter of the United Nations Chapter I." United Nations, https://www.un.org/en/sections/un-charter/chapter-i/index.html.

Chen, T. M., and S. Abu-Nimeh. "Lessons from Stuxnet." *Computer (Long Beach, Calif.)* 44, no. 4 (2011): 91-93.

Cull, Nicholas J., and Michael K. Hawes. *Canada's Public Diplomacy.* Palgrave Macmillan, 2020.

Davis, George Dewey, III. "The Digital Fog of Cyber: Case Study of the 2007 Cyber Attack on Estonia." ProQuest Dissertations Publishing, 2017.

Defence, Department of National. "Joint Doctrine Note Cyber Operations." edited by Department of National Defence, 121. Ottawa, 2017.

Defense, Department of. "Joint Publication 1-02." In Department of Defense Dictionary of Military and Associated Terms, 2016.

Defense, Office of the Secretary of. "Annual Report to Congress: Military and Security Developments Involving the People′s Republic of China." 2020.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War." *Security dialogue* 43, no. 1 (2012): 3-24.

DGIMO. "Cyber Task Force (Cyber Tf) - Vcds Establishment Directive." edited by Department of National Defence, 11. Ottawa, 2010.

Dickson, Janice. "Chinese Hackers Trigger Government Request to Spend $32.5 Million." iPolitics, https://ipolitics.ca/2015/02/19/chinese-hackers-trigger-government-request-to-spend-32-5-million/.

Elliott, Kevin A. "Active Cyber Defense and Attribution in Cyber Attacks." ProQuest Dissertations Publishing, 2018.

Evans, Mark. *Just War Theory: A Reappraisal.* New York: Palgrave Macmillan, 2005.

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival (London)* 53, no. 1 (2011): 23-40.

Fidler, David P. "Just & Unjust War, Use of Force & Coercion: An Ethical Inquiry with Cyber Illustrations." *Daedalus (Cambridge, Mass.)* 145, no. 4 (2016): 37.

Focarelli, Carlo. "Self-Defence in Cyberspace." 255-83: Edward Elgar Publishing, 2015.

Forces, Canadian Armed. "Cyber Operator." Department of National Defence, https://forces.ca.en/en/career/cyber-operator/.

FRANKLIN D. KRAMER, ROBERT J. BUTLER, and AND CATHERINE LOTRIONTE. "Cyber, Extended Deterrence, and Nato." 12. Washington D.C.: Atlantic Council, 2016.

Freeze, Colin. "China Hack Cost Ottawa ′Hundreds of Millions, Documents Show." The Globe and Mail, https://www.google.ca/amp/s/www.theglobeandmail.com/amp/news/national/federal-documents-say-2014-china-hack-cost-hundreds-of-millions-of-dollars/article34485219/.

Furnell, Steven, and Eugene H. Spafford. "The Morris Worm at 30." *ITNow* 61, no. 1 (2019): 32-33.

Gamreklidze, Ellada. "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia." *Journal of international communication* 20, no. 2 (2014): 200-17.

Green, James A. *Cyber Warfare: A Multidisciplinary Analysis.* Routledge Studies in Conflict, Security and Technology. 1 ed.: Routledge, 2015. doi:10.4324/9781315761565.

Haataja, Samuli. Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics. 1 ed. Abingdon, Oxon;New York, N.Y;: Routledge, 2019. doi:10.4324/9781351057028.

———. "Stuxnet." 136-66: Routledge, 2019.

Hayes, Jay P. Kesan and Carol M. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law & Technology* 25, no. 2 (Spring 2012 2021): 114.

Herzog, Stephen. "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity." *Georgetown journal of international affairs* 18, no. 3 (2017): 67-78.

Iasiello, Emilio J. "Russia's Improved Information Operations: From Georgia to Crimea." *Parameters (Carlisle, Pa.)* 47, no. 2 (2017): 51.

Josh Gold, Christopher Parsons and Irene Poetranto. "Canada′s Scattered and Uncoordinated Cyber Foreign Policy: A Call for Clarity." New York: Just Security, 2020.

Karlzén, Henrik. "Usefulness of Cyber Attribution Indicators." Reading, 2020.

Koch, Robert, Mario Golling, and Gabi Dreo Rodosek. "How Anonymous Is the Tor Network? A Long-Term Black-Box Investigation." *Computer (Long Beach, Calif.)* 49, no. 3 (2016): 42-49.

Kollmeyer, Barbara. "'Effectively, an Attack on the United States.' Microsoft Gets Caught up in Solarwinds Cyberattack." no. Journal, Electronic (2020).

Korzinski, Dave. "Five Years after Trudeau Promised Canada Was ′Back on the World Stage, Many Canadians Say We′re in the Same Place." Angus Reid Institute, https://angusreid.org/canada-international-reputation-un-security-council/.

Liaropoulos, Andrew. "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory." *European Conference on Information Warfare and Security* (2010): 177.

Lieblich, Eliav. "Internal Jus Ad Bellum." *The Hastings law journal* 67, no. 3 (2016): 687.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365-404.

Lonsdale, David J. "Warfighting for Cyber Deterrence: A Strategic and Moral Imperative." *Philosophy & technology* 31, no. 3 (2017): 409-29.

Lucas, George. Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Oxford University Press, 2017. doi:10.1093/acprof:oso/9780190276522.001.0001.

Macak, Kubo. "Decoding Article 8 of the International Law Commission′s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors." *Journal of conflict & security law* 21, no. 3 (2016): 405-28.

Magnus, Hjortdal. "China′s Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of strategic security* 4, no. 2 (2011): 1-24.

Masterson, Julia. "Timeline of Nuclear Diplomacy with Iran." Arms Control Association, https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran.

Meisels, Tamar. *Contemporary Just War Theory and Practice.* 1 ed. Vol. 1, Abingdon, Oxon;New York, NY;: Routledge, 2017. doi:10.4324/9781315172972.

Mejia, Eric F. "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework." *Strategic studies quarterly : SSQ* 8, no. 1 (2014): 114-32.

Meserve, Jeanne. "Study Warns of Cyberwarfare During Military Conflicts." CNN, http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html.

"The Morris Worm, the First Indictment under the Cfaa and Wake up Call of a New Age." Santa Monica: Newstex, 2020.

Nations, United. "Charter of the United Nations Chapter Vii." https://www.un.org/en/sections/un-charter/chapter-vii/index.html.

———. "UN Article 51." United Nations.

———. "UN Doc a/Res/56/83." United Nations, 2002.

"Nato Review Magazine." https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm.

Patrick Lin, Neil Rowe, and Fritz Allhoff. "Is It Possible to Wage a Just Cyberwar?" *The Atlantic*, 5 June 2012 2012.

Pomeroy, Jennifer, Nathan Swartz, Logan Suntzenich, and Kevin Winz. "Russia's Search for Stability: Cyber Capabilities and Military Buildup." *Current politics and economics of Russia, Eastern and Central Europe* 33, no. 1/2 (2018): 101-26.

Press, The Canadian. "Canadian Spies Say Chinese Hacked National Research Council." *Maclean ś* 2021, no. 28 April (2014).

publisher, No. "The Morris Worm." Washington: Newstex, 2018.

Rodriguez, Alex. "'Cyber Attack' Strikes Estonia; Ominous Denial-of-Service Campaign Wreaks Havoc: Final Edition." *The Ottawa citizen (1986)*, 2007.

"Russia′s Solarwinds Hack Was Espionage, Not an Act of War: Technology Companies Are Incensed, but the Federal Government Is More Sanguine." Washington, D.C: WP Company LLC d/b/a The Washington Post, 2020.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *The Columbia journal of transnational law* 37, no. 3 (1999): 885.

Schmitt, Michael N., and Nato Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Edited by Michael N. Schmitt and Liis Vihul. 2nd ed. Cambridge;New York, NY;: Cambridge University Press, 2017. doi:10.1017/9781316822524.

Shackelford, Scott J., and Richard B. Andres. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." *Georgetown journal of international law* 42, no. 4 (2011): 971.

Shoemaker, Dan, Anne Kohnke, and Greg Laidlaw. "Ethics and Cybersecurity Are Not Mutually Exclusive." *EDPACS* 60, no. 1 (2019): 1-10.

Sleat, Matt. "Just Cyber War?: Casus Belli, Information Ethics, and the Human Perspective." *Review of international studies* 44, no. 2 (2018): 324-42.

Springer, Paul J., Ebscohost, and Ebsco ebook. *Encyclopedia of Cyber Warfare.* Santa Barbara, Calif: ABC-CLIO, 2017.

Staff, Chief of the Defence. "Cds Initiating Directive for Defensive Cyber Operations." edited by Department of National Defence, 13. Ottawa, 2015.

Stevens, Clare. "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet." *Contemporary security policy* 41, no. 1 (2020): 129-52.

Svensson, Peter. "Georgian President′s Web Site Moves to Atlanta." *USA Today*, 11 August 2008.

Thompson, Jon. "The Morris Worm." *Personal computer world* (2009).

"Tor (Anynoymity Network)." https://en.wikipedia.org/wiki/Tor_(anonymity_network).

Tsagourias, Nicholas, and Michael Farrell. "Cyber Attribution: Technical and Legal Approaches and Challenges." *European journal of international law* 31, no. 3 (2020): 941-67.

"Uk Can Degrade Russia's Cyber Capabilities in the Same It Dismantled Isil's, Gchq Director Says." Telegraph.co.uk U6 - ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=UK+can+degrade+Russia%27s+cyber+capabilities+in+the+same+it+dismantled+Isil%27s%2C+GCHQ+director+says&rft.jtitle=Telegraph.co.uk&rft.date=2018-04-

12&rft.pub=Telegraph+Media+Group+Limited&paramdict=en-US U7 - Newspaper Article, 2018.

"Uk Can Degrade Russia's Cyber Capabilities in the Same It Dismantled Isil's, Gchq Director Says." *Telegraph.co.uk*, 2018.

Villeneuve, Nart. "Ru-Ge Skepticism." http://www.nartv.org/2009/08/25/ru-ge-skepticism/.

Walton, Robert. "Doe Confirms Its Systems Were Compromised by Solarwinds Hack." Washington: Industry Dive, 2020.

Wilby, Peter. "Georgia Has Won the Pr War." *The Guardian*, 18 August 2008.

Zetter, Kim, Inc OverDrive, and ebook OverDrive. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. 1st ed. New York: Crown Publishers, 2014.