National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

WHODUNIT: THE PROBLEM OF ATTRIBUTION AND LACK OF RECOURSE WITHIN THE CYBER DOMAIN

Major Patrick Leblanc

JCSP 45

Exercise *Solo Flight*

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 45

Exercice *Solo Flight*

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 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

WHODUNIT: THE PROBLEM OF ATTRIBUTION AND LACK OF RECOURSE WITHIN THE CYBER DOMAIN

Major Patrick Leblanc

WHODUNIT: THE PROBLEM OF ATTRIBUTION AND LACK OF RECOURSE WITHIN THE CYBER DOMAIN

Introduction

Power goes out along the entire eastern seaboard of North America. Hospitals struggle to save lives in the darkness. The stock market takes a dive. Traffic lights malfunction. The general population resorts to smart devices trying to sort out what is happening; however, all news media websites are not working and most devices have a hard time connecting to the internet. Military communications are weak at best. Chaos ensues. This situation is hypothetical; however, it is not out of the realm of the possible with the advancement of technology within the cyber domain. A similar power disruption due to malicious cyber-activity did happen briefly in Ukraine, but luckily the power companies were able to restore power quickly with the use of manual breakers.[1] This scenario could cause greater harm in North America as most power grid control systems within the US have no manual backup functionality.[2]

Since malicious cyber acts can be carried out inexpensively and from any connected location on the planet, perpetrators themselves are hard to pin down. This paper will demonstrate that no norms for recourse exist in the cyber domain due to the difficulty with attribution. Once the problem of attribution is solved, options for recourse may become standardized and a norm may develop over time. After a brief history and clarifying key definitions, examples of malicious cyber acts with the corresponding recourse taken will show the effects possible within the cyber domain. Once these effects

---

[1] Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," (*Wired*, 3 Mar 2016): Last accessed 11 Apr 2018, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[2] *Ibid.*

are demonstrated, this paper will then examine how law can be applied in the cyber domain. This law, along with the opinions of multiple organizations, will allow options for recourse to be developed which might possibly become global norms after the attribution problem is solved.

Originally created as an "open and secure commons of information,"[3] humans throughout the globe rely on the cyber domain for everything from energy to heat homes, managing transportation mediums, communications, public services, policing and military services.[4] More than 2 billion people send and receive more than 88 quadrillion emails annually.[5] This reliance on the cyber domain comes with vulnerabilities that many states are unable to effectively manage at present. The economic cost of malicious cyber activities ranges in the hundreds of billions of dollars annually on a global scale.[6] Nevertheless, trying to secure this domain to protect individuals, states, and critical public and private infrastructure must be balanced with the original intent of having a medium for unrestricted information transfer.[7]

The internet is still relatively young compared to human existence on the globe. The first modern web browser debuted in 1993.[8] As with the advent of any new technology, the full appreciation of its abilities and limitations, including vulnerabilities, is yet to be understood. Malicious activity within the cyber domain is carried out by

---

[3] Ronald J. Diebert, "Toward Distributed Security and Stewardship in Cyberspace." (Chap. 15 in *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland and Stewart, 2013): 235.

[4] Ralph Goodale, *National Cyber Security Strategy*, Ottawa: Public Safety Canada, 2018, 8.

[5] Paul Rosenzweig, "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (Fall 2012): 405.

[6] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015, 3.

[7] *Ibid.*

[8] James Joyner, "Competing Transatlantic Visions of Cybersecurity." Chap. 10 in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-172. Washington: Georgetown University Press, 2012, 159.

different groups and individuals for a multitude of reasons. Criminals or violent non-state actors might use the domain to carry out malicious acts for profit or advertise their actions in order to attract people to their ideologies, whereas states may support larger scale malicious acts for intelligence gathering purposes or more malevolent purposes.[9] When these acts occur, states react in different manners depending on a multitude of variables, including technical abilities, diplomacy, regime types, political cultures and domestic policies on privacy. There does not seem to be an excepted norm for how states can and should react to prosecute perpetrators.

Definitions

Before speaking about cyber-security issues and the problem of attribution, certain terms must be defined. The term cyberspace is used to describe the global virtual environment which "directly or indirectly interconnects systems, networks, and other infrastructures critical to the needs of society."[10] Cyberspace includes the internet. Malicious activities within cyberspace can consist of a broad range of actions, including both cybercrimes and cyber-attacks. To distinguish between cybercrime and cyber-attacks, it is generally understood that cybercrime involves using electronic means to violate domestic laws whereas cyber-attacks use electronic means to target information systems to accomplish traditional political or military objectives.[11]

Moreover, malicious cyber activity may not always or even usually constitute an actual attack. Article 51 of the UN Charter does not define what constitutes an "armed-attack," and since the applicable law depends on whether an armed attack has occurred,

[9] Ralph Goodale, National Cyber Security Strategy Public Safety Canada, 2018, 1.
[10] Johan Sigholm, "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013), 6.
[11] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." Georgetown Journal of International Law 47, no. 4 (2016): 1442.

most agree that the majority of malicious cyber activity falls below the threshold of an "armed attack."[12] The majority of malicious cyber activities fall more into the realm of cyber-espionage, which is defined as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information."[13]

Examples of Malicious Cyber Activity and Recourse Utilized

Dependency on the cyber domain has created vulnerabilities which have been exploited by state and non-state actors in the past, with each showcasing different means of recourse. Malicious cyber activities have either been offensive or exploitive. Offensive activities have endeavored to "alter, disrupt, deceive, degrade or destroy adversary computer systems"[14] whereas exploitive activities have endeavored "to obtain sensitive information."[15] Examples of these activities that have been carried out within the cyber domain showcased their increasing complexity, as well as increasing adverse effects. Malicious cyber activities have been carried out by the United States, Israel, Iran, Russia, North Korea and many other state and non-state actors.

In 2006, the U.S. and Israel created the Stuxnet worm that infiltrated the computer systems controlling nuclear power plant centrifuges in Iran. This worm created malfunctions within the machinery, causing centrifuges to spin faster than normal, resulting in physical damage to the system and impeding Iran's ability to develop nuclear weapons. This incident was one of the first times the cyber domain was used to inflict

---

[12] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." Georgetown Journal of International Law 47, no. 4 (2016): 1447; The United Nations Article 51, http://legal.un.org/repertory/art51.shtml, Last Accessed 19 April 2019.

[13] Eric Talbot Jensen, "the Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3 (2017): 756.

[14] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." Georgetown Journal of International Law 47, no. 4 (2016): 1448.

[15] *Ibid*.

physical damage.[16] Once discovered, Iran responded by launching an attack against a civilian oil company, utilizing methods and technology likely gained from studying the Stuxnet worm itself.[17] Iran's response destroyed data on more than 30,000 computers and replaced it with an image of a burning American flag.[18] Iran's response demonstrated resolve and highlighted the impact of giving away technical information by states, which is a side-effect of this kind of cyber-attack. Once Stuxnet was utilized, the creators were powerless to ensure the same technology did not fall into the hands of their adversaries.[19]

One of the most famous cyber events happened in 2007 when it was suspected that Russia launched a distributed denial of service (DDoS) attack on Estonia. Following riots in the nation's capital of Tallinn, a DDoS attack targeted Estonia's communication infrastructure.[20] The attack hijacked up to 85,000 computers and rendered Estonia unable to carry out administrative functions.[21] This incident is thought to be "one of the first known cases of a state attacking another state through cyberspace, and the first attack towards a NATO member."[22]

In 2008, Russia was once again alleged to have conducted a cyber-attack against Georgia this time. This attack defaced websites and essentially shut down Georgia's communication systems, blinding Georgian forces from the impending Russian invasion

---

[16] R.F.J. Dias, "The Lawless of Cyberspace: Do We Need an Internet Sheriff." (Joint Staff and Command College Course Paper, Canadian Forces College, 2016), 8.

[17] Alexander Moens, Seychelle Cushing, and Alan W. Dowd, "*Cybersecurity Challenges for Canada and the United States."* Fraser Institute, 2015. 12.

[18] *Ibid.*

[19] *Ibid.*

[20] *Ibid.,* 10.

[21] *Ibid.*

[22] *Ibid*.

that started the Russo-Georgian war. The cyber-attack, paired with the follow-on military offensive, demonstrated an emerging hybrid-warfare trend.[23]

In 2008, the United States was victim to exploitive malicious activity when a USB was installed in a laptop in the Middle-East. In this instance, unknown amounts of classified data were leaked.[24] Though the US did not pursue the attackers, this event did lead to the creation of the U.S. Cyber Command.[25]

In 2015, North Korea hacked into Sony enterprises due to their disapproval of the impending release of a movie about the fictional assassination of the North Korean Leader.[26] North Korean agents allegedly stole proprietary information from Sony and threatened to release the information if Sony released the motion picture. In response, the US President at the time, Barrack Obama, ordered sanctions against North Korea. This was the first time the U.S. responded to a foreign cyber-attack against a private company.[27]

More recently, in 2016, Russia is alleged to have interfered with the last U.S. Presidential election utilizing cyber means. Government computer networks were hacked and sensitive information was released in order to show vulnerabilities of presidential candidates.[28] The U.S. Intelligence community was able to attribute the attacks to Russia, paving the way for the President to issue an executive order which took measures against

---

[23] R.F.J. Dias, "The Lawless of Cyberspace: Do We Need an Internet Sheriff." (Joint Staff and Command College Course Paper, Canadian Forces College, 2016), 7.

[24] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." Georgetown Journal of International Law 47, no. 4 (2016): 1432.

[25] *Ibid.,* 1433.

[26] Peter Z. Stockburger, "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum." American University International Law Review 31, no. 4 (2016): 557.

[27] Christina Lam, "A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election." Boston College Law Review 59, no. 6 (2018): 2176.

[28] *Ibid.*, 2168.

Russia for perpetrating the theft and release of the information.[29] Some Russian individuals were blocked from conducting business within the United States and all of their assets within the United States were seized.[30] This reaction showed the US President's discontent with Russian actions during the election; however, this reaction alone did not stop or prevent further cyber intrusions from occurring.

As technology increases, the methods of inflicting harm through the cyber domain increases as well. Apart from the previous examples, there have been other instances of DDoS attacks throughout the globe. Computer networks called botnets have been created which are able to simultaneously control a large number of computers in order to overwhelm servers. Botnets make carrying out a DDoS attack achievable by sole individuals.[31] A single botnet, Rus-tock, is estimated to be responsible for two-fifths of the world's spam.[32] Both state and private industry struggle to prevent DDoS attacks and have difficulty attributing these attacks to specific perpetrators due to the widely dispersed nature of their attack.

As the previous examples show, each malicious cyber event resulted in distinct and different methods of recourse. The severity and effect of each attack was different, and the effectiveness of the recourse to prevent further attacks varied. As the rate and complexity of attacks increase, creating norms for recourse, although necessary, may become more difficult with time.

---

[29] *Ibid.,* 2169.

[30] *Ibid., 2169.*

[31] Benoit Dupont, "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime." Crime, Law and Social Change 67, no. 1 (2017): 100.

[32] James Joyner, "Competing Transatlantic Visions of Cybersecurity." Chap. 10 in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-172. Washington: Georgetown University Press, 2012. 165.

Applicability of Law in the Cyber Domain

Due to the abilities of malicious actors in the cyber domain increasing rapidly with the advancement of technology, states have struggled to create norms on how to react. Understanding what norms might be acceptable requires an understanding of what options are available under current laws in order to legitimize responses. Domestically, law enforcement systems are meant to process low-volume, high-impact crimes.[33] There is little ability of these systems, domestically or internationally, to process the high-volume, low or high impact crimes within the cyber domain, making recourse difficult.[34] Since the cyber domain crosses international boundaries, understanding how and if international law is even applicable is a starting point to creating accepted norms for offensive and defensive operations, including accepted methods of recourse.

International law's applicability within the cyber domain has been studied by numerous organizations including a group of experts brought together in Tallinn in 2012.[35] This group of experts examined how current international law was applicable in the cyber domain, not how it could be applied or altered in the future.[36] Though sponsored by the North Atlantic Treaty Organization (NATO), the authors pointed out that the manual itself was not a NATO, United Nations (UN) or U.S. Department of Defense (DoD) product, emphasizing the legitimacy of the manual on a global scale.[37] The manual was subsequently edited to broaden its scope to include cyber operations,

---

[33] Benoit Dupont, "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime." Crime, Law and Social Change 67, no. 1 (2017): 98.

[34] *Ibid*.

[35] Michael N. Schmitt, "Tallinn Manual." *YouTube* streaming. September 29, 2012. Posted March 30, 2016. http://youtu.be/wY3uEo-Itso. CyCon 2012, Tallinn, Estonia, Last Accessed 19 April 2019.

[36] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3 (2017): 738.

[37] Michael N. Schmitt, "Tallinn Manual." *YouTube* streaming. September 29, 2012. Posted March 30, 2016. http://youtu.be/wY3uEo-Itso. CyCon 2012, Tallinn, Estonia, Last Accessed 19 April 2019.

both in and out of conflict, resulting in the Tallinn Manual 2.0.[38] The experts themselves included members from both western and non-western states.[39] Though commentary throughout the manual highlights instances where the experts had differing opinions on how the law should be applied within the cyber domain, they all agreed that existing norms of international law did, in fact, apply in cyberspace.[40]

When applying international law within the cyber domain from a security perspective, it is important to understand how *jus ad bellum* and *jus in bello* come into play. *Jus ad bellum* applies prior to an armed conflict and limits states to using defensive force proportionate to the unlawful aggression of another state. If an armed conflict breaks out, *jus in bello*, or the Law of Armed Conflict (LOAC), applies, and prohibits states from attacking an enemy with force "that will lead to excessive civilian casualties in relation to legitimate military objectives."[41] Though both circumstances are applicable within the cyber domain, questions remain about permissible avenues of recourse and how victim states can respond proportionately.

Both *jus ad bellum* and *jus in bello* limit the actions of a state to be proportional to the illegal acts of an aggressor state. During an armed conflict, *jus in bello* prohibits an attack which "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in

---

[38] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3 (2017): 735.

[39] *Ibid.*, 738.

[40] Michael N. Schmitt, "International Law and Cyberwar: A Response to the Ethics of Cyberweapons." *Ethics & International Affairs*. February 10, 2014. http://www.ethicsandinternationalaffairs.org/2014/international-law-and-cyberwar-a-response-to-the-ethics-of-cyberweapons/.

[41] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." Georgetown Journal of International Law 47, no. 4 (2016): 1434.

relation to the concrete and direct military advantage anticipated."[42] This same principle can be applied in the cyber domain.[43] Since cyber-attacks may have unpredictable secondary and tertiary effects, however, it may become difficult to prevent collateral damage.[44] Most importantly, if attribution is incorrect, any recourse could also be deemed excessive or illegal.

A second issue with regards to collateral damage and proportionality is that the majority of military communications use civilian networks. This dual-use of networks makes legal distinction of military targets difficult, as well the ability to comprehend whether effects will be proportionate challenging.[45] Finally, since cyber-attacks may cause physical damage, the same law governing force must be applied to kinetic and cyber strikes. For example, destroying a civilian hospital through kinetic means or rendering it inoperable through cyber means would both violate the *jus in bello* principle of proportionality.[46]

Many scholars agree that most conflicts within the cyber domain do not pass the threshold of an armed attack, which makes the applicability of *jus ad bellum* and *jus in bello* null in these circumstances.[47] When looking for acceptable means of recourse, a more applicable method of applying an international law would be to apply the international law of countermeasures. "The international law of countermeasures

---

[42] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-885. 850. http://digitalcommons.law.yale.edu/fss_papers/3852. Last Accessed 18 April 2019.

[43] Stephen Petkis, "Rethinking Proportionality … 1439.

[44] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack… 850.

[45] D.W. Brown, "Real Problems in the Virtual World: International Law Priorities Regarding Cyber-Conflict." (Joint Staff and Command College Course Paper, Canadian Forces College, 2016), 17.

[46] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." Georgetown Journal of International Law 47, no. 4 (2016): 1457.

[47] Scott J. Shackelford, Scott Russell, and Andreas Kuchn. "Unpacking the International Law on Cybersecurity due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* 17, no. 1 (2016): 3.

regulates how states can respond to violations that do not rise to the level of an armed attack justifying self-defense."[48] Countermeasures are "otherwise unlawful actions (or omissions) that are legally permitted when used by a victim state in response to unlawful activity to induce the offending state to cease the unlawful activity."[49] Countermeasures must also be proportional, which may cause the same issues when applying *jus ad bellum* and *jus in bello* to the cyber domain. They must also be temporary in nature and reversible as far as possible, another issue that may prove difficult within the cyber domain.[50] The law also has a requirement for states to notify and potentially seek to negotiate a resolution prior to using a countermeasure.[51] This requirement may pose a problem as this would require states to showcase their technical abilities within the cyber domain which could display vulnerabilities for other enemies to exploit.

Since the majority of malicious cyber activities do not constitute attacks, viewing them like acts of espionage may offer some solutions for how states may respond. Both espionage and the majority of malicious cyber incidents do not amount to a "use of force", therefore in both instances, the LOAC does not apply.[52] Since espionage has never been considered a legitimate reason for going to war, treating malicious cyber activities in the same manner allows states to carry out methods of recourse short of

---

[48] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-885, 856. http://digitalcommons.law.yale.edu/fss_papers/3852. Last Accessed 18 April 2019.

[49] Scott J. Shackelford, Scott Russell, and Andreas Kuchn. "Unpacking the International Law on Cybersecurity due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* 17, no. 1 (2016): 17.

[50] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3 (2017): 754.

[51] *Ibid*, 754.

[52] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." *Georgetown Journal of International Law* 47, no. 4 (2016): 1447.

declaring war.[53] For acts deemed espionage, states have resorted to reducing commerce, expulsing diplomats or increasing their own espionage efforts.[54] These same avenues could be utilized when responding to a cyber-incident; however, the nature of the dispersed network of the cyber domain may cause more issues. States traditionally criminalized espionage as a matter of domestic law, which was possible given offenders were usually caught within the sovereign territory of the state.[55] This method does not work as well in the cyber domain due to the ability of cyber acts to be carried out from distant states by unknown perpetrators.

Organizations Focused on Cyber Security

Groups including the UN, the European Council, the Shanghai Cooperation Organization, the Organization of the American States (OAS), NATO, the G7, and the Internet Engineering Task Force (IETF) among others have all gathered at different times to discuss cyber security on a global level. The majority of the groups agree that international law and the UN Charter apply within the cyber domain and all discussed methods to develop norms for security. The problem of attribution was mentioned by some groups, but not all. Having all groups globally agree is a challenge; however, that goal is being taken on by the Global Commission on the Stability of Cyberspace (GCSC).

The UN has looked at issues of security within the cyber domain and how its own Charter would apply. Part of the mandate of the UN Security council is to "determine the existence of a threat to the peace, breach of the peace, or act of aggression," and can

---

[53] D.W. Brown, "Real Problems in the Virtual World: International Law Priorities Regarding Cyber-Conflict." (Joint Staff and Command College Course Paper, Canadian Forces College, 2016), 21.

[54] *Ibid*.

[55] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3 (2017): 742.

decide what actions could be taken in accordance with Articles 41 and 42.[56] Given this responsibility, it would seem fitting that this organization looked at establishing norms and applying international law within the cyber domain. In 1999, the UN sponsored a meeting to "grasp the security implications of emerging information technologies."[57] Follow up resolutions called for further discussions on cyber security; however, these meetings never produced any binding set of norms that states could reference when devising methods of recourse after suffering from malicious cyber activities.[58]

The United Nations also created the Group of Governmental Experts on Developments in the Field of Information and Telecommunications (UN CGE) in 2004, initially consisting of 15 countries which grew to 25 countries by 2016.[59] The UN CGE agreed that international law and the UN Charter, along with sovereignty and norms associated with sovereignty, all applied within the cyber domain.[60] The UN CGE emphasized that "states must meet international obligations regarding internationally wrongful acts attributable to them."[61] This obligation would have been difficult to enforce within the cyber domain due to the issues surrounding attribution. The UN CGE did agree that states have jurisdiction over ICT infrastructure within their territory, solidifying the need for states to police the cyber domain within their territorial boundaries.[62] The UN CGE clarified that states are not to use proxies to commit

---

[56] United Nations, "UN Charter," Article 39. https://www.un.org/en/charter-united-nations/

[57] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-885, 860. http://digitalcommons.law.yale.edu/fss_papers/3852. Last Accessed 18 April 2019.

[58] *Ibid*.

[59] Michael N. Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN CGE's Failure to Advance Cyber Norms", Just Security, 30 Jun 2017. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cybernorms/

[60] *Ibid.*

[61] *Ibid.*

[62] *Ibid.*

internationally wrongful acts; however, the ability to monitor and enforce this would have been difficult.[63] Ultimately, this group collapsed due to irreconcilable differences between some states' acceptance of the applicability of self-defense and countermeasures. Cuba, in particular, did not agree that malicious use of ICTs could amount to an 'armed attack' as provided for in Article 51 of the UN Charter. Some, however, speculate that the real issue was the inequality between states' technical ability to attribute hostile cyber operations which caused Cuba to see this as a disadvantage.[64]

The European Council has also studied security in the cyber domain, resulting in the promulgation of policy that actually has some binding effect. In 2001, the council held a convention on cybercrime that created a policy relying on international cooperation and legislation.[65] Signatories to the convention agreed to cooperate with cybercrime investigations; however, no repercussions were conveyed should a state breach the intent of the convention.[66]

Regional groups also discussed cyber-security issues and attempted to establish norms. The Shanghai Cooperation Organization, which was founded in 2001 by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan, stressed the importance of ensuring international information security, however did not provide expected norms for recourse.[67] This group thought that state control over information technologies and threats was permitted and viewed the "dominant position in the information space" of

---

[63] *Ibid.*
[64] *Ibid.*
[65] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-885, 863. http://digitalcommons.law.yale.edu/fss_papers/3852. Last Accessed 18 April 2019.
[66] *Ibid.*, 864.
[67] *Ibid.*, 865.

Western nations to be threats to their own sovereignty.[68] This rift impeded any developments of global norms for recourse that may have been constructed.

In South America, the OAS approved a resolution in 2004 encouraging states to evaluate the principles that came out of the Council of Europe Convention on Cybercrime. The OAS also adopted a cyber-security strategy which aimed to adopt "cybercrime policies and legislation that will protect internet users and prevent and deter criminal misuse of computers and computer networks, while respecting the privacy and individual rights of internet users."[69] The OAS went one step further when it agreed to deploy experts to draft and enact laws that punish cybercrime and recommended that all members establish state bodies for investigating and prosecuting cyber-crimes which would enable international cooperation at the same time.[70] Though promising, the problems of attribution and the lack of technical ability to achieve it were not addressed, preventing norms for recourse from being developed.

NATO also conducted its own studies of cyber-security. Although the organization agreed that international law and the UN Charter applied in cyberspace,[71] it failed to come to a consensus on what global norms should be accepted. NATO was the driving factor behind the Tallinn manual and created the Cooperative Cyber Defence Centre of Excellence (CCD COE).[72] As a purely defensive organization, NATO was not in a position to use offensive cyber capabilities; however, some of its members were, and

---

[68] Rosenzweig, Paul. "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (Fall 2012): 427.

[69] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-885, 864. http://digitalcommons.law.yale.edu/fss_papers/3852. Last Accessed 18 April 2019.

[70] *Ibid.*, 865.

[71] Wales Summit Declaration (5 September 2014), Last accessed 11 April 2019. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[72] R.F.J. Dias, "The Lawless of Cyberspace: Do We Need an Internet Sheriff." (Joint Staff and Command College Course Paper, Canadian Forces College, 2016), 6.

continue to be, world leaders in cyber operations.[73] These states give NATO offensive capabilities that can act as a deterrence factor from cyber aggression and may provide a method of recourse when required.[74] NATO members have agreed their common approach to cyber-defense will obligate members to consult with one another under Article 4 of the NATO treaty; however, a cyber-attack may not be treated the same as an armed attack under Article 5 of the treaty.[75] This may limit options for recourse from less technically savvy members when they fall victim to malicious cyber activities. When and if a cyber-attack should be treated under Article 5 of the treaty would be looked at on a case-by-case basis by NATO, indicating that no norms for recourse have yet been invented.[76]

Members of the G7 have also discussed security within the cyber domain and in 2017 approved a Declaration on Responsible State Behaviour in Cyberspace.[77] Within this declaration, G7 members were concerned about the risk of escalation of malicious cyber activity between states. The declaration encouraged all states to engage in "law-abiding, norm-respecting and confidence building behavior in the use of ICT."[78] Suggestions within the declaration included not allowing ICT infrastructure to knowingly be used for malicious activities, not perpetrating wrongful acts through proxies, cooperating to prosecute offenders, respecting human rights within the cyber domain,

---

[73] James Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence." *CCDCOE Tallinn Paper*, no. 8 (2015). 2.

[74] *Ibid.*, 3.

[75] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-885, 846. http://digitalcommons.law.yale.edu/fss_papers/3852. Last Accessed 18 April 2019.

[76] Wales Summit Declaration (5 September 2014), Last accessed 11 April 2019. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[77] Mariarosaria Taddeo, "Deterrence by Norms to Stop Interstate Cyber Attacks." Minds and Machines 27, no. 3 (2017): 387.

[78] G7 Declaration on Responsible States Behavior in Cyberspace LUCCA, 11 APRIL 2017, 1. https://www.mofa.go.jp/files/000246367.pdf

helping victim states when required, reporting ICT vulnerabilities and fixes for these vulnerabilities, abstaining from stealing intellectual property for competitive edges and protecting the integrity of the ICT supply chain so end products are safe for consumers.[79] The declaration recognized that international law and the UN Charter was applicable within the cyber domain and stated that law provided a framework for responses to wrongful acts that do not amount to an armed attack.[80] Though the declaration stated that proportionate countermeasures, including hack-back techniques, were acceptable, it also acknowledged the problem of attribution and the difficulty for some states to accomplish this necessary task prior to applying any methods of recourse.[81]

Some groups possess technical abilities that need to be incorporated in developing any norms for methods of recourse. The Internet Engineering Task Force (IETF) is one of these groups. The IETF develops technical aspects of computer code and protocols that drive the internet.[82] The group is comprised of an "open international community of network designers, operators, vendors and researchers concerned with the evolution of the internet architectures and the smooth operation of the internet."[83] Though their mission is to make the internet function better technically, their technical ability may be required to both help states with the problem of attribution and develop effective means of stopping malicious cyber acts. Since this group is open, inclusive and non-partisan, the standards set by this group have already become globally accepted, which may give them leverage when attempting to create global norms for recourse.[84]

---

[79] *Ibid.*, 4.
[80] *Ibid.*, 2.
[81] *Ibid.*, 3.
[82] Paul Rosenzweig, "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (Fall 2012): 410.
[83] *Ibid.*, 410.
[84] *Ibid.,* 411.

Most groups discussing security in the cyber domain agree in some areas but not all. To bring these groups together, the GCSC was formed in 2014 to make recommendations about the future of global internet governance.[85] This commission is an international initiative that hopes to facilitate effective cooperation on the global level. The commission promotes mutual awareness and understanding amongst the many different groups discussing cyber security, including private industry, academics, state and non-state actors. This initiative may be able to link the opinions of different organizations in hopes of finally coming up with a globally accepted set of norms and proposals within the cyber domain which all states can draw from when deciding on methods of recourse for malicious cyber acts.[86]

The Problem of Attribution

Applying any law in the cyber domain requires proper attribution. The dispersed network makes the process of attribution problematic, if not impossible, depending on the technical expertise resident within a victim state.[87] For most laws, being able to pinpoint a perpetrator is necessary in order to pursue any recourse against that entity. Before any recourse can be actuated, understanding who the perpetrator is, whether they are a state, non-state actor or an individual, may pose different options for that recourse.[88] Denial of service attacks that overload servers usually come from thousands of distributed computers at the same time.[89] Spoofing or hiding the location of the origin of a cyber-

---

[85] Global Commission on the Security of Cyberspace, www.cyberstability.org.

[86] *Ibid.*

[87] James Joyner, "Competing Transatlantic Visions of Cybersecurity." Chap. 10 in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-172. Washington: Georgetown University Press, 2012. 160.

[88] D.W. Brown, "Real Problems in the Virtual World: International Law Priorities Regarding Cyber-Conflict." (Joint Staff and Command College Course Paper, Canadian Forces College, 2016), 10.

[89] Stephen Petkis, "Rethinking Proportionality in the Cyber Context." *Georgetown Journal of International Law* 47, no. 4 (2016): 1445.

incident is also common practice amongst perpetrators and makes attributing incidents to a state extremely difficult. [90] As technology advances, the ability to pinpoint perpetrators increases; however, these same technological advancements may enable perpetrators better options for concealing their true identity. If attribution is unattainable, yet required for legal prosecution either domestically or internationally, then there may be no legal means of recourse available.

Much focus is placed on securing the cyber domain rather than providing avenues to pursue perpetrators. Perhaps this is due to a growing realization that pursuing perpetrators is technically difficult due to the issue of attribution. Without the ability to accurately attribute any malicious activity to a perpetrator, then the option of "hack-back" is not viable as wrongful accusations may cause greater repercussions.[91] As technologies advance and the availability of methods of distinguishing attribution becomes attainable to more states, a global ability to pursue perpetrators may increase. Understanding trademarks of certain malicious actors within the cyber domain may also allow for the buildup of a library where states would be able to leverage the information in order to ascertain where malicious cyber activity originated.[92]

Even if states obtain the abilities that would allow them to correctly attribute cyber activities to perpetrators, pursuing and apprehending those responsible may prove impossible. The intelligence used for attribution may not be admissible as evidence in court, and states may not even be willing to disclose how they obtained the necessary

---

[90] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3 (2017): 751.

[91] Ingolf Pernice, "Global Cybersecurity Governance: A Constitutionalist Analysis." Global Constitutionalism 7, no. 1 (2018): 117.

[92] Eric Lipton and David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times, 13 Dec 2016. Last Accessed 23 April 2019. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

intelligence required for attribution in the first place. Since the International Criminal Court takes on cases of genocide, war crimes, crimes against humanity and crimes of aggression,[93] there may be no international venue to try perpetrators in the cyber domain.

Though experts agree that law applies in the cyber domain, who should create norms within the cyber domain and what avenues for recourse should be made available are debatable. Differing states do not even agree on who should take the lead on cyber security and recourse, with the US and UK treating cyber-security as a national security problem to be handled by the military and the rest of the European Union treating cyber threats as a commerce and private industry problem to be dealt with by civilian and private enterprises.[94]

To pursue any perpetrator, the problem of attribution must be overcome. In order to properly attribute malicious activity, private companies with the expertise must be leveraged and paired with policy makers and law enforcement.[95] Leveraging private industry expertise may also allow reverse engineering of malicious cyber activity, giving states more offensive capability when required.[96] Private industry should look at this as an opportunity to expand their business through the development of new products and services.[97] Companies such as Crowdstrike have already displayed an ability to successfully attribute cyber-attacks to certain perpetrators, as evidenced in the alleged

---

[93] International Criminal Court "About" https://www.icc-cpi.int/about - Last Acessed 04 May 2019.

[94] James Joyner, "Competing Transatlantic Visions of Cybersecurity." Chap. 10 in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-172. Washington: Georgetown University Press, 2012. 159.

[95] Victor Platt, "Still the fire-proof house? An analysis of Canada's cyber security strategy." *International Journal* 67, no. 1 (Winter 2011/2012): 164.

[96] Alexander Moens, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015. 7.

[97] Ron Deibert, Canada and the Challenges of Cyberspace Governance and Security School of Public Policy, University of Calgary, 2013. 3.

Russian hacking during US elections.[98] Microsoft has also been leveraged to stop botnets by using their own technology to intercept malicious software, preventing more machines from becoming infected and identifying the source machines from which malicious code originated.[99] Internet service providers (ISPs) can also be leveraged in investigations as they hold a monopoly over technical infrastructure that allows data to flow over the Internet.[100] Western nations have already begun to leverage ISPs to assist with policing the internet, however so far the policing has had little judicial oversight.[101] In order for this trend of state-private industry partnership to evolve, policy makers must allow this relationship to tackle the problem of attribution legally.

Once attribution has successfully been accomplished, then states can consider options for recourse. Depending on the nature of a cyber-incident, a realm of possibilities exists for recourse. In extreme circumstances, possibilities could consist of using kinetic effects. This would hold true if the nature of the cyber incident was considered to have breached the level of an armed attack.

If the armed attack threshold was crossed, then options for recourse would need to comply with the Article 51 of the UN Charter.[102] If the armed attack threshold was not deemed to have been crossed, then cyber incidents would be treated at a lower level and

---

[98] Eric Lipton and David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times, 13 Dec 2016. Last Accessed 23 April 2019. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

[99] Brad Smith, "The need for a Digital Geneva Convention", RSA Conference, Feb 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[100] Benoit Dupont, "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime." Crime, Law and Social Change 67, no. 1 (2017): 108.

[101] Ron Deibert, "Canada and the Challenges of Cyberspace," Governance and Security School of Public Policy, University of Calgary, 2013. 3.

[102] Michael N. Schmitt, "International Law and Cyberwar: A Response to the Ethics of Cyberweapons." *Ethics & International Affairs*. February 10, 2014. http://www.ethicsandinternationalaffairs.org/2014/international-law-and-cyberwar-a-response-to-the-ethics-of-cyberweapons/.

responses would need to be proportional. To counter cyber incidents that fall below the threshold of an armed attack, the law of countermeasures would apply and limit options for recourse for states.[103] Some forms of recourse could include economic or diplomatic sanctions or a counter-cyber operation that could be controlled to meet proportionality requirements.[104]

Since the law of countermeasures only applies to states, if malicious cyber activities are carried out by non-state actors, then domestic law, partnered with private industry, must be able to prosecute these perpetrators.[105] There is a growing consensus that the establishment of state cybercrime laws are growing into international obligations.[106] If states are able to definitively attribute malicious cyber activities to perpetrators and align their responses, perhaps more would be willing to enter into treaties making avenues of recourse *Opinio Juris*, forcing non-signatory states into compliance.[107] Over time, norms for recourse may be recognized and could potentially become customary international law.

Conclusion

Though the cyber domain is relatively new, malicious offenders have already taken advantage of the dispersed network to carry out harmful activities from a safe distance. Examples of these acts are numerous, yet the responses to each one seems to have varied in structure and effectiveness. Even though most groups agree that law is

---

[103] *Ibid.*

[104] Scott J. Shackelford, Scott Russell, and Andreas Kuchn. "Unpacking the International Law on Cybersecurity due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* 17, no. 1 (2016): 31.

[105] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3 (2017): 753.

[106] Scott J. Shackelford, Scott Russell, and Andreas Kuchn. "Unpacking the International Law on Cybersecurity due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* 17, no. 1 (2016): 6.

[107] *Ibid*., 7.

applicable within this new domain, the problem of attribution prevents recourse norms from being developed. Multiple organizations have created different solutions to how the cyber domain should be secured; however, none have solved the attribution problem.

Not only is attribution difficult due to the technical knowledge required, states may also be reluctant to prove attribution. Displaying proof of attribution might showcase a state's abilities within the cyber domain which may be knowledge they would not want other adversaries to know. Fear of damage to reputations or market perceptions within the private industry may also dissuade victims of malicious cyber acts from attempting to recover losses or seek recourse.[108] To overcome the difficulties associated with attribution, cooperation will be necessary amongst armed forces, law enforcement, intelligence agencies, private industry, technical experts and average internet users.[109]

In a utopian society, a new treaty could be developed that regulated everyone's actions within the cyber domain, making these regulations law.[110] Perhaps a new global organization that could govern the cyber domain is required much like the international atomic energy agency governs nuclear weapons.[111] The problem in the cyber domain is that attribution is difficult, whereas "nuclear missiles come with a return address."[112] The

---

[108] Guy Batar, The legal ramifications of a cyber attack, Chief Information Officer Magazine, International Data Group, 26 Aug 2015. https://www.cio.com.au/article/583042/legal-ramifications-cyber-attack/

[109] Ronald J. Diebert, "Toward Distributed Security and Stewardship in Cyberspace." Chap. 15 in *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland and Stewart, 2013, 242.

[110] Christina Lam. "A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 u.s. Presidential Election." Boston College Law Review 59, no. 6 (2018): 2196.

[111] Brad Smith, "The need for a Digital Geneva Convention", RSA Conference, Feb 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[112] James Joyner, "Competing Transatlantic Visions of Cybersecurity." Chap. 10 in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 159-172. Washington: Georgetown University Press, 2012. 160.

suggestion of such a group has been made by numerous organizations already and yet norms for recourse cease to exist. Norms take time to construct and until states can accurately and easily attribute malicious cyber activities to definite perpetrators, recourse norms will never develop.

BIBLIOGRAPHY

Arquilla, John. “The Computer Mouse that Roared: Cyberwar in the Twenty-First Century.” *Brown Journal of World Affairs* 18, no. 1, 2011.

Batar, Guy, The legal ramifications of a cyber attack, Chief Information Officer Magazine, International Data Group, 26 Aug 2015. https://www.cio.com.au/article/583042/legal-ramifications-cyber-attack/

Brown, D.W. “Real Problems in the Virtual World: International Law Priorities Regarding Cyber-Conflict.” Joint Staff and Command College Course Paper, Canadian Forces College, 2016.

Dias, R.F.J. “The Lawless of Cyberspace: Do We Need an Internet Sheriff.” Joint Staff and Command College Course Paper, Canadian Forces College, 2016.

Deibert, Ronald J. “Canada and the Challenges of Cyberspace Governance and Security.” School of Public Policy, University of Calgary, 2013.

Diebert, Ronald J. “Toward Distributed Security and Stewardship in Cyberspace.” Chap. 15 in *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland and Stewart, 2013.

Dupont, Benoit. "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime." Crime, Law and Social Change 67, no. 1, 2017.

G7 Declaration on Responsible States Behavior in Cyberspace LUCCA, 11 APRIL 2017 https://www.mofa.go.jp/files/000246367.pdf

Global Commission on the Stability of Cyberspace, https://cyberstability.org/about/

Goodale, Ralph. National Cyber Security Strategy Public Safety Canada, 2018.

Gopalan, Sandeep, “Is Counter-Attack Justified Against a State Sponsored Cyber-Attack? It’s a Legal Grey Area. The Conversation, 27 March 2018. http://theconversation.com/is-counter-attack-justified-against-a-state-sponsored-cyber-attack-its-a-legal-grey-area-94023

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." California Law Review 100, no. 4, 2012. http://digitalcommons.law.yale.edu/fss_papers/3852

International Criminal Court. “About” https://www.icc-cpi.int/about

Jensen, Eric Talbot. "the Tallinn Manual 2.0: Highlights and Insights." Georgetown Journal of International Law 48, no. 3, 2017.

Joyner, James. “Competing Transatlantic Visions of Cybersecurity.” Chap. 10 in *Cyberspace and National Security: Threats, Opportunities, and Power in a*

Virtual World, edited by Derek S. Reveron, 159-172. Washington: Georgetown University Press, 2012.

Lam, Christina. "a Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 u.s. Presidential Election." Boston College Law Review 59, no. 6, 2018.

Lewis, James. "The Role of Offensive Cyber Operations in NATO's Collective Defence." *CCDCOE Tallinn Paper*, no. 8 (2015).

Lipton, Eric and David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times, 13 Dec 2016. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Moens, Alexander, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute, 2015.

Pernice, Ingolf. "Global Cybersecurity Governance: A Constitutionalist Analysis." Global Constitutionalism 7, no. 1 (2018): 112-141.

Petkis, Stephen. "rethinking Proportionality in the Cyber Context." Georgetown Journal of International Law 47, no. 4, 2016.

Platt, Victor. "Still the fire-proof house? An analysis of Canada's cyber security strategy." *International Journal* 67, no. 1 (Winter 2011/2012): 155-167.

Rid, Thomas. "Cyberwar and Peace: Hacking can Reduce Real-World Violence." Foreign Affairs 92, no. 6 (2013): 77-87.

Rosenzweig, Paul. "The International Governance Framework for Cybersecurity." *Canada-United States Law Journal* 37, no. 2 (Fall 2012): 405-432.

Royal Canadian Mounted Police Cybercrime Strategy Royal Canadian Mounted Police, 2015. https://www.deslibris.ca/ID/248701

Schmitt, Michael N. "Tallinn Manual." *YouTube* streaming. September 29, 2012. Posted March 30, 2016. http://youtu.be/wY3uEo-Itso. CyCon 2012, Tallinn, Estonia.

Schmitt, Michael N. "International Law and the Use of Force (The Jus Ad Bellum)." *YouTube* streaming. 01 April 2014. https://www.youtube.com/watch?v=fcGfvWSXEHA

Schmitt, Michael N. "International Law and Cyberwar: A Response to the Ethics of Cyberweapons." *Ethics & International Affairs*. February 10, 2014. http://www.ethicsandinternationalaffairs.org/2014/international-law-and-cyberwar-a-response-to-the-ethics-of-cyberweapons/.

Schmitt, Michael N. and Liis Vihul, “International Cyber Law Politicized: The UN CGE’s Failure to Advance Cyber Norms”, Just Security, 30 Jun 2017. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cybernorms/

Schmitt, Michael N. and NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge;New York;: Cambridge University Press, 2013.

Schmitt, Michael N. and NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge;New York, NY;: Cambridge University Press, 2017

Shackelford, Scott J., Scott Russell, and Andreas Kuchn. "Unpacking the International Law on Cybersecurity due Diligence: Lessons from the Public and Private Sectors." Chicago Journal of International Law 17, no. 1, 2016.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013)

Smith, Brad. “The need for a Digital Geneva Convention”, RSA Conference, Feb 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

Stockburger, Peter Z. "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum." American University International Law Review 31, no. 4, 2016.

Taddeo, Mariarosaria. "Deterrence by Norms to Stop Interstate Cyber Attacks." Minds and Machines 27, no. 3 (2017): 387-392.

The United Nations, “UN Charter,” Article 39. https://www.un.org/en/charter-united-nations/

The United Nations, “UN Charter, Article 51, http://legal.un.org/repertory/art51.shtml

Wales Summit Declaration (5 September 2014), Last accessed 11 April 2019. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

Who Runs the Internet? Centre for International Governance Innovation, 2016.

Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”Wired, 3 Mar 2016. Last accessed 11 Apr 2018. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/