Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law.

Jason D. Jolley †

Submitted in fulfillment of the degree of Doctor of Philosophy, School of Law, University of Glasgow

PhD Thesis
University of Glasgow

† The author is a retired law enforcement officer of the United States federal government. All material and opinions herein are the authors alone and do not reflect any official position of the United States government. No classified information was utilized in this study from any source. The author is bound by United States federal law and a non-disclosure agreement between the author and the United States government as put forth in 32 C.F.R. 2001/2003 *et seq*. (2016) prohibiting discussion concerning any past, current, or future unauthorized disclosures of any classified information irrespective of source or follow-on reporting. Specifically, the author has been advised that:

> the unauthorized disclosure… of classified information [by the author] could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. [The author has agreed] that [he] will never divulge classified information to anyone unless: (a) [the author has] officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) [the author has]been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting [the author] a security clearance that such disclosure is permitted. [The author] understand[s] that if [he is] uncertain about the classification status of information, [he is] required to confirm from an authorized official that the information is unclassified before [he] may disclose it, except to a person as provided in (a) or (b), above. [The author] further understand[s] that [he is] obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information. (NDA, SF-312 (1-00)).

As such, this study does not address any allegations concerning reported classified intelligence operations conducted on behalf of the United States government disclosed by Edward Snowden or WikiLeaks, irrespective of the source of said information.

Abstract

Malicious cyber-attacks, those cyber-attacks which do not rise to the level of force in international law, pose a significant problem to the international community. Attributing responsibility for malicious cyber-attacks is imperative if states are to respond and prevent the attacks from continuing. Unfortunately, due to both technical and legal issues attributing malicious cyber-attacks to the responsible state or non-state actor is difficult if not impossible in the vast majority of attacks. Even if an injured state may recursively trace the malicious cyber-attack to the responsible IP address, this is not enough under the current international customary law to hold a state or non-state actor responsible for the cyber-attack as it is virtually impossible to bridge the air gap between the computer system and end user to demonstrate affirmatively who initiated the attack. Even if a state could demonstrate the identity of the end user that initiated the attack, this is not enough to link the end user to the state for responsibility to lie under existing customary international law. As such this study was conducted to analyze the issue of malicious cyber-attacks as a matter of customary international law to ascertain mechanism to hold states responsible for malicious cyber-attacks which originate from a state's sovereign territory. Specifically, this study addresses the issue of legal and technical attribution of malicious cyber-attacks for the purposes of holding states responsible for those attacks.

This study argues that under existing customary international law attributing malicious cyber-attacks for the purpose of ascertaining state responsibility is difficult if not impossible. As such, this study proposes alternative theories, which already exist within customary international law, for holding states responsible for malicious cyber-attacks which originate from their sovereign territory. This study addresses alternative theories of state responsibility existing in customary international law such as those put forth in Trail Smelter and Corfu Channel and the theory of strict liability for ultra-hazardous activities. In addition, this study addresses the theory of indirect responsibility, the duty to prevent harm, and due diligence in cyber-space. Lastly this study analysis the impact of the post-9/11 invasion of Afghanistan by the United States and NATO forces and determines that a burgeoning rule of attribution may be present which would impact the attribution of malicious cyber-attacks to states.

This study makes an original and important addition to the corpus of international law by addressing the issues of technical and legal attribution, state responsibility, and the duty to prevent malicious cyber-attacks as a matter of customary international law. This study is needed; malicious cyber-attacks implicate international law, as the majority are interstate in nature. However, international law currently has no paradigm, per se, in place to effectively deal with the issue of malicious cyber-attacks.

Declaration

No part of this thesis has previously been submitted for the award of a degree at the University of Glasgow or at any other University. This thesis is based solely upon the author's research.

Signed: _ 

Statement of Copyright

Contents

> While we now may be coming to the realization that the Cyber Age is a revolution of historic proportions, we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be. The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow. Packingham v. North Carolina, 582 U.S. ____ (2017).

Part I: Initial Matters

Chapter One: Study Introduction

1. Introduction

The history of humanity is dictated by the technology that is available to it. Each successive wave of technological advancement alters humanity; some technological advancement may change little, while other advancements may affect almost every facet of humanity. As technology advances, so too must the law that governs it. When a new technology emerges, the existing law is faced with three alternatives: (1) ignore the advancement and maintain the legal status quo; (2) govern the new technology by analogy; or (3) create new laws that address the changing technology, either through legislation or custom. When the technology is such that it alters almost every aspect of society, the legal paradigms in place must adapt rapidly lest the law itself becomes irrelevant.

The advent of the Internet,[1] the World Wide Web,[2] and associated information technologies (collectively, cyberspace)[3] is one of the technological advancements that have impacted almost every facet of humanity. It is submitted that no previous technological advancement has impacted humanity in such a way as that of the advent of the Internet. The Internet has arguably affected, directly or indirectly, every facet of life for much of humanity, impacting virtually every state and people, some faster than others.

The international legal framework has been slow to adapt to the changes brought by the Internet and the "information society"[4] that has evolved in the Internet's wake. In response to the Internet and the subsequent changes, the international legal order has seemingly embraced all three of the above-posited responses. States and scholars have: (1) ignored the Internet, (2) attempted to regulate the Internet through analogy to older technologies such as the telephone, telegraph, and wire services; and (3) attempted to legislate the Internet via domestic and international legislation.

As with any emerging technology, there are positives and negatives associated with the Internet. If technology may be used to the benefit of humanity, then in most cases, it may

---

1 The Internet is a decentralized global network of connected computer systems linked together through smaller networks to allow for information exchange. The Internet is not solely the World Wide Web ("WWW") … The Internet may be best visualized by thinking of millions of computers interconnected for the purpose of information exchange. Vangie Beal, *Internet*, Webopedia (2014), http://www.webopedia.com/ TERM/I/Internet.html. This study adopts "the usual convention of capitalizing *Internet* when referring specifically to the global Internet, and use a lower case to refer to private internets that use TCP/IP technology." Douglas E. Comer, *Internetworking with TCP/IP, Principles, Protocols and Architecture* 2, n. † (5th ed. 2006).

2 A widely-used multimedia information system on the Internet, whereby documents stored at numerous locations worldwide are cross-referenced using hypertext links, which allow users to search for and access information by moving from one document to another. *World Wide Web*, Oxford English Dictionary (2014), http://www.oed.com/view/Entry/248002?redirectedFrom= world+wide+web#eid.

3 Cyberspace may be understood as "an interactive domain" composed of inter-dependent digital networks "that [are] used to store, modify, and communicate information. [Cyberspace] includes the Internet, but also other information systems." *U.K. Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, Cabinet Office (Nov. 2011).

4 *See*, Nick Moore, *The Information Society* 271-272, *in*, World Information Report 1997-1998, UNESCO, http://www.unesco.org/webworld/wirerpt/wirenglish/chap20.pdf. (Defining an information society as one where "information is used as an economic resource… [where] [p]eople use information more intensively in their activities as consumers: to inform their choices between different products, to explore their entitlements to public services, and to take greater control over their own lives… ")

also be used as a detriment. The Internet is no different: it has benefited and harmed humanity. There is no doubt that the Internet has had a positive impact on society. Unfortunately, the Internet and society's dependence upon it have expanded the reach of traditional crimes, created new mechanisms for exploitation, created new forms of espionage, and allowed for the development of cyber-based weapons.

This collective exploitation of the Internet, commonly referred to by the generic term cyber-attack,[5] is a transnational issue differing in scope and immediacy from any other international issue. Never have entities residing in one state had the ability to impact the territory of another state,[6] irrespective of the state's location, in near-instantaneous time and with potentially drastic results,[7] while leaving the injured state little recourse for holding the responsible party to blame due to technical and legal issues.

Cyber-attacks are a global problem that is proving to be difficult for states to respond to. As will be discussed later in this study, the ability to launch a cyber-attack for criminal, military, espionage, or other malicious or exploitive reasons is due to several issues associated with the advent and growth of the Internet. First, the Internet is a decentralized service which is stateless[8] and has varying levels of government oversight depending upon jurisdiction, but there is no single controlling entity. Second, the Internet has evolved through an ad hoc mechanism driven by business, government use, personal recreation, and crime. Third, disparate information exchange systems have grown together to form a "web" of international connections that allow for the free exchange of information. As will be discussed in Chapter Four, the Internet is an open system that is designed to allow for maximum interoperability with minimal built-in security measures.

---

5 The general term cyber-attack should be understood to encompass all forms of cyber-attacks discussed.

6 The term territory, as used here, implicates both a state's virtual (cyber) territory and its physical territory.

7 Drastic in terms of monetary harm done by such attacks. As discussed later in this chapter, cyber-attacks result in potentially billions of dollars in damages per year.

8 Karanpreet Singh, Paramvir Singh, and Krishan Kumar, *A Systematic Review of IP Traceback Schemes for Denial of Service Attacks*, 56 Computer & Security 111, 111 (2016). ("The stateless nature of [the] Internet makes it nearly impractical to identify the true origin of attack…")

Moreover, the Internet is an anonymous system with no true mechanism built-in to identify end users. Anonymity is an important and driving element of many aspects of the Internet. The anonymity of the end user is an important feature that must be balanced against the prevention of cyber-attacks. The Internet has played an important role in protecting free speech and the free exchange of information, much of which depends upon the anonymity of the Internet. As such, the anonymity inherent to the Internet must be maintained.

Complicating this issue is that the Internet, in its current iteration, is operating on software specifications that were neither intended nor designed to handle either secure transactions or the vast amount of information for which the Internet is now responsible.

Cyber-attacks engage all levels of society and present unique challenges to international peace and security despite traditionally being viewed as each individual state's problem (that is, cyber-attacks of all types have been left to each state to deal with through that state's own internal law enforcement and judicial systems, irrespective of the jurisdictional issues regarding perpetrators and the inability to properly attribute cyber-attacks at the individual level). Cyber-attacks arguably degrade the peace and security of the international order as they impact a wide variety of domestic infrastructure, government agencies, and military readiness in individual states. Cyber-attacks are directed at all levels of government and commerce, which, this study believes, will inevitably lead to a further escalation with a high probability of kinetic overlap.[9]

Every state has been subjected to cyber-attacks in one form or another. Each state has responded to cyber-attacks through different mechanisms. Some states treat cyber-attacks as a criminal matter and subject the perpetrators to criminal prosecution. Some states have levied sanctions against the state they believe responsible, while other states have attempted to reverse hack the apparent perpetrators of a cyber-attack. Cyber-attacks are an international legal problem affecting all states within the international order, a problem that is growing exponentially with "a new strain of malware appear[ing] faster than one [every]

9 Kinetic overlap, as used herein, refers to the use of physical military force as opposed to digital force, which only applies to cyberspace.

second…"[10] The constant growth and change in cyber-attacks have overwhelmed states and individuals attempting to protect the Internet, and it has seemingly overwhelmed the international legal order attempting to find a means of dealing with this problem.

Most cyber-attacks are launched for exploitative or malicious reasons, with attacks directed at all the disparate actors within a state: the more dependent a state is on the Internet, the more likely the state will be attacked via the Internet. If an actor in cyberspace (this study will use both cyberspace and the Internet interchangeably as they represent the same basic idea) may benefit or profit from attacking another entity in cyberspace, it is almost certain that it will be attacked. As cyber-attacks continue, the likelihood of kinetic spillover also grows; i.e., a state may respond to cyber-attacks by utilizing conventional military force, either to prevent cyber-attacks originating from another state or to punish another state for allowing its cyber territory to be used for cyber-attacks.

Another motivating factor for cyber-attacks is that the Internet is the key mechanism for states to engage in espionage[11] and state-sponsored crime for a state's benefit. It is well known that states actively engage in cyber-espionage and surveillance on both friend and foe alike. Also, many states may engage in cyber-attacks or maintain willful ignorance of these acts perpetrated by their citizens to either directly or indirectly derive a technical or monetary benefit from allowing cyber-attacks to be launched from their cyber infrastructure. For instance, some states have been accused of being havens for cybercrime, as they derive financial benefit from cyber-related criminal acts.[12] The cyber security

---

10 Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* *548 (Kindle ed. 2011).

11 Espionage, as used herein, means both national security espionage and industrial/economic espionage conducted via cyberspace. *See also*, Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 Fletcher Sec. Rev. 55 (Spring 2014).

12 *See, e.g.*, Press Release, Hon. Mark Kirk, *Kirk, Warner to Introduce Cybersecurity Amendment to Ukrainian Aid Bill on Monday* (Mar 23, 2014), http://www.kirk.senate.gov /?p=press_release&id=1033. ("Internet security experts tell us Ukraine is home to some of the world's most sophisticated cyber criminals, and the previous Ukrainian government routinely turned a blind eye to cybercrime…")

company, McAfee,[13] estimates that cyber-crime[14] and espionage cost businesses and governments an estimated $400 billion per year in losses.[15] If cyber criminals make a return on their activities of 25%, then cyber-crime injects $100 billion into economies worldwide. This economic influx is an incentive for many states to ignore cyber activities that do not directly harm the host state.

States may actively engage in cyber-crime and espionage to directly benefit themselves. Mandiant, a U.S. cybersecurity consulting company, has released a report[16] alleging wide-scale espionage and theft by or on behalf of the Chinese government. In its *APT1* report, Mandiant alleged that China operates specialized military units tasked with engaging in espionage and stealing proprietary information from civilian and state organizations in countries located outside of China.[17] It also alleged that China has engaged in this conduct to derive strategic benefit for China's domestic industries and military. It is argued that China is not alone in taking such actions, but that most states engage in such behavior at varying levels. It is also argued that cyber-espionage poses a threat to international peace and security, as the potential for a state to respond to cyber-espionage through kinetic means is high.

State and non-state actors may also create weaponized packages of computer code that utilize the Internet as a vector of attack. Weaponized computer code may create situations where physical damage results: the weaponized computer code may intrude on computer systems that control physical elements, such as pumps or valves or other processes. Alternatively, the weaponized code may strictly impact data stored within a computer

13 McAfee, *Net Losses: Estimating the Global Cost of Cybercrime* 2 (June 2014), http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf.

14 There is no set style for the use of the prefix of "cyber" e.g., cybercrime, cyber-crime, or cyber crime.

15 McAfee, *Net Losses: Estimating the Global Cost of Cybercrime* 2 (June 2014), http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf.

16 Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, (Feb. 2013), http://intelreport. mandiant. com/Mandiant_APT1_Report.pdf.

17 *Id.* at 20-26.

system. The primary example of the former is the Stuxnet worm,[18] reportedly a joint United States-Israel program which has been blamed for the destruction of Iranian nuclear centrifuges, thus confirming the fear that states may utilize weaponized computer code, which then poses a real-world kinetic threat. This fear of weaponized code, more commonly referred to as cyber weapons, has resulted in a large amount of scholarship concerning the legality and international legal issues associated in *jus in bello* and *jus ad bellum.*

The attention paid to the issue of cyber-warfare is such that most legal scholarship focuses solely on the issue of cyber weapons and cyber-warfare in the context of United Nations Charter Art. 2(4) (use of force violations) and Art. 51 (right to self-defense by states). The focus of the scholarship on cyber-warfare and associated cyber-attacks has created a situation where other forms of cyber-attacks, such as the malicious cyber-attacks discussed herein, are overshadowed and seemingly pushed to the side. The irony of this is that the clear majority of cyber-attacks occurring at present are malicious in nature, and very few could be classified as cyber-attacks related to cyber warfare.[19] The result is a mass of legal scholarship that has created confusion as to what legal paradigms control cyber-attacks, irrespective of source and objective intent of the actors propagating the cyber-attacks. This problem is compounded by the media and many commentators as they fail to differentiate between cyber-attacks that are intended for malicious purposes and cyber-attacks that are intended as cyber weapons and cyber warfare; they mistakenly classify both under the general term of "cyber-attacks." Compounding the problem is the fact that it is difficult to differentiate between the different types of attacks, as they may call for subjective interpretation.

Adding to the confusion regarding the differentiation of cyber-attacks is the fact that computer code written for malicious or exploitive purposes may also serve as a platform for cyber weapons and vice versa. In addition, states may not, per se, be the best

---

18 Stuxnet did not utilize the Internet for propagation purposes, per se; it was reported that it was initially uploaded via a contaminated USB drive or similar device that then was propagated through either an intranet or contaminated hardware. *See*, Greg Keizer, *Why Did the Stuxnet Worm Spread?*, ComputerWorld, (Oct. 1, 2010), http://www.computerworld.com/article/2516109/security0/why-did-stuxnet-worm-spread-.html.

19 *See e.g.*, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, R.11, n. 1-11 (Michael N. Schmitt ed. 2013). (Explaining how force in cyber-attacks may be defined and analyzed.)

promulgators of cyber-attacks and cyber weapons because many non-state actors possess the knowledge and skill to launch cyber-attacks (in either form) on par with or exceeding that of the state, adding to the general confusion and panic surrounding the issue.[20]

This confusion regarding the blurring of the lines between state and non-state actors in cyberspace is just one issue in the overall problem of cyber-attacks. There is a multitude of technical and legal challenges posed by malicious cyber-attacks. This study is presented to focus on one area of challenge within the greater problem. Specifically, the issue of state responsibility and attribution of malicious cyber-attacks. Simply put, this study addresses the problem of how to hold states responsible for cyber-attacks that are traced to the attacking state's cyber-territory, and how such attacks may be attributed to a state. This is a challenging question as there are no concrete and definitive means of linking cyber-attacks which originate from a state's cyber-territory to the state itself for the purpose of attribution and for holding the state responsible for the attack. Computer science has a difficult time tracing cyber-attacks to the computer system or systems responsible for launching a cyber-attack, and there are no means to "jump the air gap" and link the computer system used in the cyber-attack to an actual, identifiable, individual for the purposes of ascertaining whether the individual actor was acting on behalf of a state.

1.1. Structure of Argument

This study focuses on the issue of malicious cyber-attacks as a matter of customary international law (CIL) with a specific focus on the work of the International Law Commission (ILC) and the general principles put forth in the ILC's *Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARS)*. This study addresses the issues relating to attribution and state responsibility for malicious cyber-attacks; alternative

20 *See e.g.*, Mark Bowden, *Worm: The First Digital War* 122-124 (2013). (Discussing issues surrounding the conficker variant worm [malware] that is largely believed to have been written by either Russian or Ukrainian hackers. Bowden related that the authors of the worm were on par or better than most of those attempting to stop the worm. In one incident, Bowden related that at one point, researchers discovered a variant of the conficker worm that was utilizing a 4096-bit key to encrypt its communications; prior to that discovery, 4096-bit encryption had only been theoretical and was four times greater than the standard encryption protocols called for by the United States Federal Information Processing Standards at the time. Bowden believes that only a handful of individuals in the world would have been able to understand and utilize the encryption.)

theories for holding states responsible for cyber-attacks when technical and legal attribution fail; and the duty of states to prevent malicious cyber-attacks as a matter of CIL. As such, this study does not address other issues related to state responsibility, nor does it engage in an in-depth discussion regarding the ILC's ARS except where the questions intersect.

This study utilizes CIL and the ILC's ARS for the purposes of analysis and discussion for multiple reasons. The first is that there is a scarcity of treaty law on the instant issue, making it is necessary to focus on CIL, as international law principles control cyberspace.[21] Second, CIL is ideally suited to deal with the instant issue, as the issue is relatively new and evolving rapidly. Thus, state practices are evolving as the issue advances, and it is state practice which is partly responsible for the formation of CIL. Third, CIL is based on hundreds of years of evolution, and while CIL may not have addressed the issue on point previously, the body of CIL is deep enough to allow for guidance by analogy. That is, CIL has addressed issues that are similar enough in theory to guide the discussion and application of CIL by analogy to the instant issue. Lastly, state responsibility (as discussed in Chapter Two) is a product of CIL. The legal principles applicable for attributing a cyber-attack to the state and holding the state responsible for that attack are products of CIL. The law of state responsibility has been for a large part codified by the ILC in its ARS (it is recognized that portions of the ARS have been subject to much scholarly debate and have not been accepted by many scholars as reflecting CIL. However, the ILC's codification of the rules of state responsibility and the rules of attribution found in Chapters One and Two of the ARS are commonly recognized as the least controversial and most accepted aspects of the ARS enjoying almost universal acceptance.) This study utilizes the ARS as it is recognized as the baseline for state responsibility and is based on over 50 years of work by some of the

---

21 Harold H. Koh, Legal Advisor, U.S. Department of State, Address to the United States Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012). As prepared: https://www.state.gov/s/l/releases/remarks/197924.htm. ("[I]nternational law principles do apply in cyberspace… the United States has made clear our view that established principles of international law do apply in cyberspace.") *See also*, Andreas Zimmermann, *International Law and 'Cyber Space'*, 3 Eur. Soc. Int'l L. Reflection *1-6 (Jan. 10, 2014). http://www.esilsedi.eu/sites/default/files/ESIL%20Reflections%20-%20Andreas%20 Zimmermann_ 0.pdf. ("[A]ctivities in 'cyber space' … are governed by international law as such, and be it only by the norm that where no (general or specific) rule prohibiting the in question exists, states retain their freedom to act. However… it is for lack, for the time being, of more specific rules, that the basic and general norms of international law govern cyber activities, including concepts such as jurisdiction or attribution."). Gary Brown and Keira Poellet, *The Customary International Law of Cyberspace*, Strategic Studies Quarterly 126 (Fall 2012). ("[C]ustomary international law occupies a position of preeminence in developing areas of the law…")

greatest legal minds in international law. It has been accepted by the ICJ and lesser tribunals as the *de facto* rules of international law for state responsibility. The ARS is utilized herein as a baseline for issues relating to attribution and state responsibility.

This study holds that the ILC's ARS is not a perfect fit when applied to the issue of cyber-attacks and state responsibility. This imperfect fit of the ARS is due, in part, to the fact that (a) the ARS is based on pre-cyber age customs for attribution and state responsibility, (b) the inability of technical attribution techniques to affirmatively link a state to a malicious act in cyberspace by direct evidence, (c) the inability of technical attribution to "bridge the air gap" between computer and individual user,[22] and (d) the reliance by the ARS on the "effective control test" elucidated by the ICJ in *Nicaragua* and reaffirmed by the *Bosnian genocide* case to link the acts on non-state actors to the state. As such, this study hypothesizes that alternative theories of state responsibility, which exist in CIL already, are better suited for allowing those states injured by cyber-attacks to hold responsible those states in which the malicious cyber-attacks originate. In addition, this study argues that states are bound under CIL to prevent and use due diligence in their efforts to prevent malicious cyber-attacks from originating from within a state's sovereign territory.

This study is tailored to the specific issues put forth *supra,* utilizing doctrinal legal research methods with a side of pragmatism.[23] This study has been undertaken to address a void that currently exists within international legal scholarship relating to state responsibility regarding malicious cyber-attacks. This study adopts and utilizes what Allen and Engholm call, "plain language legal drafting" [24] to the greatest extent possible. While this study

22 "Bridging the air gap" is the affirmative identification of the end user on a given computer system responsible for initiating a cyber-attack or responsible for drafting the computer code responsible for an attack. While technical attribution may in limited cases identify the IP address used to initiate an attack, affirmatively identifying the computer used for the attack is even more doubtful, and identifying the user of that computer is virtually impossible to meet the legal standard necessary for attribution under the ARS.

23 Richard A. Posner, *Law, Pragmatism, and Democracy* 25-56 (2003). (As used herein, pragmatism relates to the idea of "everyday pragmatism" as put forth by Posner rather than the legal philosophy of pragmatism.)

24 Laymen E. Allen & C. Rudy Engholm, *The Need for Clear Structure in "Plain Language" Legal Drafting*, 13 U. Mich. J. L. Reform 455 (1980). *Cf.,* Learned Hand, *Is There a Common Will*, 28 Mich. L. Rev. 46, 52 (1929). ("The language of the law must not be foreign to the ears of those who are to obey it.")

utilizes legal terms of art, the structure and drafting of this study is meant to make it accessible to legal scholars of disparate backgrounds.

This study utilizes computer science literature and theory to demonstrate the technical issues affecting cyber-attack attribution. This study utilizes current computer science theory to demonstrate how existing legal theory regarding cyber-attack attribution does not work when considering current computer science abilities.[25] This study will discuss technical attribution in Chapter Four to demonstrate the practical difficulties involved with technical attribution of any cyber-attack. This study will demonstrate that a state may not be held responsible under the existing laws of state responsibility without direct attribution to the state via technical attribution. This study argues that legal theory alone is not enough without the pragmatic guidance of computer science, and as such, a basic understanding of the Internet and attack attribution is necessary prompting, thus necessitating an in-depth discussion on the issue.

This study is one of only a few studies available that address the issue of cyber-attack attribution while understanding and discussing the practical issues associated with the technical problems surrounding cyber-attack attribution in computer science. It is argued by this study that one of the greatest strengths of this study is the fact that it takes into consideration the pragmatic issues related to cyber-attack attribution and addresses the legal issues in harmony with computer science to construct legal solutions for the kinetic world.

1.2. Preliminary Matters

Before discussing substantive matters, this study will discuss and establish a baseline understanding concerning the key terms that it covers. An effective information exchange (that is, the sharing of knowledge and ideas between disparate parties) operates best when

---

[25] *See,* Allan Cook, et al., *Attribution of Cyber Attacks on Industrial Control Systems*, ICST Transactions (Preprint, 2017), https://www.researchgate.net/profile /Leandros_ Maglaras/ publication /293811556_Attribution_of_Cyber_Attacks_on_Industrial_Control_Systems/links/56bc70dd08aebaa770e863de.pdf. ("[I]t is perhaps more practical to focus on deterrence rather than prosecution. Libicki, discussing cyberattacks in the context of cyberwarfare, argued "cyberattacks can be launched from literally anywhere, including cybercafés, open WiFi nodes, and suborned third-party computers. They do not require rare or expensive machinery. They leave no physical trace. Thus, attribution is often guesswork…")

all parties understand the basic operation and terminology of the study. Therefore, a brief discussion regarding key terms utilized herein is presented.

The initial matter is defining what is meant by the term cyber-attack as used in this study. The second issue is to discuss who the primary actors are that may be responsible for malicious cyber-attacks. The third is to establish the differences between cyber-attacks and malicious cyber-attacks.

1.2.1. Defining Cyber-Attacks

A baseline understanding of what a cyber-attack is and how a cyber-attack is defined must be set out before any in-depth discussion on the issue. The challenge, however, is that there is no consensus as to what constitutes nor how to define a cyber-attack. Due to the relative newness of the Internet, the disparate parties involved, and misuse of the terms by different sources, definitional conflicts regarding the subject of cyber-attacks abound. This issue is exacerbated by the usage of the term cyber-attack by states, commentators, and media sources without a shared understanding of the term.[26] To narrow the scope of this study, this study adopts and utilizes the term malicious cyber-attack to refer to the types of attacks covered by this study. However, as this inevitably creates misunderstandings, this study will briefly address the definition and usage of the term cyber-attack to enhance the information exchange within this study.

1.2.2. Cyber-Attacks as a Specialized Term in International Law

The generic term cyber-attack is a legal misnomer. The term "attack" in international law is a specialized term with specific meanings and application in both *jus in bello* and *jus ad bellum*.[27] Schmitt posits that the term attack in international law refers to any use of force

---

26 *See e.g.*, Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, *in* 4th International Conference on Cyber Conflict 283, 284 (C. Czosseck, R. Ottis & K. Ziolkowki eds. 2012). (Schmitt splits the groups into two separate categories of "legal and non-legal communities.")

27 *Id.* at 285-293.

that is such to meet the UN Charter Art. 51 baseline of an "armed attack" or, as in international humanitarian law (IHL), "a distinct category of military operations."[28] IHL defines an attack as "acts of violence against the adversary, whether in offense or defense."[29] Thus, a proper understanding of a cyber-attack would be an act of violence utilizing cyberinfrastructure, where the violence meets the minimum requirement of an armed attack as defined by the ICJ in *Nicaragua.*[30]

There is also a distinction between an attack and an armed attack that is important to understand. Any malicious act against a state that does not rise to the level of U.N. Charter Art. 2(4), force or implicate the right to, U.N. Charter Art. 51, self-defense may be an attack, but it is not an armed attack even though it may violate international law. An armed attack[31] almost always implicates both the use of force *and* the right to self-defense under charter law. The distinction between the two types of attacks may be blurred; the ICJ held that to differentiate between the types of attacks, one must look to the "scale and effect"[32] of the attack. It is necessary to distinguish an armed attack, which implicates the right to self-defense, from a malicious act, which does not implicate the right to use force in self-defense. The ICJ does not clarify where the difference lies; thus it is up to states and CIL to determine what is or is not an armed attack.

As Zemanek explains:

> the thrust of the Court's thinking [on determining an armed attack] is clear: an isolated minor incident which, by the manner in which it takes place, cannot be mistaken for a threat to the safety of the state would not qualify as an armed attack under Art. 51 UN Charter.[33]

---

28 *Id*. n. 24.

29 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) Art. 49, para. 1 (June 8, 1977). Schmitt, *id.* n.28.

30 *See*, Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. US), 1986 I.C.J. 4, 93-95 (June 27).

31 *Id*. at ¶ 195. *See also*, Karl Zemanek, *Armed Attack*, in, Max Planck Encyclopedia of Public International Law (Oct. 2013).

32 *Nicaragua*, *id*.

33 Karl Zemanek, *Armed Attack*, *in*, Max Planck Encyclopedia of Public International Law (Oct. 2013).

However, as Zemanek points out:

> [t]hat law [as put forth by the ICJ in *Nicaragua*] may not be the same today. The cardinal point in the Court's reasoning was the emphasis on the customary nature of the applicable international law, and custom is a dynamic body subject to modification by a change of *opinio iuris* confirmed by corresponding State practice. To determine the law as it now stands, therefore, requires a review of its application during the last decades and its possible development in that process.[34]

Hence, the evaluation of determining whether an attack rises to the level of an armed attack, particularly in the light of technological advancements since *Nicaragua* (and similar ICJ cases), must be undertaken in consideration of both the ICJ holdings on the matter and any evolving custom. This study discusses cyber-attacks, a topic which the ICJ has not addressed, and a type of attack not necessarily envisioned in any recent ICJ decisions. However, this study deals exclusively with those cyber-attacks that do not rise to the level of armed force by either the ICJ or CIL standard.

The term cyber-attack has been applied to a multitude of different computer network and Internet-based actions that range from simple computer intrusion (hacking) to traditional crimes carried out via computer systems such as fraud, theft, espionage, and pornography. The term cyber-attack may also relate to interference with the Internet and with computer networks, such as denial-of-service attacks of various scales. Cyber-attacks may also refer to those computer or network-based attacks that inflict kinetic damage upon a target. As such, the term cyber-attack has become a catch-all phrase for any wrongful act carried out via the Internet or cyberspace.

This issue is compounded by the different terms utilized to describe vectors of attack for cyber-attacks, and for attacks that do not utilize the Internet as a vector but impact electronic or digital infrastructure. All these attacks are still generally referred to as cyber-attacks. Such attacks as Trojans, worms, viruses, phishing, etc. are referred to as a type of cyber-attack even though the vector of attack does not necessitate the use of the Internet.[35]

---

34 *Id.*

35 Different states posit numerous definitions for cyber-attacks, which confuses the issue. For instance, the United States Department of Defense defines a cyber-attack as:

At its simplest, a cyber-attack may be understood to mean any action taken by one party to the detriment of another, which involves computer code created as a tool to inflict harm, irrespective of the vector used in the attack. The primary focus of such attacks will be other systems which rely on computers and computer code to work. However, the harm inflicted by such attacks is not limited to any single sphere (e.g., the digital sphere or physical sphere), and the effects of such attacks may extend out to impact other interconnected spheres. The harm done by the computer code is not restricted to the direct effect of the computer code, but it may also include the "knock-on" effects of the computer code, irrespective of the intent of the individual who wrote the code. The harm may be digital, physical, monetary, psychological, etc., but the harm must relate back to the use of the computer code to inflict the original harm.

Cyber-attacks may also be militarized attacks where a state or non-state actor creates computer code with the intent to do digital or physical harm to a group or state. The difference is that in militarized cyber-attacks, the computer code takes the place of a kinetic (physical) weapon and acts in a similar manner and the attack results in a similar effect as that of a traditional kinetic weapon. This idea will be discussed in-depth in the next section.

There is an extensive crossover between the types of cyber-attacks and the code used for each attack that may be the same or similar to that used in a completely different attack. This makes defining cyber-attacks or even grouping similar attacks difficult, as there is an immense crossover between the attack vector, attack type, cyber payload, and authorship. To clarify this issue and to allow for a broader understanding of cyber-attacks and the legal issues surrounding them, this study will utilize the term, malicious cyber-attack to reflect those types of cyber-attacks that fall within the purview of this study.

> [a] hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The Intended effect of cyber-attacks are not necessarily limited to the targeted computer systems or data themselves… A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code or human operators…

Joint Chiefs of Staff, *Joint Terminology for Cyberspace Operations, attch. I, Cyberspace Operations Lexicon*, Department of Defense (2009).

This study adopts the prefix malicious[36] to separate out those cyber-attacks which are initiated to do harm to another state or non-state actor, but which do not necessarily rise to the level of force as discussed *infra*. Malicious cyber-attacks are those attacks which are (1) initiated for the sole purpose of inflicting harm upon the target where the harm is less than that of an armed attack, (2) those attacks that are intended to be utilized for traditional crimes such as theft, fraud, blackmail, etc., and/or (3) espionage when the harm inflicted does not rise to the level of U.N. Charter Art. 2(4)/Art. 51 force. The generic term cyber-attack will refer to the militarized attacks by specifically-designed computer code that rises to the level of Art. 2(4)/Art. 51 force as this definition is most in line with the majority of literature.

1.2.3. The Use of Force Dichotomy for Defining Cyber-Attacks

It should be understood that the term malicious cyber-attack refers to any use of the Internet that is exploitive, criminal, or wrongful, including both economic and military espionage, or any attack that does not meet the definition of the use of force/armed attack as discussed *infra* or as evaluated by the Schmitt criteria and *Tallinn Manual*,[37] nor does it have a kinetic effect[38] as the result of the cyber-attack.

The posited definition only addresses the objective measure of the attack and not the subjective intent of the cyber-attack authors. If the attack authors intended to promulgate a kinetic cyber-attack, but the result is the loss of computer information and not the actual hardware, and there is no kinetic impact, the cyber-attack would be regarded as a malicious

---

36 As used herein, malicious is defined as "[s]ubstantially certain to cause injury… [and] without just cause or excuse." *Black's Law Dictionary* 1043 (2011).

37 *See,* Michael N. Schmitt, *Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Columbia J. of Transnat'l L. 885, 914 (1999). (Setting eight "factors" to be utilized in determining whether a cyber-attack rises to the level of prohibited force. These Factors are "Severity… Immediacy… Directness… Invasiveness… Measurability of effects… Military character… State Involvement… Presumptive legality…") *See also, Tallinn Manual on the International Law Applicable to Cyber Warfare* R. 11, cmt. 9a-h, (Michael N. Schmitt ed., 2013).

38 *See, Tallinn Manual on the International Law Applicable to Cyber Warfare* R. 11 (Michael N. Schmitt ed., 2013).

cyber-attack. However, if the attackers only wanted to conduct a traditional cyber theft or other similar hacks which then resulted in physical loss or damage, the attack would be a cyber-attack and not subject to this study. Simply put, the test is based upon the direct effect of the cyber-attack.

This study, however, does not differentiate between the types and purposes of a cyber-attack for definitional purposes. Irrespective of whether the cyber-attack is for theft, disruption, espionage, or any purpose less than the use of force, those attacks would be considered malicious cyber-attacks. As such, there is no need to differentiate attack vectors and the purpose behind the malicious cyber-attack as all malicious use of cyberspace may fall within the theories posited herein. As long as the malicious cyber-attack may be viewed as an internationally wrongful act, as discussed *infra*, said attacks would fall within the purview of this study. It is recognized that there may be cases where cyber-attacks may be a mixture of both. Those cases at present are rare, with attacks such as Stuxnet, Duqu, Flame, Mask/Careto, and the Regin variant known as of writing. In instances like this, the *jus in bello*/*jus ad bellum* paradigms control since such attacks are analogous to the customary use of force and espionage seen in traditional kinetic attacks/use of force events.

This study, therefore, concerns those attacks that are less than the use of force irrespective of the intent/mens rea of the attacker. This study solely focuses on the end results of the cyber-attack. This study does not ignore the use of force/U.N. Charter Art. 2(4) paradigm which is utilized to illustrate different theories relating to issues of proof and state responsibility. However, this study focuses on those attacks that are malicious in nature and do not rise to the level of prohibited force.

1.3. The Attacks: A Brief Discussion on the Cyber-Attacks on Georgia, Estonia, the Stuxnet Cyber-Attack on Iran, and the Sony Hack.

This study refers to multiple cyber-attacks for illustrative and reference purposes. The main attacks discussed within this study are the Distributed Denial of Service (DDoS)[39] attacks on Estonia (2007) and Georgia (2008); the Stuxnet (and its variants) attack on Iran (2012); and the Sony Hack (2014). These attacks are a very small sample of the multitude of cyber-attacks occurring daily. These attacks were selected to illustrate the types of attacks that are occurring, e.g., DDoS attacks for political purposes, cyber-attacks as adjuncts to kinetic attacks, cyber-espionage, and cyber-crime. These cyber-attacks also illustrate the difficulties of technical and legal attribution of malicious cyber-attacks.

1.3.1. Estonia and Georgia

The Estonia and Georgia attacks involved massive DDoS attacks directed at civilian and government infrastructure and other online services. Both attacks were blamed on Russia by the respective injured states, yet neither attack was ever legally attributed to a state, nor has any state been held responsible for the attacks.

1.3.1.1. Estonia

In 2007, Estonia was one of the most "wired" states on earth.[40] Almost every facet of Estonia's government and commerce relied upon the Internet and cyberspace, making

39 Christos Douligeris and Aikaterini Mitrokotsa, *DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art*, 44 Computer Networks 643, 643-644 (2004). ("[A] DoS [Denial of Service] attack can be described as an attack designed to render a computer or network incapable of providing normal services. A DoS attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user. These attacks don't necessarily damage data directly or permanently, but they intentionally compromise the availability of resources…")

40 Associated Press, *A Look at Estonia's Cyber Attack in 2007*, NBC News (http://www.nbcnews.com/id/ 31801246/ ns/technology_and_science-security/t/look-estonias-cyber-attack/#. V2BUFjZdE2x). *See also*, Andreas Schmidt, *The Estonian Cyber Attacks* 174-193, *in*, A Fierce Domain: Conflict in Cyberspace, 1986-2012 (Jason Healey ed., 2013). Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*,

Estonia particularly susceptible to malicious cyber-attacks. Estonia is a former Soviet Satellite State, which has a large Russian ethnic minority. The post-Soviet Estonia of 2007 was ideologically different and opposed to the government in post-Soviet Russia, causing tension between the states. This tension was exacerbated when Estonia joined NATO in 2004, and was further fueled by Estonia's actions to rid itself of reminders of the Soviet era, such as the removal of Russian world war two memorials, and move closer to the West in terms of its ideology and association with NATO.[41]

The tension between Estonia and Russia hit a critical point in January 2007, when "the Estonian government announced that it would move a World War II monument from the center of Tallinn to a military cemetery on the outskirts of the city." [42] The removal of the statue was opposed by ethnic Russian-Estonians and by the state of Russia, both of whom perceived the move as an attack on the memory of Soviet soldiers of World War II. The issue culminated when, bowing to internal domestic politics, the Estonian government moved the statue on April 26, 2007.[43]

The very next day, Estonia was subjected to large-scale cyber-attacks that included DDoS attacks[44], e-mail spam and phishing attacks, and website defacement. The attacks were directed at government websites, banking systems, media systems, and communication systems.[45] These initial cyber-attacks continued until April 30, 2007, however, after this, the cyber-attacks became more focused and coordinated. The post-April 30 cyber-attacks consisted mainly of DDoS attacks against critical Estonian infrastructure, utilizing

4 J. Strategic Sec. 49-60 (2011). William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, 5-13 (2009).

41 *Id.*

42. Nate Anderson, *Massive DDOS Attacks Target Estonia; Russia Accused*, ARS Technica (May 14, 2007), http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/. *See also*, Kara Flook, *Russia and the Cyber Threat*, AEI (May 13, 2009), http://www.criticalthreats.org/russia/russia-and-cyber-threat.

43 *Id.*

44 *Id.* at n.43

45 Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

botnets[46] to facilitate large-scale DDoS attacks. The attacks carried on through until May 18, 2007.[47] Estonia claimed that the cyber-attacks had been traced to IP addresses in Russia.[48] The attacks were also traced to infected botnets around the world.[49]

The cyber-attacks against Estonia varied in sophistication from basic hacking of websites, email spam, and phishing attacks, to sophisticated DDoS attacks utilizing botnets consisting of thousands of zombie computers.[50] The attacks focused on government systems, banking systems, and news providers. The attacks did not, per se, cause any kinetic damage, but did result in the loss of millions of dollars to the government and other industries.

The attacks were never legally attributed to Russia or any other state. Although Estonia has publicly blamed Russia for the attack, Russia, in turn, has blamed the attacks on overzealous patriot hackers and has denied any official government involvement.[51] The

---

46 A "botnet" is "a network of private computers infected with malicious software and controlled as a group without the owners' knowledge… or to be utilized in DDoS attacks by sending requests for services to a server. Oxford Dictionaries (2016), https://en.oxforddictionaries .com/definition/botnet.

47 There is some discrepancy in the literature on when the attacks against Estonia ceased. Ashmore puts the date that the attacks ended as May 9, 2007. Schmidt, however, demonstrates that the cyber-attacks lasted until May 18, 2007.

48 Nate Anderson, *Massive DDOS Attacks Target Estonia; Russia Accused*, ARS Technica (May 14, 2007), http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/. *See also*, Kara Flook, *Russia and the Cyber Threat*, AEI (May 13, 2009), http://www.criticalthreats.org/russia/russia-and-cyber-threat. ("The Russian government has denied all culpability, pointing out that though the attacks can be traced to Russia, they cannot be traced to government agents or computers.")

49 Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

50 *Id., See also*, Kelly Burton, *The Conficker Worm* (n.d.), https://www.sans.org/security-resources/malwarefaq/conficker-worm.php. National Public Radio, *The Worm That Could Bring Down the Internet* (Sep. 27, 2011), http://www.npr.org/2011/09/27/140704494/the-worm-that-could-bring-down-the-internet. *See also*, Schmidt, *supra*, n.40.

51 Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 J. Strategic Sec. 49-60 (2011). *See also*, Jason Healey, *Concluding Remarks*, 265-278 *in*, A Fierce Domain: Conflicts in Cyberspace, 1986 -2012 (Jason Healey ed., 2013). (Discussing the circumstantial attribution of malicious cyber-attacks and discussing the Estonia attacks as an example.)

cyber-attacks on Estonia gave rise to the new phenomena in cyberspace: that of the patriot hacker/state-proxy who conducted cyber-attacks on behalf of their championed state with or without the state's support or permission. The cyber-attacks on Estonia also demonstrated the effects of cyber-attacks on advanced societies and the dangers thereto. They demonstrated the problems inherent with the attribution of conduct via cyberspace and the inability to hold states responsible for acts originating from their sovereign territories in cyberspace.

1.3.1.2. Georgia

The Republic of Georgia gained its independence from the Soviet Union in 1991 and, like Estonia moved to distance itself from its Soviet past and Russia. Georgia was one of the first former Soviet republics to attempt to join NATO.[52] Like Estonia, Georgia had a troubled relationship with Russia. But unlike Estonia, Georgia was in an ongoing dispute with Russia over control of the semi-autonomous regions of South Ossetia and Abkhazia. This dispute turned kinetic in August 2008 when Georgian forces were ejected by Russia from both South Ossetia and Abkhazia.[53] The kinetic attacks by Russia were preceded by large-scale cyber-attacks against the Georgian government and civilian infrastructure.

These cyber-attacks against Georgia are the first reported cases of cyber-attacks being utilized prior to and concurrently with a kinetic conflict.[54] The cyber-attacks were used as an adjunct to the kinetic attacks to degrade Georgian communications systems and prevent command and control coordination by Georgian military forces.[55] In addition, these attacks were "designed to control the flow of information or influence people's perception

---

52 *See*, North Atlantic Treaty Organization, *Relations with Georgia* (June 7, 2016), http://www.nato.int/cps/en/natolive/topics_38988.htm. (As of this writing, Georgia has not become a full member of NATO, yet remains active in NATO missions.)

53 Andreas Hagen, *The Russo-Georgian War 2008, in*, A Fierce Domain: Conflict in Cyberspace, 1986-2012, 194-196 (Jason Healey ed., 2013). British Broadcasting Corp., *Georgia Profile – Timeline*, (December 24, 2014), http://www.bbc.com/ news/world-europe-17303471.

54 Hagen, *id*. David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars J. (2011).

55 *Id*.

regarding the conflict between Georgia and Russia. They were also part of information exfiltration activities that were designed to steal and accumulate military and political intelligence from Georgian networks."[56] The cyber-attacks, which started roughly three weeks before ground operations by Russia, consisted mainly of the same type of attacks as seen in the Estonian cyber-attacks of 2007.

While the cyber-attacks against Georgia began at least three weeks before the military operations by Russia, the frequency and sophistication of the cyber-attacks grew concurrently with the kinetic attack by Russia.[57] The cyber-attacks were better coordinated than the 2007 Estonia attacks: target lists, attack tools, and instructions were published on Russian language websites and message boards available to any Russian-speaking person.[58]

The cyber-attacks against Georgia, like those against Estonia, were never legally attributed, and no state was ever held responsible. However, many security experts linked the attacks to Russian IP addresses, and the attacks have been circumstantially attributed to Russia.[59] Russia denied any involvement in or control over the cyber-attacks, again claiming that overzealous patriot hackers and assorted hacking collectives were responsible. The timing, coordination, and sophistication of the attacks would militate against the claims by the Russian government. However, under the CIL of state responsibility, without a showing of effective control by the Russian government or agents thereof, Russia could not be held responsible.

The cyber-attacks against Georgia demonstrated a new threat: cyber-attacks could be used as a tool in kinetic conflicts and during times of peace. The cyber-attacks against Georgia,

---

56 Andreas Hagen, *The Russo-Georgian War 2008*, *in*, A Fierce Domain: Conflict in Cyberspace, 1986-2012, 196 (Jason Healey ed., 2013).

57 Hagen *id*. at 197. David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars J. (2011), William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, 11 (2009).

58 Hagan, *id*. at n. 59.

59 *Id. See also*, Jason Healey, *Concluding Remarks*, 265-278, *in*, A Fierce Domain: Conflicts in Cyberspace, 1986 -2012 (Jason Healey ed., 2013).

like the Estonian attacks, demonstrated the difficulties involved with issues of attribution and state responsibility. Finally, the cyber-attacks against Georgia demonstrated the ease with which states and individual actors can impact the cyberinfrastructure of another state.

1.3.2. Stuxnet and its Variants

The Stuxnet worm and its variants are the most sophisticated malware discovered to date. The discovery of Stuxnet in 2010 vindicated the fears of many scholars: first, that computer code could and would be weaponized;[60] and second, that the weaponized code could cause kinetic damage by manipulating devices (e.g., pumps or motors, as in the instant matter) attached to a system. Stuxnet was discovered in the summer of 2010 and was later found to be responsible for the destruction of gas centrifuges at the Iranian nuclear facility in Natanz, Iran.[61] Stuxnet has been described by Ralph Langner as a cyber-warhead where the worm's "goal was to physically destroy a military target—not just metaphorically, but literally."[62] In this instance, Stuxnet destroyed an estimated 1,000 centrifuges utilized in Iran's nuclear program by causing the centrifuges to spin out of control until they malfunctioned due to exceeding technical limits for the devices.[63]

---

60 Cyber-attacks that have had a kinetic effect have been alleged previously; most notable was the supposed attack on the Soviet gas pipeline by Canada and the United States in 1983, where a Trojan was utilized to disrupt a SCADA controller causing an explosion. Neither this attack, nor the tools utilized therein have ever been confirmed. *See*, Thomas Reed, *At the Abyss: An Insider's History of the Cold War* 4714-4722 (Kindle ed., 2004).

61 Chris Morton, *Stuxnet, Flame, and Duqu – the Olympic Games*, *in*, A Fierce Domain: Conflicts in Cyberspace, 1986-2012, 212-231 (Jason Healey ed., 2013). Ralph Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE Sec. & Privacy 49-51 (May/June 2011). David Kushner, *The Real Story of Stuxnet*, IEEE Spectrum 49-53 (Mar. 2013). Boldizsár Bencsáth, *Duqu, Flame, Gauss: Followers of Stuxnet* (Presentation), RSA Conf. Eur. (2012), http://www.rsaconference.com/writable/presentations /file_upload/br-208_bencsath.pdf. Nicolas Falliere, Liam O Murchu, and Eric Chien, *W.32 Stuxnet Dossier* v1.4, Symantec (Feb. 2011).

62 Langner, *id.*.

63 Morton; Langner; Kushner; *supra*, n. 64. (To date, Iran has not publicly revealed the extent of the damage caused by the Stuxnet worm to its nuclear program.)

Stuxnet itself was not designed to do anything other than target a specific type of Supervisory Control and Data Acquisition (SCADA) controller produced by Siemens Corporation[64] and utilized by Iran in its nuclear program. However, the computer code that Stuxnet was based upon gave rise to Duqu and Flame variants of the Stuxnet worm. Duqu and Flame were not designed, per se, to do damage to any computer or component; instead, they were designed to conduct cyber-espionage. Like Stuxnet, these variants were extremely sophisticated, but unlike Stuxnet (which limited itself to a highly specific target), Duqu and Flame targeted general Windows-based platforms. Duqu and Flame were designed to steal information either through digitally copying files or indirect means utilizing a PC system's microphone and video camera. Once the information was captured, it was sent via the Internet to an unidentified end user.

Like the cyber-attacks on Estonia and Georgia, no state has ever been held responsible for Stuxnet and its variants, or for the destruction of nuclear centrifuges in Iran. While most commentators have circumstantially attributed the attacks to the United States and Israel,[65] neither state has accepted responsibility, and Iran has not sought to hold any state responsible.

Stuxnet, Duqu, and Flame demonstrated several distinct issues not found in the Estonia and Georgia attacks. First, Stuxnet was utilized as a directed weapon toward a specific target. However, Stuxnet was not propagated through, nor did it rely upon, the Internet. Stuxnet is thought to have been propagated through infected USB drives or software. Stuxnet did eventually work itself into the wild, though; e.g., it has been propagated by the Internet, but that seems to have been a knock-on effect of the original release. Stuxnet was sophisticated,

64 Langner, *id*., at 64. (Langner explains that Stuxnet targeted two specific controllers produced by Siemens: the 315 controller and the more sophisticated 417 controllers.) *See also*, Ralph Langner, *Cracking Stuxnet, a 21st-Century Cyber Weapon*, TED Talks (transcript) (Mar. 2011), http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon/transcript. (Langner noted that Stuxnet would not target any other system, stating "Stuxnet behaved like a lab rat that didn't like our cheese —sniffed, but didn't want to eat. Didn't make sense to me. And after we experimented with different flavors of cheese, I realized, well, this is a directed attack. It's completely directed.")

65 *See also*, Chris Morton, *Stuxnet, Flame, and Duqu – the Olympic Games*, *in*, A Fierce Domain: Conflicts in Cyberspace, 1986-2012, 223-231 (Jason Healey ed., 2013). (Discussing the motivation on behalf of the United States and Israel to conduct such a cyber-attack, the technical abilities of both states, and the motivation of both states to conduct such an attack.)

weaponized code intended to destroy a specific target, whereas the DDoS attacks on Estonia and Georgia were meant to disrupt military and civilian digital infrastructure and command and control functions—they were not intended to have a kinetic effect. Second, technical attribution and legal attribution of the Stuxnet attacks relied entirely on the forensic analysis of the computer code utilized within the attacks. While the attacks may be circumstantially attributed to a state or states, there has been no direct evidence of state involvement demonstrated to date. Finally, Stuxnet was at a technical level never seen before in malware, and the production of the malware necessitated a large investment in money and technical knowledge; it demonstrated a long-term plan on behalf of a state or non-state actor.

Duqu and Flame demonstrated that unknown actors might utilize cyberspace and the Internet to actively conduct espionage, either militarily or industrially, on a given target. While espionage has existed as long as states have and is not necessarily unlawful in international law, the ability to acquire sensitive data on such a large level has never before been achievable in espionage. Espionage such as this is particularly worrisome as states that lose sensitive data on a large scale may be more likely to use unlawful means, including kinetic acts, to prevent the loss of important state and industrial secrets.

1.3.3. The Sony Hack

In late 2014, the computer systems of Sony Pictures were subjected to wiper malware "which erased all the data on infected PCs and servers they were connected to."[66] In

66 Sean Gallagher, *Sony Pictures Hack Gets Uglier; North Korea Won't Deny Responsibility*, ARS Technica, (Dec. 2, 2014), http://arstechnica.com/security/2014/12/sony-pictures-hack-gets-uglier-north-korea-wont-deny-responsibility/. *See also*, Adam Clark Estes, *The Sony Pictures Hack Was Worse than Everyone Thought*, Gizmodo, (Dec. 3, 2014), http://gizmodo.com/the-sony-pictures-hack-exposed-budgets-layoffs-and-3-1665739357/1666122 168. Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, Wired, (Dec. 03, 2014). James Rogers, *Was the Sony Pictures Hack an Inside Job?*, Fox News, (Dec. 5, 2014), http://www.foxnews.com /tech/ 2014/12/05/was-sony-pictures-hack-inside-job.html. Seth Rosenblatt, *13 Revelations from the Sony Hack*, CNET, (Dec. 13, 2014), http://www.cnet.com/news/13-revelations-from-the-sony-hack/. Rebecca Keegan, *Sony Hack 'Unprecedented, Damaging and Unique' Cyber Security Firm Says*, L.A. Times, (Dec. 6 2014), http://www.latimes. com/ entertainment/envelope/cotown/la-et-ct-sony-hack-20141206-story.html

addition, at least 25 gigabytes of sensitive data were stolen and then published online.[67] A hacking group calling themselves the "Guardians of Peace" claimed responsibility for the hack. However, many commentators and the U.S. government believed that the government of North Korea was behind the hack. Their suspicion of North Korea was due, in part, to the planned release of the Sony movie *The Interview*, a movie depicting "an ill-conceived CIA plot to kill North Korean's leader Kim Jong-un."[68] North Korea had previously complained to the United Nations about the release of the film. North Korea did not deny responsibility for the attacks, lending some credence to the assertion.[69]

The United States publicly stated that North Korea was responsible for the Sony Hack. While the United States imposed sanctions on North Korea in January 2015, the basis for responsibility being attributed to North Korea has not been definitively established. The United States has merely asserted that analysis of the attack, analysis of the attack tools, and intelligence demonstrated North Korea's culpability. However, many commentators and security experts question the attribution of the Sony Hack to North Korea, believing instead that it was an "inside job."[70] This claim that the hack was an inside job is based on a forensic analysis of the malware used in the attack, the different servers that were impacted, and the ease in which disparate information was accessed. One security expert explained:

> [f]rom the samples we obtained, we can say the attackers knew the internal network…[and] the malware samples contain hardcoded names of servers inside Sony's network and even credentials/usernames and passwords that the malware use[d] to connect to systems inside the network.[71]

---

67 Gallagher, *id*. (The group claiming responsibility for the attack claimed to have up to 10 terabytes of data stolen from Sony.) Estes, *id.* (Stating that Gizmodo was able to download at least 40 gigabytes of data relating to "everything from medical records to unreleased scripts.")

68 Zetter, *supra*, n.65.

69 Gallagher, *supra*, n. 65.

70 James Rogers, *Was the Sony Pictures Hack an Inside Job*? Fox News, (Dec. 5, 2014), http://www.foxnews.com/tech/2014/12/05/was-sony-pictures-hack-inside-job.html.

71 Rogers, *supra*, n.66.

The Sony Hack is important in that it demonstrated the difficulties in attributing malicious cyber-attacks. The United States government has not publicly released the means or sources it utilized to conclude that North Korea was responsible, leaving many questions unanswered. However, this study will argue that technical issues aside, the United States, under existing CIL, should not have imposed sanctions upon North Korea without an affirmative showing of direct government involvement in the attacks. Merely linking the attacks to known IP addresses used by North Korea, or finding Korean language code within the malware is not enough to establish state responsibility under existing CIL without a further showing of involvement by the government or its agents.[72]

1.4. The Actors in Cyberspace: The Authors Behind the Attacks

The issue of who authors a cyber-attack directly impacts the existing legal paradigms. Simply put, if a state is the author of an attack, under existing CIL, then state responsibility would attach if such authorship could be demonstrated to a clear and convincing level.[73] As will be discussed *infra*, in Chapter Four, properly identifying the author of a cyber-attack is difficult, if not impossible: there are no means readily available to identify who authored an attack, and the technical sophistication of an attack is not necessarily an indicator of authorship.[74] Compounding the issue of authorship are the blurred lines between states and so-called patriot hackers (hacktivists) or state proxies (proxies): hacktivists and proxies may carry out cyber-attacks (both malicious and militarized) on a perceived enemy of their state with acquiescence from said state. Such cyber-attacks have been seen in both of the DDoS attacks on Georgia and Estonia.

---

72 *Supra*, n.66.

73 Presuming that the cyber-attack is "attributable to a state in international law" and "constitutes a breach of an international obligation of the state." Int'l L. Comm., *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Art. 2 *et seq*. U.N.G.A. A/56/10 (2001).

74 It is difficult, as a general proposition, to accurately claim that a state is an author of an attack based on the type of code utilized for the attack. However, some attacks are so advanced and costly that the probability of who could be responsible is limited. *See, e.g*., Kaspersky Lab, *Regin: Nation-state Ownage of GSM Networks* (Nov. 24, 2014), https://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/.

Adding to this confusion, the computer code responsible for both forms of cyber-attacks may be reusable. Any cyber-attack author with a modicum of technical knowledge might reuse existing computer code to perpetrate additional attacks even if he was not the original author of the code. Numerous cyber-attacks may be spawned from a single source of software code and adapted by multiple individuals each time the adversary changes its defenses or when the author wishes to target a new victim. As such, multiple actors may utilize a single source of software as a platform to create multiple cyber threats. Looking at the code for the software may be misleading and may cause misattribution.

In cyber-attacks, a single actor may play many roles. Knowledge is portable: one actor may play a role as an individual actor hacking for fun, another role as a cyber-criminal exploiting the Internet for profit, another role as a hacktivist or proxy supporting his identified cause against another state, or even as an agent of a state programming cyber weapons. As a general proposition, the roles of individual actors within cyber-attacks lack clearly delineated boundaries or definitions. One may define the roles and activities of these actors in broad generalities, but one must be aware that the actor may switch between roles at any time and at will.

As a general proposition, this study addresses the individual cyber-attack authors under the generic definition of computer hackers who may either be non-state actors or state actors. This study avoids labeling the individual hackers as malicious since their individual acts may be for a multitude of legitimate and lawful reasons, including expressions of an individual's right to free speech. It is when those individual acts cause harm, which negatively impacts a state through the malicious exploitation of the Internet, that the individual hackers fall into the purview of this study. Outside of this delineated range, an individual hacker is subject to the domestic law of the state in which his acts were perpetrated or the injured state which his acts impacted.

It is important, though, to attempt to understand the individual actors as the driving force behind many cyber-attacks. This study utilizes four broad categories of actors within cyber-attacks: hackers, cyber criminals, hacktivists/proxies, and states.[75] This study does not

[75] Actors may also be engaging in active re-hacking or hackback attacks in which the victim attempts to hack the hackers to recover data or attempt to harm hacking activities. *See*, Craig Timber, Ellen Nakashima, and Danielle Douglas-Gabriel, *Cyberattacks Trigger Talk of 'Hacking Back"*,

address those authors involved with cyber terrorism, nor does it address the issue of cyber terrorism itself. This study posits that the only difference between the issues discussed in this study and the issue of cyber terrorism is the subjective political intent of the attack authors.

Hackers can be described as the basic actors within cyber-attacks. They range in sophistication from the derisively-termed script kiddies[76] to advanced computer scientists holding post-graduate degrees in computer science. These hackers who intentionally exploit and disrupt computer systems for criminal or monetary reasons may also be referred to as crackers.[77] Hackers are responsible for the majority of cyber-attacks, but they are not, per se, subject to international law as individuals.

Cyber criminals are individual hackers who engage in traditional crimes such as fraud or theft via the Internet, or they may be organized crime groups that employ hackers for that purpose. Cybercrime is a major international problem costing states and businesses untold amounts of money. The exact costs of cybercrime are much debated, but General Keith Alexander has called cybercrime the "greatest transfer of wealth in human history…"[78] with loss estimates to the United States between $100 billion to $1 trillion per year.[79]

Wash. Post (Oct. 9, 2014), http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/ 10/09/6f0b 7a24-4f02-11e4-8c24-487e92bc 997b_ story .html. *See also.,* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for The Use of Active Defenses Against States Who Neglect Their Duty to Prevent,* 201 Mil. L. Rev. 1 (2009). (Discussing the right by states to use active defenses to stop an ongoing cyber-attack).

76 A "script kiddie" is normally a juvenile or a less technically sophisticated hacker who relies on pre-written software to exploit a known weakness. These hackers may not understand the complexity of the code they are utilizing, but they are motivated to seek out and exploit systems, causing untold damage in their wake. Symantec, *What is a Script Kiddie?* (2010), http://www.pctools.com/security-news/script-kiddie/.

77 Symantec, *What are Crackers and Hackers?* (2010), http://www.pctools.com/security-news/crackers-and-hackers/. ("It should be noted that numerous philosophies exist behind hacking, some hackers identify as 'white hat' hackers and actively seek out exploits with the intention of creating better security for the Internet. 'Black hat' hackers are those who seek out exploits for personal gain, whether monetary or for notoriety.")

78 *As quoted in*, Siobhan Gorman, *Annual U.S. Cybercrime Costs Estimated at $100 Billion*, Wall St. J. (July 22, 2013), http://www.wsj.com/articles/SB10001424127887324328904578621880966242990.

79 *Id.*

Hackers are not alone in committing cybercrime; a state may engage in espionage and cybercrime to further its domestic agenda,[80] or some states may engage in willful blindness or acquiesce to cybercrime due to the wealth such activities bring to its economy indirectly. A state may engage in or be complicit in such criminal acts, and it may be held responsible in international law only if the cyber acts can be attributed to it for the purposes of state responsibility.

Hacktivists sometimes referred to as patriot hackers,[81] or proxies,[82] are groups of hackers who share a political or religious ideology, who band together to promote, protect, and defend their shared ideology through actions on the Internet.[83] Hacktivists may be anonymous groups of unknown hackers working together and never knowing other actor's identities within their group (other than a *nom de guerre*/hacker identity), or they may be close-knit groups who actively interact outside of the cybersphere and utilize the Internet to promote an identity that the members share. Hacktivists pose unique problems in that they may act as an adjunct to an ongoing conflict. For example, hacktivist groups have been blamed for the DDoS attacks on Georgia and Estonia during their conflicts with Russia. Hacktivists have also taken part in the ongoing Israeli-Palestinian conflict with groups on both sides engaging in cyber skirmishes ranging from website defacement to small-scale DDoS attacks.[84]

Hacktivist groups are engaged in a variety of attacks and other activities throughout the world. If there is a conflict, in many instances, it is likely that hacktivist groups are supporting it or fighting it on the Internet. A recent example of this is the hacking group,

---

80 Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, (Feb. 2013), http://intelreport.mandiant. com/Mandiant_APT1_Report.pdf.

81 Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners* 197 (2011).

82 Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 Fletcher Sec. Rev. 55 (Spring 2014). (Describing proxies as those cyber actors who "act in varying degrees of support for particular states and their policy objectives.")

83 *Id.*

84 Sam Frizell, *Off the Battlefield, Hackers Are Waging Cyberwar Against Israel and Palestine*, TIME (Aug. 7, 2014), http://time.com/3089473/israel-gaza-hackers/.

anonymous, and its malicious cyber-attacks on the United States, including attacks after grand juries in the United States, returned no-bills (the individuals accused of wrongdoing were not indicted by a Grand Jury) in police officer use-of-force cases against African Americans in Missouri and New York.[85] In these incidents, Anonymous hacked websites, exposed personal information, conducted DDoS attacks, and ran amok against the United States cyberinfrastructure in protest. These attacks by Anonymous, while arguably an expression of its individual member's freedom of expression, was arguably criminal in that they violated domestic United States law. They could also be considered malicious cyber-attacks in that they are malicious uses of the Internet which engage the international legal order: the majority of these attacks were launched from states other than the United States.

While hacktivist groups do not necessarily engage the state for purposes of state responsibility, they take on a pseudo-state role in many instances and create a troublesome development for international law. As Pernek states:

> interstate political and military conflicts involve increasingly non-state actors; and lines between the actions of state entities and criminal individuals engaged in illegal activities are increasingly blurred…[86]

Thus, hacktivists may act as cyber militias for a state without engaging a state for the purposes of state responsibility. Given the difficulties regarding technical attribution of cyber-attacks, even with active engagement by state agents, it may be difficult or impossible to prove a link between a state and hacktivists acting on its behalf. This makes hacktivists an ideal intermediary for malicious acts in cyberspace since they allow a state plausible deniability, and current CIL on state responsibility is such that a state may escape international responsibility for the use of hacktivists or proxies—that is, as long as the state minimizes its contact and control of such hacktivists to avoid the threshold of "effective control" as put forth by the ICJ in *Nicaragua*.

---

85 Dara Kerr, *Ferguson, Mo., Police Site Hit with DDoS Attack*, CNET (Aug. 14, 2014), https://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/.

86 Piret Pernik, *Different Tactics, Same Story*, Int'l Center for Def. Studies (March 28, 2014), http://blog.icds.ee/article/255/different-tactics-same-story. *See also*, Piret Pernik, *A Playbook for Hybrid War in Cyberspace?* Int'l Center for Def. Studies (Aug. 29, 2014), http://blog.icds.ee/article/cyber-security/a-playbook-for-hybrid-war-in-cyberspace.

Lastly, states may be responsible for malicious cyber-attacks under certain circumstances. While no individual state has yet been found to be directly and actively engaging in malicious cyber-attacks, there is some circumstantial evidence that states have done so both with malicious cyber-attacks[87] and with use-of-force cyber-attacks.[88] State-sponsored cyber-attacks may utilize the same malware as similar non-state attacks, or they may be so advanced that they could only have been carried out by a state-sponsored cyber-attack. These attacks are as difficult to attribute like any other cyber-attack, and such cyber-attacks may intentionally lay a false attribution trail, complicating an already complicated problem.

For the purpose of this study, as a general proposition, states will be treated like any other actor who is utilizing malicious cyber-attacks. Indeed, it cannot be stressed enough that the difficulty of attributing individual attacks means that one might never truly identify the authors of the attacks, making it as likely as not that a state could be responsible. Therefore, it is necessary to utilize other types of attribution paradigms. The breadth and variety of the potential cyber-attack authors and the difficulties with attributing cyber-attacks to unidentifiable individuals, groups, and states significantly impede attribution for the purposes of state responsibility. As such, this study will explore alternative paradigms for attribution for the purposes of holding a state responsible for cyber-attacks in an attempt to posit a working paradigm for the protection of states.

1.5. Study Parameters

This study addresses the issue of malicious cyber-attacks and attribution, state responsibility, and the duty to prevent them in international law. This study focuses on those cyber-attacks that do not rise to the level of force, a subject that has not until recently attracted much attention from the international legal community and is a distinct emerging

87 The Duqu, Flame, and Stuxnet cyber-attacks appear to have been state-sponsored cyber-attacks and have been circumstantially attributed to the United States and possibly Israel. It is probable that more recent cyber-attacks such as the Regin malware are also state sponsored. *See*, Electronic Frontier Foundation, *State Sponsored Malware* (n.d.), https://www.eff.org/issues/state-sponsored-malware.

88 E.g., Stuxnet attacks which resulted in kinetic damage.

legal issue.[89] This study is not solely on the existing CIL of state responsibility—it also addresses alternative theories for state responsibility, attribution, and issues of proof. This study is not a general study of the law of state responsibility as applied to cyber-attacks; it focuses on issues related to attribution for the purpose of holding states responsible under CIL. This study also addresses alternative theories for attribution and state responsibility.

This study makes a significant and important contribution to the existing corpus of international law. It addresses the most prevalent forms of cyber-attacks (malicious cyber-attacks), a problem which has largely been left to individual states to deal with, although it arguably impacts all states. Malicious cyber-attacks are an international problem as they routinely implicate multiple states, and the harm suffered from such attacks often originates from another state. As malicious cyber-attacks have seemingly been ignored in international law, this study addresses the issue in depth. This study addresses the issues of malicious cyber-attacks as a matter of public international law. As such, it utilizes sources of law as put forth in Art. 38 of the *Statute of the International Court of Justice*.[90]

As the majority of scholarship on this topic in public international law is in regards to cyber warfare, cyber terrorism, and those cyber-attacks that may be considered a use of force, there will be a large volume of argument by analogy as the principles are similar, yet different. This study relies in part on the *Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual)*.[91] It must be noted that while the *Tallinn Manual* should be regarded as what Art. 38(1)(d) of the *Statute of the International Court of Justice* refers to as, "teachings of the most highly qualified publicists…" the *Tallinn*

89 *See*, e.g., Robin Geiss and Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Toward Non-Forcible Countermeasures and Collective Threat-Prevention*, *in*, Peacetime Regime for State Activities in Cyberspace (K. Ziolkowski ed., January 1, 2014). http://ssrn.com/abstract=2462950.

90 Statute of the International Court of Justice (1949). *See also*, Kirthi Jayakumar, *Where Does Article 38 Stand Today?*, E-Ir, (Oct. 12 2011), http://www.e-ir.info/2011/10/12/where-does-article-38-stand-today. H.C. Gutteridge, *The Meaning of Article 38(1) of the Statute of the International Court of Justice*, 38 Problems of Public and Private Int'l L. 125 (1952). Aldo Zammit Borda, *A Formal Approach to Article 38(1)(d) of the ICJ Statute from the perspective of the International Criminal Courts and Tribunals*, 24 Eur. J. Int'l L. 649 (2013).

91 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Michael N. Schmitt ed. 2013).

Manual only reflects one view on the issues presented, and should not be considered governing law; it is more akin to that of a restatement of law and thus open to debate. Also, the *Tallinn Manual* concerns itself with those attacks that implicate UN charter Art. 2(4). Accordingly, the controlling legal regimes posited by the *Tallinn Manual* may differ from those put forth herein.

This study also discusses the technical aspects of cyber-attack attribution from the computer science standpoint. This study operates under the belief that at present, there are no true and timely means of attribution for the majority of malicious acts in cyber-space.[92] Thus, necessitating a legal mechanism in lieu of true attribution for the purposes of state responsibility.

This study discusses malicious cyber-attacks, including cyber espionage. As a matter of public international law, it must be noted that espionage is not, per se, an illegal act. There is no explicit prohibition in either treaty law or CIL that prohibits most common forms of espionage. While there is, an ongoing debate regarding whether the prohibition contained in the *Vienna Convention on Diplomatic Relations* specifically covers electronic communication as analogous to other diplomatic communication,[93] such nuance is not addressed within this study. This study instead addresses the issue of attribution of malicious cyber-attacks that result in harm to a state. That is, this study does not differentiate between vectors and types of cyber-attacks. Simply put, if an act that could be defined as cyber-espionage causes harm to another, then this study would apply; if no harm results from cyber-espionage, then this study would not apply.

---

92 *Developing Norms for Cyber Conflict*, *in*, Research Handbook on Remote Warfare (Forthcoming), (J. Ohlin ed, 2016), http://papers.ssrn.com/sol3/ papers. cfm?abstract_id=2736456. ("Prompt attribution of an attack and even threat identification can be very difficult.") Kosmas Pipyros, Lilian Mitrou,, Dimitris Gritzalis, Theodoros Apostolopoulos, *Cyberoperations and International Humanitarian Law : A Review of Obstacles in Applying International Law Rules in Cyber Warfare*, 24 Information and Computer Security 38 (2016). ("The absence of a widely accepted legal framework to regulate jurisdictional issues of cyber warfare and the technical difficulties in identifying, with absolute certainty, the perpetrators of an attack, make the successful tackling of cyber attacks difficult.")

93 *See, Vienna Convention on Diplomatic Relations*, Art. 27, June 24, 1964, 500 U.N.T.S. 91 (Discussing the "inviolability of official consular communications…")

1.6. Study Overview

Chapter Two will begin with a general discussion regarding the formation of CIL, the CIL on state responsibility, and the *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Chapter Two continues with an in-depth discussion regarding the formation of CIL and select theories concerning the formation of CIL. This discussion on the formation of CIL is important, as the majority of this study relies upon customary international law in one form or another. As discussed *supra*, the law of cyberspace is for all intents and purposes a CIL, as existing treaties are either too narrow in scope, outdated or not widely accepted. There is currently no treaty in place that addresses the issues put forth in this study, and the likelihood of a single treaty concerning malicious cyber-attacks being adopted by the major powers is nil, due to significant differences in the use and control of cyberspace. This lack of a treaty, therefore, makes the CIL, the only law available to guide states in their actions in cyberspace. Additionally, the law of state responsibility is a product of CIL and will evolve in response to changes in custom. This study, therefore, operates under the belief that a solid discussion on the formation of custom is needed prior to any further discussion, as the formation of custom and associated theories directly impact the laws controlling cyberspace and state responsibility.

The discussion regarding CIL relies in large part on the work of the International Law Association (ILA). This study utilizes their work as the ILA is composed of subject matter experts and the work has been cited favorably by international courts and tribunals. By focusing on the work of the ILA, this study is able to present needed information in the least controversial manner possible, because as with any legal theories, even the formation of custom has its controversies. This study attempts to avoid most controversies regarding the formation of CIL by utilizing the work of the ILA, and only briefly discussing the more controversial theories of CIL formation.

Chapter Two finishes with a generalized discussion regarding state responsibility, setting the foundation for the follow-on chapters and establishing a baseline for further discussion regarding state responsibility as put forth by the ILC in its ARS. As noted *supra*, the work of the ILC is part of the CIL and has been accepted by international courts and tribunals as such. This study utilizes the work of the ILC and cases from the ICJ to demonstrate what the basic rules of state responsibility are, and how they are applied to the instant issue. This

section is presented in order to build on the discussion on the formation of CIL and the formation of the CIL of state responsibility. Each chapter in this study builds upon knowledge and information conveyed in earlier chapters, enabling the reader to understand the concepts and theories presented in each follow-on chapter.

Chapter Three is an in-depth analysis regarding the attribution of malicious cyber-attacks and the evidentiary burden associated with attributing malicious cyber-attacks as a matter of CIL. This chapter is a follow-on to the Chapter Two discussion on the ILC's ARS as the rules of attribution are part thereof. In addition to discussing the rules of attribution, the evidentiary burden associated with the proof of a violation needed to trigger attribution and how an act may be attributed to a state is also discussed. This discussion regarding the rules of attribution demonstrate the difficulties of attributing a malicious cyber-attack to a state, as both the evidentiary burden needed to attribute an act to the state is difficult to meet, and as is the evidentiary burden of proving that a state had effective control over a non-state actor for state responsibility to lie.

Chapter Four discusses the basic operation of the Internet and cyberspace and how computer science approaches the issue of cyber-attack attribution. This chapter discusses both technical attribution through the lens of computer science and circumstantial attribution which melds legal and technical attribution theories and techniques. This chapter serves to demonstrate the technical difficulties involved with affirmatively identifying and attributing a cyber-attack to a state. This issue is discussed in depth to demonstrate to the reader how legal attribution of a malicious cyber-attack fails due to the limitations and difficulties involved with technical attribution. This chapter builds on the discussion in Chapter Three to demonstrate that without affirmative technical attribution to the individual level (i.e., bridging the air gap between the computer system(s) used for an attack and the individual programmer or programmers), legal attribution as established by the ARS is not possible. In addition, this chapter demonstrates that under existing CIL and ICJ case law, circumstantial attribution is not a valid means of attribution, as the ICJ has held that circumstantial evidence is not enough to link a state to wrongful conduct. Chapter Four will conclude Part One of this study.

Chapter Five serves as the introduction to Part Two in which this study looks to alternative theories found in CIL for attributing and holding states responsible for malicious cyber-

attacks which are traced back to a state's sovereign territory, yet cannot be affirmatively attributed to the state itself. Chapter Five introduces the reader to theories which this study puts forward as a means of holding states responsible for malicious cyber-attacks without direct affirmative attribution of those attacks. This chapter discusses the prohibition on unlawful political intervention, the Trail Smelter arbitration and the prohibition on transboundary harm, the Corfu Channel principles, and the theory of strict liability for ultra-hazardous activities. These theories are used herein as it is argued by this study that they are analogous to the instant issue and demonstrate that alternative means of holding states responsible exist in CIL.

Chapter Six continues with the discussion regarding alternative theories in which to hold states responsible for malicious cyber-attacks under existing theories of CIL. Chapter Six addresses the theories of indirect responsibility, the due diligence principle, and the duty to prevent harmful conduct as applied to malicious cyber-attacks. This chapter builds upon the discussion in Chapter Five and the theories presented therein. Chapter Six again discusses existing theories of CIL and applies them to the instant issue in order to demonstrate additional means of holding states responsible for malicious cyber-attacks that exist in CIL.

Chapter Seven addresses recent developments within CIL and state responsibility by analyzing and discussing the post-9/11 invasion of Afghanistan by the United States and its allies. This study argues that the acts of the United States and its allies of holding the de facto government of Afghanistan, the Taliban, responsible for the acts of Al-Qaeda and the terror attacks on the United States was in contravention to the existing CIL of state responsibility. As such, new CIL may have sprung from the acts of the United States and its allies. This chapter addresses this theory in depth. This chapter is important as it demonstrates that CIL may adapt to changing state practice in response to new types of warfare. This chapter is particularly suited for the discussion herein as terrorism, like malicious cyber-attacks, are an evolving legal phenomenon and those acts taken in response to terror attacks may control by analogy to the instant issue.

Chapter Eight concludes this study with a discussion regarding how the international community and individual states may prevent future malicious cyber-attacks. In addition, this study will address the idea of a cyberweapons treaty and the idea of self-help by injured states prior to concluding this study.

Chapter Two: Customary International Law and State Responsibility in Cyberspace

2. Introduction

This study begins in Chapter Two with a discussion concerning the formation of customary international law before turning to a discussion concerning the ILC's ARS and the basis of state responsibility for wrongful acts. This chapter begins with a discussion on the formation of CIL for four reasons: (1) custom forms the basis for all the legal theories discussed in the substantive portions of this study; (2) the laws of state responsibility have evolved through the CIL process and respond to changes through the continued evolution of CIL; (3) the law of cyberspace is CIL until such time as a treaty or treaties may be concluded on point; and (4) it is argued by this study that the best solution to the issue of malicious cyber-attacks and attribution thereof is to be found within existing CIL which controls by analogy. This study believes that a solution to the instant issue exists within CIL and will discuss this approach in later chapters. As such, this chapter will begin with a discussion regarding the formation of CIL to establish a base of understanding for future arguments.

2.1. Initial Matters

Prior to engaging in an in-depth discussion and analyses concerning this matter, this study must address: (1) what is meant by the term attribution as used herein and how does it apply to the issue of state responsibility for malicious cyber-attacks; (2) why is this issue worthy of scholarly discussion; (3) why does this study address the issue of attribution of malicious cyber-attacks from both a legal and technical viewpoint; and (4) why does this study utilize the sources of law that it does?

State responsibility, as put forth by the ARS Art. 2, requires two elements, (1) an internationally wrongful act; and (2) attribution of that act to a state, which will be discussed in detail, *infra*.

Attribution, in relation to malicious cyber-attacks, may be defined in the technical sense as the determination of the original Internet Protocol (IP) address for the system responsible for initiating an attack.[1] In theory, this process of determining the originating IP address is straightforward.[2] As will be discussed in depth in Chapter Four, technical attribution is quite challenging with numerous techniques available to the attacker to thwart attribution.[3]

In the legal context, attribution may be understood as assigning a party legally responsible for an act. In the context of this study, attribution is understood as the assigning of responsibility to a state or third-party for initiating a malicious cyber-attack. However, under existing CIL, as put forth by the ICJ and as adopted by the ARS, the assignment of responsibility to a state is not as simple as tracing the IP address for an attack to a state.[4]

It must be noted prior to any discussion that there is much debate over the issue of whether the technical and legal attribution of malicious cyber-attacks is even possible. Some commentators hold that technical and legal attribution of malicious cyber-attacks is impossible. Other commentators, based in part upon comments of the former United States.

---

1 Paul J. Springer, *Cyber Warfare: A Reference Handbook* 92-93 (2015). *See also*, Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in*, Research Handbook on International Law and Cyberspace 62 (Nicholas Tsagourias and Russell Buchan, eds. 2016). ("[I]t is almost impossible to identify directly and with certainty the person or entity operating a personal computer. Identification of persons, and by consequence, attribution is only possible via identification of a computer by way of its IP address that identifies its precise location.") *Cf.* Neil C. Rowe, *The Attribution of Cyber Warfare*, *in*, Cyber Warfare: A Multidisciplinary Analysis 60-70 (James A. Green, ed., Kindle ed., 2015). (Discussing the difficulties of cyber-attack attribution.)

2 *Id.*

3 Neil C. Rowe, *The Attribution of Cyber Warfare*, *in,* Cyber Warfare: A Multidisciplinary Analysis 60-70 (James A. Green, ed., Kindle ed., 2015).

4 Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in*, Research Handbook on International Law and Cyberspace 62-71 (Nicholas Tsagourias and Russell Buchan, eds. 2016).

Secretary of Defense, Leon Panetta,[5] and other sources, plausibly argue that technical and legal attribution is achievable with current technology.[6] However, as will be explained in this study infra Chapter Four, this study rejects this idea based upon both the CIL of state responsibility and the technical reality of attribution. It is argued herein, that even when computer science can positively identify the IP address for the computer system responsible for a malicious cyber-attack, that identification alone, under existing CIL, does not demonstrate that a state is responsible for the attack (although this study will argue that this alone may be enough to hold a state responsible for malicious cyber-attacks under alternative theories of responsibility.) Attribution to the IP address level under existing CIL does not demonstrate that the state itself ordered or directed the cyber-attacks and therefore legal attribution cannot lie.[7]

The issue of state responsibility for malicious cyber-attacks is worthy of in-depth, scholarly review as it is an unanswered question. Malicious cyber-attacks can impact any state and determining the responsible party for the attacks is arguably paramount to avoid wrongful attribution and potential kinetic overflow from a cyber incident. As will be discussed *infra*, malicious cyber-attacks are responsible for what has been called "the greatest transfer of

---

5 Leon Panetta, U.S. Sec'y of Def., Speech Concerning Cyber Security to Business Executives for National Security in New York City, (October 11, 2012). *As published in*, Council of Foreign Relations (October 12, 2012). http://www.cfr.org/ cybersecurity/secretary-panettas-speech-cybersecurity/p29262. (Secretary Panetta stated, "[o]ver the last two years, DoD [(the United States Department of Defense)] has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment." This led many commentators to speculate that the United States could have the technology to attribute malicious cyber-attacks. This study rejects this interpretation without further supporting evidence of the means and methods of attribution. Secretary Panetta merely states that the United States has invested in forensics, which could mean a multitude of different computer techniques to attempt to identify an attacker, and given the United States' many failures to properly attribute such attacks, e.g., the Sony cyber-attacks in 2015 and the DNC Hacks in 2016, it is highly unlikely that the forensics Secretary Panetta is discussing, at least publicly, are working as well as hoped.)

6 *Cf.* Neil C. Rowe, *The Attribution of Cyberwarfare* 62, in, Cyberwarfare: A Multidisciplinary Analysis (James A. Green ed., Kindle ed. 2015) ("[A]ttribution of cyber-attacks is definitely possible. The evidence will always be circumstantial in the legal sense since cyber-attacks cannot be witnessed inside computers directly.") *See also*, Jason Healey, *Concluding Assessment, in*, A Fierce Domain: Conflict in Cyberspace 1986-2012, 265-278 (Jason Healey, ed. 2013). (Discussing circumstantial attribution of cyber-attacks.)

7 *Cf.*, Rowe, *id*. Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in*, Research Handbook on International Law and Cyberspace 62-71 (Nicholas Tsagourias and Russell Buchan, eds. 2016).

wealth in history."[8] It is argued herein that malicious cyber-attacks are one of the biggest challenges facing the international legal order in the 21st century. The issue of attribution and state responsibility for malicious cyber-attacks is at present a problem without a solution in international law.

2.2. The Works of the ILC and the ILA

This study will rely in great part on the writings of both the ILC and the ILA. Much of the work by the ILC on state responsibility is recognized as part of the corpus of CIL. That is, the work by the ILC on the ARS elucidated for the most part, what is or is not part of the CIL relating to state responsibility. The ARS itself is recognized as reflecting CIL, and the ARS is recognized as part of the CIL. The reliance on the work of the ILC on the ARS by the ICJ, NATO, states, and numerous commentators [9] is well documented and supports this proposition.

The work of the ILA, while more controversial[10] (due largely to the controversy surrounding the formation of CIL itself and not as a reflection on the quality of work

---

8 Josh Rogin, *NSA Chief: Cybercrime Constitutes Greatest Wealth Transfer in History*, Foreign Policy (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/. (Citing U.S. General Keith Alexander "U.S. companies lose about $250 billion per year through intellectual property theft, with another $114 billion lost due to cyber [-] crime, a number that rises to $338 billion when the costs of down time due to crime are taken into account…)

9 Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in*, Research Handbook on International Law and Cyberspace 58 (Nicholas Tsagourias and Russell Buchan, eds. 2016). ("Since 2001 [the ARS] has been [] extensively cited by international courts and tribunals, as well as in State practice, []it is considered as an authoritative statement of the customary international law of State responsibility.") *See also*, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, R 6, cmt. 1, (Michael N. Schmitt ed. 2013). ("This Rule [R.6] is based on the customary international law of State responsibility, which is largely reflected in the International Law Commission's Articles on State Responsibility.") *Id*. R.9, cmt. 1, ("Rule 9 and its accompanying Commentary are derived from Articles 22 and 49 to 53 of the International Law Commission's Articles on State Responsibility." The *Tallinn Manual* notes that "certain provisions" of the ARS are controversial and may not reflect customary international law. Those articles, which deal with the questions of countermeasures and the ILC's approach are not discussed herein.) James Crawford, *Brownlie's Principles of Public International Law* 540 (8th ed. 2012). Simon Olleson, *infra*, n.10.

10 Michael Wood, *Formation and Evidence of Customary International Law* 305 ¶5, Report of the International Law Commission, 63rd Sess. (26 April-3 June and 4 July-12 August, 2011) U.N.G.A. A/66/10/Annex 1. ("[P]revious collective efforts to describe, systematically, the process of formation of customary international law, while containing much useful material, have not met with general approval.'")

performed by the ILA), is authoritative in the instant issue regarding the general theories of CIL formation. This study bolsters the work of the ILA by utilizing the work of the ILC on the *Identification of Customary International Law*.[11] The work of the ILC on the identification of customary international law is the most current work available on the subject and is the work of arguably some of the best commentators on the subject. The work of both the ILA/ILC is utilized herein to avoid being dragged into the multiple controversies that abound whenever any discussion concerning the formation of custom is undertaken.[12] The work of both the ILA/ILC is of the highest scholarly quality and is deserving of the importance placed on it herein. It is accepted that neither the work of the ILA or ILC on CIL is a perfect solution, but taken together they represent the core rules on the formation of CIL. However, as needed, this study will go beyond the work of the ILA/ILC and utilize the work of recognized experts on point with the discussion.

This study in section 2.3., infra, will begin with a discussion on the formation and role of CIL. This study will then address the general principles of state responsibility in section 2.4. before turning to the issue of attribution in chapters three and four.

2.3. The Formation of Customary International Law

As the law governing both state responsibility and cyberspace are CIL (combined, therefore controlling the attribution and state responsibility for malicious cyber-attacks), this study opens with a general discussion regarding the formation of CIL. This study presents this information to support later discussion within this study. This study will portray the discussion regarding the formation and application of CIL in as neutral a manner as possible as to avoid controversies[13] surrounding the instant issue. As such, this study will rely on

11 International Law Commission, *Identification of Customary International Law*, Draft Conclusions, U.N. Doc. A/CN.4/L.872 (30 May 2016). *Report of the International Law Commission*, 68th Sess., U.N. Doc. A/71/10 (2 May-10 June and 4 July-12 August 2016).

12 *See e.g.*, Jörg Kammerhofer, *Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems*, 15 Eur. J. Int'l L. 523-553 (2004). (Discussing the issues and controversies surrounding the formation of CIL).

13 *See e.g.*, Anthea Elizabeth Roberts, *Traditional and Modern Law Approaches to Customary International Law: A Reconciliation*, 95 Am. J. Int'l L. 757, 767 (2001). (Discussing the

the works of the ILA/ILC and select scholars, who are recognized as experts on the subject. The discussion is presented to ensure a shared basis of understanding to facilitate further information exchange in later chapters. CIL consists of two elements: state practice, and *opinio juris.*[14] State practice is the objective element[15] and is easiest to discern from the actual acts and practices of states. *Opinio juris* is the subjective element and is often the most difficult to discern as states may act for multiple reasons and a state's reason for acting is often different from what it publicly says and privately believes.[16] *Opinio juris* is also "a tool by which [s]tates regulate the emergence, interpretation, and evolution of legal norms."[17] As such, *opinio juris* is an important tool for states to analyze emerging norms in cyberspace, as each state will interpret the practices of other states to discern if those acts are legal or are giving rise to new custom.

formation of CIL and the lack of "procedural normativity" which is responsible for much debate on the issue.)

14 Antonio Cassese, *International Law* 156 (2nd ed. 2005). ("General practice, or *usus* or *diuturnitas*"). Ian Brownlie, *Principles of Public International Law* 6-12 (6th ed. 2003). *See also,* Christopher Greenwood, *Sources of International Law: An Introduction* (2008), http://untreaty.un.org/cod/avl/pdf/ls/ greenwood_outline.pdf. Anthony Aust, *Handbook of International Law* 6-7 (2nd ed. 2011). Ernest A. Young, *Sorting Out the Debate Over Customary International Law*, 42 Va. J. Int'l L. 365, 372-373 (2002). *But cf*., Antonio Cassese, *International Law* 156 (2nd ed. 2005). (Cassese breaks *opinio juris et neccessitatis* into two distinct categories "*opinio juris*" which he defines as "conviction that such practices reflect, or amounts to law" and "*opinio necessitates"* practice that "is required by social, economic, or political exigencies.") *See also*, Anthony D'Amato, *The Concept of Custom in International Law* 49 (1971). For an updated discussion, *see*, Christian Dahlman, *The Function of Opinio Juris in Customary International Law*, 81 Nordic J. Intl L. 327, 330 (2012). *See also*, Michael N. Schmitt and Sean Watts, *The Decline of Opinio Juris and the Law of Cyber Warfare*, 50 Tex. Int'l L. J. 189 (2016). (Discussing the role of states in the formation of *opinion juris* and the declining involvement of states in the formation of the same.) International Law Commission, *Identification of Customary International Law*, Draft Conclusion 2, U.N. Doc. A/CN.4/L.872 (30 May 2016). (To determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice that is accepted as law (opinio juris)).

15 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference) 29 (2000). Michael P. Scharf, *Customary International Law in Times of Fundamental Change: Recognizing Grotian Moments* 47-57 (2013).

16 *See*, Christian Dahlman, *The Function of Opinio Juris in Customary International Law*, 81 Nordic J. Intl L. 327 (2012).

17 *See*, Michael N. Schmitt and Sean Watts, *The Decline of Opinio Juris and the Law of Cyber Warfare*, 50 Tex. Int'l L. J. 189, 193 (2016).

There is no set method for determining which element is more important, nor is there a set ratio of which element is needed for custom to bloom. However, "[e]ach of the two constituent elements is to be separately ascertained. This requires an assessment of evidence for each element."[18] Determining what constitutes "custom is not a matter of exact science."[19] This lack of formality in the formation of custom creates great controversy and allows for multiple theories for discerning the formation and existence of a custom in international law.[20] What can be agreed upon by most is that the instant matters of state responsibility and the law of cyberspace are governed by CIL. As such, this study will look at the elements necessary for the formation of CIL and two theories concerning the formation of CIL which are applicable to the instant issue.

2.3.1. Customary International Law Formation: State Practice and *Opinio Juris*

The elements needed to form CIL, (1) state practice, and (2) *opinio juris,*[21] will be addressed in an attempt to individualize the separate elements as "[i]t is often difficult or even impossible to disentangle the two elements…"[22] The goal is to distil the elements to the simplest construction in order to better recognize these elements when applied to later discussions in regards to state responsibility, attribution, and malicious cyber-attacks.[23]

---

18 International Law Commission, *Identification of Customary International Law*, Draft Conclusion 3(2), U.N. Doc. A/CN.4/L.872 (30 May 2016).

19 Tom Ruys, *'Armed Attack' and Article 51 of the UN Charter Evolutions in Customary Law and Practice* 30 (2011).

20 *Id.*

21 International Law Commission, *Identification of Customary International Law*, Draft Conclusion 3(1), U.N. Doc. A/CN.4/L.872 (30 May 2016).

22 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference) ¶ 10(c) at 7 (2000) *quoting, La Doctrine Des Deux Elements Du Droit Coutumier Dans La Pratique De La Cour Internationale*, 90 RGDIP 5, 114 (1986).

23 *Cf.* International Law Commission, *Identification of Customary International Law*, Draft Conclusion 3(2), U.N. Doc. A/CN.4/L.872 (30 May 2016). ("Each of the two constituent elements is to be separately ascertained. This requires an assessment of evidence for each element.")

2.3.1.1. State Practice

At its simplest, state practice is the conduct of a state in regards to any act. However, when seeking to define what constitutes state practice, the ILA Reports suggests that "it is necessary to take account of the distinction between what conduct counts as state practice and the weight to be given it."[24] Thus not all acts by states are of equal weight, an issue that complicates discerning state practice in cyberspace as those acts are not always overt and are prone to misattribution. As such, the ILA Reports treats this distinction as that of evidence before a court, and advises those seeking to distinguish acts to look to the "admissibility of the acts and [their] weight."[25]

Public acts, whether verbal or physical acts or omissions, may count as acts of a state for the purposes of counting as state practice.[26] The ILA Reports and the ILC work posit that both the verbal and physical acts of a state may form state practice.[27] As a pre-cyber age document, the ILA Reports does not address the formation of custom via cyberspace, and the ILC work does not address separate acts in cyberspace;[28] as such, some application by analogy is necessary. While both verbal and physical acts may apply to the formation of

---

[24] ILA, *id.*, Art. 3.

[25] *Id.* Art. 3 *et seq*. *See also*, *supra*, n. 23.

[26] International Law Associations Committee on Formation of Customary (General) International Law, Statement of *Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference), Arts. 4-6 (2000). The ILA adopts the position of the PCIJ in the S.S. Lotus Case (Judgement), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 27). *See*, *id*., Art. 6, cmt. 1. *See,* International Law Commission, *Identification of Customary International Law*, Draft Conclusion 5, U.N. Doc. A/CN.4/L.872 (30 May 2016). ("State practice consists of conduct of the State, whether in the exercise of its executive, legislative, judicial or other functions.") *Id.* at 6(2).

[27] International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference) Art. 4 at 14-15 (2000). ILC, *id.*, at Draft Conclusion 6(1).

[28] *See, e.g*., International Law Commission, *Identification of Customary International Law*, Draft Conclusion 6(2), U.N. Doc. A/CN.4/L.872 (30 May 2016). ("Forms of State practice include, but are not limited to: diplomatic acts and correspondence; conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference; conduct in connection with treaties; executive conduct, including operational conduct "on the ground"; legislative and administrative acts; and decisions of national courts.")

custom in cyberspace, it is necessary to also consider virtual acts in cyberspace, those acts that only occur in cyberspace and are neither physical nor verbal, but analogous thereto. However, identifying state acts in cyberspace is complicated as per the ILA, as all acts for the purpose of identifying state practice must be "public."[29] As cyber-attacks have emerged as a means for commercial and military espionage, a medium for various forms of attack, and a tool for other exploitive activities, states are not going to announce their actions in cyberspace, thus making it difficult to establish accepted state practice in cyberspace.

Neither the ILA nor the ILC place emphasis on the duration of practice to establish CIL. The ILC for example simply states that "1. The relevant practice must be general, meaning that it must be sufficiently widespread and representative, as well as consistent. 2. Provided that the practice is general, no particular duration is required."[30]

Both the ILA/ILC hold that omissions or failure to act are a positive act for determining state practice for the purpose of establishing CIL.[31] Omissions, as will be discussed Chapter Six, are an important element in not only determining state responsibility, but in the instant issue; a state not acting on a matter may signal acquiescence to the practice, or a non-act may be seen as an affirmative act in itself. Omissions are particularly important when a state takes an affirmative action that lays outside of the customary acts in international law and other states do not comment or take acts against the state. Such omission of action may rightly signal a state's acceptance of the act and may eventually (if there is enough density of practice) form CIL. For example, when the United States took action against North Korea after the Sony hacking incident and other states took no action pro or against the actions of the United States, even though those hacks were never attributed to North Korea by any reasonable measure of CIL, the omissions by those states may be objectively viewed as supportive of the actions on behalf of the United States. These omissions may be seen as state practice.

---

29 *Id*. Art. 5 at 15.

30 International Law Commission, *Identification of Customary International Law*, Draft Conclusion 8, U.N. Doc. A/CN.4/L.872 (30 May 2016).

31 ILA, *id*, at Art. 6.

Brownlie and other commentators apply different and more stringent criteria to the act of discerning state practice. Brownlie, for instance, looked at "[d]uration… [u]niformity, [c]onsistency of practice… [and] [g]enerality of practice."[32] Brownlie adopted his criteria based upon the ICJ's decision in the *Peruvian–Colombian Asylum Case*[33] where the court stated:

> [t]he Party which relies on a custom…must prove that this custom is established in such a manner that it has become binding on the other Party. The Colombian Government must prove that the rule invoked by it is in accordance with a constant and uniform usage practiced by the States in question…[34]

D'Amato offered "four modalities…duration, repetition, continuity, and generality"[35] for determining usage (state practice) which he contended were not "entirely separate"[36] but offered a "convenient classification."[37] D'Amato contends, though, that there is "no standard[] or criteria for determining how much time is necessary to create usage that one can qualify as CIL…"[38] Essentially, since each instance of custom formation is fact-specific, no two situations giving rise to custom are identical and too many factors play a role in the need for custom to rise. Although D'Amato does recognize that "the time factor cannot be ignored…,"[39] D'Amato does address "density of usage,"[40] as put forward by other commentators who contend that "what happens within a certain time is more important than the mere lapse of time."[41] D'Amato posited that regardless of the elements one looks to in an attempt to discern practice, these elements only serve to make the practice

---

32 Ian Brownlie, *Principles of Public International Law* 7 (6th ed. 2003).

33 1950 I.C.J. 266, (Nov. 20).

34 *Id*. at 276-277. Ian Brownlie, *Principles of Public International Law* 7 (6th ed. 2003).

35 Anthony A. D'Amato, *The Concept of Custom in International Law* 56 (1971).

36 *Id.*

37 *Id.*

38 *Id*. at 58.

39 *Id*. at 59.

40 *Id.*

41 *Id. quoting* Zdenek Slouka, *International Custom and the Continental Shelf* 13 (1968).

more "visible."[42] That is, breaking the custom down into distinct elements helps one discern the custom, but in the end, it is the customs itself, not the elements, that are of relevant importance.

Cassese[43] looked to the ICJ for guidance in determining the existence of state practice, quoting the decisions from both the *North Sea Continental Shelf cases* and *Nicaragua (Merits)*. From the *North Sea Continental Shelf case*s, Cassese noted that the "court stated that state practice, including that of states whose interests are specifically affected, should be both extensive and virtually uniform…"[44] From *Nicaragua (Merits)*, Cassese elucidated that,

> State practice need not be absolutely uniform. Individual deviations may not lead to the conclusion that no rule has crystallized but on the contrary, confirm the existence of a rule, in that either they are regarded as breaches of international law or the State concerned claims that its conduct was justified by exceptional circumstances.[45]

However, Cassese recognized that both elements (extensive and uniform) need not be present. Cassese contended that custom "evolves… [from] the impulse of economic, political, or military demands."[46] If the emerging custom does not "encounter strong and consistent opposition from other states but is…accepted or acquiesced"[47] to, then custom emerges. Simply put, once a state starts to follow an international legal norm from a sense of legal obligation, custom emerges[48]

As to the temporal element, Cassese argued, "the time element in the formation of customary rules may vary, depending upon the circumstances of the case and the states'

---

42 Anthony A. D'Amato, *The Concept of Custom in International Law* 67 (1971).

43 Antonio Cassese, *International Law* 157 (2nd ed. 2005).

44 *Id.*

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.* at 157-158.

interest at stake."[49] As long as state practice and *opinio juris* are present, then custom is formed.[50] Cassese recognized that custom might emerge in a relatively short period and also recognized the phenomena of "instant custom."[51] Thus attempting to clarify the debate as to whether custom may come about instantaneously or whether custom must be a matter of long-standing evolution and practice of the law prior to becoming custom.[52]

Young simplified the idea of state practice by focusing on "generality, duration, and consistency"[53] to establish state practice. Many commentators have moved away from Brownlie's consistency of practice prong without comment, but other commentators have debated whether the consistency of practice and duration are a necessary element, given the theory of instant custom. The theory of instant custom, discussed *infra*, however, is in itself highly controversial and lies at the fringe of public international law.

One element that all commentators seem to agree upon is that there needs to be density of practice. Density, meaning that enough states practice the act and that those state actions, as per the ILA, are "uniform, extensive and representative."[54] There is neither a set time period nor an exact number of states needed to demonstrate density of practice. The ICJ in the *North Sea Continental Shelf cases* held that "an indispensable requirement would be that within the period in question, short though it might be, state practice, including that of states whose interests are specifically affected, should have been both extensive and

---

49 Antonio Cassese, *International Law* 158 (2nd ed. 2005)

50 *Id.*

51 *Id.*

52 *Cf.* Ian Brownlie, *Principles of Public International Law* 7 (7th ed. 2008). *See also*, Anthony Aust, *Handbook of International Law* 7 (7th ed. 2011).

53 Ernest A. Young, *Sorting Out the Debate Over Customary International Law*, 42 Va. J. Int'l L. 365, 372-373 (2002).

54 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference) Art. 12 (2000).

virtually uniform in the sense of the provision invoked…"[55] Thus, as the ILA points out, there is no temporal requirement, and it is dependent upon "sufficient density of practice."[56]

The role of specially affected states is important to understand in the context of state practice. When attempting to determine the formation of custom, the ICJ[57] has emphasized the importance of the role of those states which have acted in response to a stimulus, giving rise to the formation of a new custom. In the instant matter, this study argues that the specially affected states important to the determination of state practice are primarily the United States, its NATO allies, and the P5 members of the Security Council.[58] This study argues that the acts of the United States should be viewed as those of a specially affected state as the United States suffered the worst terror attack (stimuli) in modern history. Its response to that stimuli, was based upon what the United States believed was the legal and proper action in international law, thus the acts of the United States should be viewed with a greater importance as the actions of the United States in response to the stimuli "occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved."[59] Specifically, the United States held the Taliban, the de facto if not the de jure government of Afghanistan responsible for the actions of al Qaeda outside of the CIL for state responsibility as they were understood at that time.

---

55 *North Sea Continental Shelf* (Fed. R. Ger. v. Den., Fed. R. Ger. v. Neth.), 1969 I.C.J. 3, 43 ¶74 (Feb. 20).

56 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference) Art. 12 cmt. a (2000). *But cf.*, Jack L. Goldsmith & Eric A. Posner, *The Limits of International Law* 23 (2005). ("[C]ustomary international law is usually based on a highly selective survey of [S]tate practice that includes only major powers and interested [S]tates.")

57 *North Sea Continental Shelf* (Fed. R. Ger. v. Den., Fed. R. Ger. v. Neth.), 1969 I.C.J. 3, 43 ¶74 (Feb. 20).

58 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference) Art. 14 cmt. e (2000).\

59 *North Sea Continental Shelf*, *id*, n. 57.

The actions of NATO members should be viewed as those of specially affected states as they not only enacted article 5 of the NATO Treaty,[60] thus viewing the attacks on the United States as an armed attack, and agreeing with the United States that the Taliban were responsible in part for the actions of al Qaeda. In addition, NATO (and 44 other aligned and non-aligned states) were specially affected as they, in one form or another, committed military forces to the fight in Afghanistan thus putting their citizens in harm's way in response to the stimuli that was the 9/11 terror attacks. This act of committing military forces by these states demonstrates not only their support for the United States but also the support that the United States was acting legally in response to the stimuli. It is their conviction and response to the stimuli that makes them specially affected, not necessarily their geographical location. If a state places its citizens in harm's way in response to specific stimuli, it is arguably specially affected by said stimuli.

The actions of the P5 members of the Security Council should be viewed as those of specially connected to the stimuli as not only are the United States, the United Kingdom, and France members of NATO but the other two P5 members of the Security Council, China, and Russia, had a role in determining the legality of the actions of the United States and its allies in Afghanistan. In this instance, China, and Russia acted as a form of a special referee who could have vetoed the Security Council resolutions giving rise to the military action against Afghanistan. Indeed, one may argue that the fact that China, and Russia, supported the actions of the United States bolsters the argument that the acts of the United States were legal and new custom rose there from. In addition, the fact that China and Russia offered both humanitarian and military assistance in Afghanistan supports this idea concerning the perceived legality of the United States actions. Lastly, the importance of the P5 members of the Security Council is important as the acts of the Security Council binds all United Nations members and the P5 members are the only members of the United Nations who can stop the acts of the Security Council by veto. Thus, China or Russia could have stopped the resolutions giving rise to the legal basis for the invasion of Afghanistan and the holding of the Taliban partially responsible for the acts of al Qaeda.

60 The North Atlantic Treaty (4 April 1949).

It is important to remember that not all states may be impacted by the same stimuli; and for those states which act in response to specific stimuli, their actions will be given greater weight than the acts of those states which are not necessarily impacted or affected. In the cyber for example, the response of Estonia and Georgia to the massive DDoS attacks would be given greater weight than to those states which have not suffered such attacks if the ICJ or other body were attempting to determine what the CIL is for responding to such attacks over the acts of states that have not suffered the same type attacks.

2.3.1.2. Opinio Juris

Brownlie defined *opinio juris*, the subjective element necessary for the formation of CIL, as actions on behalf of a state which are undertaken due to "a sense of legal obligation, as opposed to motives of courtesy, fairness, or morality."[61] That is, state practice is undertaken by states out of a sense of legal obligation or right. *Opinio juris*, in the words of the ILA, is a more controversial concept. The ILA explains that the controversy surrounding *opinio juris* derives from the difficulty of defining, applying, discerning the role of, and determining the importance of *opinio juris.*[62]

The subjective intent of a state is discussed by the ILA Reports in Art. 17, which posits that if a state does an act without the subjective belief that it is acting under a legal obligation to do so, no custom will rise from the act. This idea extends to areas of comity where no custom arises since the states are simply acting out of courtesy.[63] This is an interesting, albeit strained, concept in that many customs arguably derived from comity, particularly in the area of consular relations. Unfortunately, the ILA Reports provides little clarification

61 Ian Brownlie, *Principles of Public International Law* 8 (7th ed. 2008). *See also*, International Law Commission, *Identification of Customary International Law*, Draft Conclusion 9(1), U.N. Doc. A/CN.4/L.872 (30 May 2016). (To "be accepted as law (opinio juris) means that the practice in question must be undertaken with a sense of legal right or obligation.")

62 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference), Art. 15 cmt. (b) ¶2-3 (2000).

63 *Id.* Art. 17 (i).

on the subjective element; instead the ILA Reports allows each state to decide the matter for itself, forcing other states to adopt their postures based upon an unknown element, thus allowing states to act "just because" another state has done so before, irrespective of the traditional legality of the act.

The ILC does not engage at present in an in-depth exploration of *opinio juris*. The ILC simply reiterates the position of the ILA Reports stating that "the practice in question must be undertaken with a sense of legal right or obligation."[64] The ILC then continues by saying "opinio juris is to be distinguished from mere usage or habit."[65] The ILC then discusses what evidence supports the finding of *opinio juris*.[66]

When attempting to identify *opinio juris* in regards to state practice, the ILA Reports cautions that it is important to distinguish various elements including:

> (1) … individual views or position of states and their collective view or position; (2) the different forms these views or positions may take–on the one hand, belief, and on the other, will or consent; (3) the different stages in the life of a customary rule, and especially the time when it begins to be formed, on the other hand, and the time when it is already established, on the other hand.[67]

Brownlie believes, however, that the ICJ:

> provides a general guide to the nature of the problem–there are two methods of approach. In many cases, the Court is willing to assume the existence of an *opinio juris* on the basis of evidence of general practice, or a consensus in the

---

64 International Law Commission, *Identification of Customary International Law*, Draft Conclusion 9(1), U.N. Doc. A/CN.4/L.872 (30 May 2016).

65 *Id.* at 9(2).

66 International Law Commission, *Identification of Customary International Law*, Draft Conclusion 10, U.N. Doc. A/CN.4/L.872 (30 May 2016). ("1. Evidence of acceptance as law (opinio juris) may take a wide range of forms. 2. Forms of evidence of acceptance as law (opinio juris) include, but are not limited to: public statements made on behalf of States; official publications; government legal opinions; diplomatic correspondence; decisions of national courts; treaty provisions; and conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference. 3. Failure to react over time to a practice may serve as evidence of acceptance as law (opinio juris), provided that States were in a position to react and the circumstances called for some reaction.")

67 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference), Art. 16 cmt. (b) ¶2 (2000).

> literature, or the previous determinations of the Court or other international tribunals.[68]

The other method discussed by Brownlie involves "a more rigorous approach… [Where the PCIJ/ICJ] has called for more positive evidence of the recognition of the validity of the rules in question in the practice of states."[69] This "more rigorous approach" is seen in a minority of the cases before the court. In these cases, the court is faced with a lack of settled state practice or contention as to what the practice is, and the court is forced to make a determination as to the evidence.[70]

D'Amato, in discussing the various positions taken by commentators on this debate, posited that outside of specific exceptions, such as that posited by Bin Cheng on instant custom discussed *infra*, there is no way to prove *opinio juris* "apart from usage."[71] State practice is the only sure method of showing what a state intends. A state may say many things, in many different ways, "[b]ut a state can act in only one way at one time, and its unique actions, recorded in history, speak eloquently and decisively."[72] D'Amato recognized though that *opinio juris* plays an important role "when a state disputes the content of customary law."[73] Specifically, D'Amato pointed to the formation of new customs as an important role for *opinio juris.*[74]

D'Amato posited in his "reformation of the theory"[75] that the simplest means of ensuring that *opinio juris* is recognized is to place a "requirement that an objective claim of international legality be articulated in advance of, or concurrently with the act which will

---

68 *Id.* at 8-9.

69 Ian Brownlie, *Principles of Public International Law* 9 (7th ed. 2008).

70 Brownlie, *Id.*

71 Anthony A. D'Amato, *The Concept of Custom in International Law* 50 (1971).

72 *Id.* at 51.

73 *Id.* at 74.

74 *Id.* at 74-75.

75 *Id.*

constitute the quantitative elements of customs."[76] To support this idea, D'Amato cited Lon Fuller, who stated that articulation "is one of the most basic inherent requirements of any system of lawmaking. It is reflected in Art. 38 of the Statute of the International Court of Justice defining custom as evidence of general practice accepted as law."[77] By making states articulate their position before the act or concurrently with it, D'Amato believes this will "give a state notice that its action or decision will have legal implications."[78]

In addition, any act articulated by a state "must be a characterization of legality."[79] That is, the act must be distinguishable from other common acts such as "social habit, courtesy, comity, moral requirements, political expediency, plain usage, or any other norm."[80]

The ILA Reports provides two exceptions to this problem in that they allow states to utilize "disclaimers."[81] A state may disclaim its conduct so as to not give rise to the formation of custom that could eventually be used against it. Additionally, the ILA Reports holds that ambiguous conduct on behalf of a state will only give rise to custom "if there is positive evidence that the state or states concerned intended, understood, or accepted that a customary rule could result from, or lay behind the conduct in question."[82]

One issue with *opinio juris* is ascertaining whether the state is truly acting out of a sense of legal obligation or whether it is claiming legal cover for dubious actions. Given the varying interpretations concerning the role of *opinio juris*, it is impossible to know why a state undertakes any practice. In addition, the ILA Reports recognizes that even acts that may be deemed unlawful at the time of the act may eventually become legal through custom. This creates a circular argument. One must accept the fact that states will act in the manner they

---

76 *Id.* at 74.

77 *Id.* at 75.

78 *Id.*

79 D'Amato, *id.* at 76.

80 *Id.*

81 ILA Reports Art. 17 (iii).

82 *Id.* Art. 17 (iv) cmt. a-b.

deem best for themselves and then use legal maneuvers to make the act savory to the public at large. This fact lends credence to the argument that a state's action must be judged in toto, devoid of the spin and maneuvering that states may apply to convince the public at large.

The debate over the primacy of *opinio juris* is without a definitive answer. It is sufficient to recognize that there must be a belief on the part of a state that it is doing an act out of a sense of legal obligation or permissiveness to satisfy the *opinio juris* element. In the cyber context, discerning what constitutes *opinio juris* will rely greatly on the public acts and statements of a state, as other acts in cyberspace without proper attribution to a state cannot fulfill the *opinio juris* element. In respect to the examples discussed in Chapter One, the overt acts of the United States in regards to the Sony hack incident and the statements by the United States president would signify *opinio juris* in regards to the acts taken by the United States in retaliation to the alleged hacking by North Korea. In addition, the overt acts, or omissions, by the governments of Estonia, Georgia, and Iran, in response to the cyber-attacks on their cyber infrastructure may be seen as *opinio juris.*

2.3.2. Alternative Theories of Customary International Law Formation

The debate concerning the primacy of the elements for CIL has led to other theories concerning the formation of CIL. Two theories, Bin Cheng's "instant custom" and Fredric Kirgis's "sliding scale" deserve mentioning as they demonstrate alternative theories regarding the formation of CIL that have achieved some modicum of support from various commentators.[83] These theories are not without controversy as they lay at the edges of

83 *See, e.g.,* Benjamin Langille, *It's "Instant Custom": How the Bush Doctrine Became Law After the Terrorist Attacks of September 11, 2001*, 26 B.C. Int'l & Comp. L. Rev. 145 (2003). (Discussing the instant custom theory and applying it to the issue of the 9/11 attacks. Langille contends that in moments of overwhelming state acts, custom may be created in a compressed time span.) Jacob M. Harper, *Technology, Politics, and the New Space Race: The Legality and Desirability of Bush's National Space Policy Under the Public and Customary International Laws of Space,* 8 Chi. J. Int'l L. 681, 690-691 (2010). *But cf.,* Andrew T. Guzman, *Saving Customary International Law*, 27 Mich. J. Int'l L. 115, 157-159 (2006). (Discussing that custom needs some span of time to form.) *North Sea Continental Shelf* (Fed. R. Ger. v. Den., Fed. R. Ger. v. Neth.), 1969 I.C.J. 3, 43 ¶74 (Feb. 20). (Stating that custom needed some time to develop.) *See also*, Anthea Eizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 Am. J. Int'l L. 757 (2001). (Expanding on Kirgis's

international law and legal theory. They are discussed here to demonstrate the variety of thought by learned individuals on the subject and to demonstrate additional theories as to how custom may arise from the acts of states.

2.3.2.1. Instant Custom

Cheng posited perhaps one of the more controversial legal theories within the state practice – *opinio juris* debate. In 1965, in response to the UN resolutions on outer space,[84] Cheng posited that:

> the role of usage [(State practice)] in establishment of rules of international customary law is purely evidentiary; it provides evidence on the one hand of the contents of the rule in question and on the other hand of the *opinio juris* of the States concerned. Not only is it unnecessary that the usage should be prolonged, but there need also be no usage at all in the sense of repeated practice, provided that the *opinio juris* of the States concerned can be clearly established. Consequently, international customary law has in reality only one constitutive element, the *opinio juris*.[85]

Cheng based this theory, in part, on the idea that in international law, states create their own law.[86] In doing so, this law creation may come about due to each state agreeing to be bound,[87] and if states consent to be bound by their own will and belief, then they are bound without any need for state practice.[88] Although Cheng recognized that this agreement to be bound could only come about in rare instances such as the unanimous vote by the UNGA, this idea is interesting, as theoretically, CIL could spring forth in response to any external stimuli and the action of the UNGA.

---

theory in an attempt to reconcile the difference between traditional CIL formation and what is described as modern approaches or a deductive approach to CIL.)

84 *International Co-operation in the Peaceful Uses of Outer Space*, G.A. Res. 1721 (XVI), U.N. GAOR, 16th Sess., Annex., U.N. Doc. A/5026 (20 Dec. 1961); *Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Outer Space*, G.A. Res. 1962 (XVIII), U.N. GAOR, 18th Sess., U.N. Doc. A/5656 (13 Dec. 1963).

85 Bin Cheng, *United Nations Resolutions on Outer Space: "Instant" International Customary Law*, 5 Indian J. Int'l L. 23, 35 (1965).

86 I*d.* at 37.

87 *Id.*

88 *Id.*

Cheng recognized that UNGA resolutions in themselves did not constitute law. Cheng posited that "[m]ember states voting in favor of those resolutions of either law-finding or a fact-finding character may, on the basis of the principle of good faith, be prevented from denying the veracity of what is stated in the resolution."[89] To create law-finding resolutions, Cheng stated two requisite elements: first, the members of the UNGA must know "what they are enunciating in the resolution represents binding rules of international law."[90] The second element requires specificity of writings in that "the wording of the resolution must not merely identify clearly the contents of the rules in question, but most unequivocally express *opinio juris communis*."[91]

Cheng differentiated between what he terms *opinio juris generalis* and *opinio juris communis*. *Opinio juris generalis*, he contends, relates to that law of custom that develops on the municipal level and requires "general and usually prolonged practice"[92] to establish; whereas *opinio juris communis* may be understood as "the universal juridical conscience through the observance, by most of the members of the international community, of a determined practice because it is obligatory."[93]

If what Cheng posited is true, then it raises the possibility that a single overwhelming act by the international community on a single occasion may give rise to a near-instant custom based solely on the acts of states in response to single stimuli. That is, a single act with near universal consent and an overwhelming single incident of practice could give rise to CIL that would control future similar incidents.

However, Cheng's theory contradicts what the ICJ held in the *North Sea Continental Shelf cases*, which the ICJ put forth five years after Cheng posited his theory. The ICJ held that:

89 *Id.* at 39.

90 Cheng, *id.*

91 *Id.*

92 *Id.* at 37.

93 Baena Ricardo et al. Judgment, Inter-Am. Ct. H.R., (Ser. C) No. 104, ¶ 102 (November 28, 2003).

> [a]lthough the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law on the basis of what was originally a purely conventional rule, an indispensable requirement would be that within the period in question, short though it might be, State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked; and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved.[94]

The ICJ in the *North Sea Continental Shelf cases* were asked, in part, to determine the existence of CIL in relation to the equidistance principle relating to international boundaries as put forth by Denmark and the Netherlands. As such, the ICJ was well placed at that time to consider what elements were necessary for the formation of CIL and recognized that state practice was a necessary element for the formation of CIL.

However, Cheng's theory is not without some merit. Overwhelming acts by a majority of states may give rise to custom over a short period. Although this study believes that it is doubtful that custom would develop without some modicum of state practice, this theory is particularly attractive in emerging legal areas such as terrorism or cyber-attacks. However, Cheng's theory has not been widely accepted and is open to great controversy.

2.3.2.2. The Sliding Scale Theory of Customary International Law

Frederic L. Kirgis, Jr. put forth the theory of custom on a sliding scale,[95] in which he argued that the more of one constitutive element present; the less the other is needed in the formation of CIL.[96] Simply, the greater the presence of state practice, the less *opinio juris* that is needed to justify the formation of CIL or vice-versa. Kirgis did so, at least in part, based upon what he termed the "restrictive customary rules"[97] that the ICJ found in the *Nicaragua* decision and the seeming focus by the court on *opinio juris* rather than state

94 *North Sea Continental Shelf* (Fed. R. Ger. v. Den., Fed. R. Ger. v. Neth.), 1969 I.C.J. 3, 43 ¶74 (Feb. 20).

95 Frederic L. Kirgis, Jr., *Custom on a Sliding Scale*, 81 Am. J. Int'l L. 146 (1987).

96 *Id.*

97 *Id.* at 147.

practice.[98] Kirgis argued that "there is precedent for the converse: a focus on state practice without paying attention to governmental assertions and acquiescence that would establish an *opinio juris*."[99] Kirgis noted that this had been the case in several significant ICJ cases prior to *Nicaragua,* in which the court looked to state practice alone with little regard to *opinio juris*.[100] Kirgis contended that these acts by the court might be "reconciled…if one views the elements of custom not as fixed and mutually exclusive, but as interchangeable along a sliding scale."[101] The caveat is that the amount needed for either constitutive elements "depends on the activity in question and the reasonableness of the asserted customary rule… [and] the more destabilizing or morally distasteful the activity…The more readily international decision makers will substitute one element for the other, provided that the asserted restrictive rule seems reasonable."[102] Kirgis argued that the inverse is true in that the more morally tasteful the new rule is, the less the court will analyze its constitutive elements.

The major criticism of this theory is focused on the attempt by Kirgis to construct a theory to justify the court's holding in *Nicaragua,* a holding that has been thoroughly criticized by commentators.[103] Kirgis' theory, instead of clarifying the subjectivity of CIL, adds more guesswork for those attempting to discern *opinio juris.* Commentators and practitioners would be forced to delve into even more subjective areas to ascertain the reasonableness of the act, applying individual morality to a state's decision to take action.

Kirgis' theory raises an interesting question: could instant custom be equally applicable to those rare moments when states act in concert against a common problem without elucidating a clear statement as to the lawfulness of the action? One may argue that if instant

98 *Id.* at 148.

99 *Id.*

100 81 Am. J. Intl'l L. 146, 149. Ian Brownlie, *Principles of Public International Law* 9 (7th ed. 2008).

101 *Id.*

102 *Id.*

103 *See e.g.*, Anthony A. D'Amato, *Trashing International Law*, 81 Am. J. Int'l L. 101 (1987). (The decision in *Nicaragua* "reveals the judges of the World Court deciding the content of customary international law on a *tabula rasa*. Sadly, the judgment reveals that the judges have little idea about what they are doing…" at 101-102.)

custom is possibly based solely on the subjective belief of a majority of states, then it is also true that custom may lay in the instant acts of states working together against a common problem. This, however, is purely theoretical and not readily accepted in international law.

Kirgis' theory is particularly appealing when discussing the formation of CIL in regards to cyberspace, as state practice may be more easily discernable than *opinion juris*. Thus, allowing the formation of CIL by a demonstration of more state practice verse *opinio juris*.

2.3.3. Customary International Law: Analysis and Conclusion

This study will now turn to the topic of state responsibility in general and the ARS in particular, to gain an understanding of what state responsibility is and how it operates as a matter of law. As this study moves forward, it is important to keep in mind the question of how the problem of malicious cyber-attacks plays into and is impacted by CIL and how in turn the evolution of new CIL impacts the law of state responsibility. The questions may be broken down into two lines: whether CIL has been static, and new custom has not formed because of the technological advancements; or whether CIL has formed or is forming because of the technological advancements.

2.4. The Law of State Responsibility

This study now turns to the subject of state responsibility. Section 2.4 et seq. will discuss state responsibility in general and chapters three and four of this work will focus on both legal attribution and technical attribution respectively. This study begins the discussion on state responsibility with the caveat that any discussion concerning state responsibility may be complex and difficult. The law of state responsibility has been described by one commentator as "one of the most complex areas of international law…"[104] The source of this complexity lies, in part, on the fact that the basis of state responsibility is "largely

[104] James D. Fry, *Coercion, Causation, and the Fictional Elements of State Responsibility*, 40 Vand. J. Transnat'l L. 611, 612 (2007). *Cf. State Responsibility in International Law* 12 (Rene Provost ed., 2002). ("The law of state responsibility tends to be a complex field in which principles are articulated at a level of abstraction that obfuscates their theoretical underpinnings.")

theoretical."[105] As Aust[106] explained, "[t]he law of state responsibility is customary international law… state responsibility is pre-eminently an area of international law developed by state practice and international judgments…."[107] However, as discussed *supra*, due to the nature of cyberspace and the instant issue, identifying the development of CIL and its necessary components is difficult and subject to great debate thus subjecting the law of state responsibility to the same arguments concerning development and application as that of the identification of CIL. This study will utilize the work of the ILC to facilitate the discussion and in an attempt to avoid the majority of the controversies surrounding the application of the CIL of State responsibility. Thus study focuses on parts I-II of the ARS which are arguably the least controversial. The work of the ILC in the ARS is not a perfect fit for the issues addressed by this study, however, as will be discussed in section 2.4.1.1. This study will discuss general concepts of state responsibility in section 2.4.1. and then move to the ILC ARS in section 2.4.1.1. This study begins with the general concepts to assist the reader in understanding the general nature of state responsibility prior to delving into the specifics of the ARS and to emphasize the CIL nature of state responsibility.

2.4.1. State Responsibility in General

State responsibility is arguably one of the most important areas within public international law, James Crawford has called state responsibility the "cardinal institution of international law,"[108] state responsibility impacts all areas of international law to some extent. State responsibility is based upon the state's obligations in international law, as state's "are the principle bearers of international obligations."[109] It is a breach of a state's international

105 *Id.*

106 Anthony Aust, *Handbook of International Law* 407 (2007).

107 *Id.*

108 James Crawford, *State Responsibility*, Max Planck Encyclopedia of International Law (Sept. 2006).

109 *Id.*

obligations (norm) which gives rise to a state's responsibility. What constitutes a breach depends upon the obligation in question and depends upon the state itself. [110]

This study is narrowly tailored to address the issue of state responsibility and attribution of malicious cyber-attacks. This study addresses those malicious cyber-attacks that constitute internationally wrongful acts and thus are an internationally wrongful act. The emphasis of this study being how to attribute malicious cyber-attacks to a state. However, the rules of state responsibility, in general, must be understood to lay the proper foundation for understanding the rules and role of attribution for the purpose of state responsibility. This study will engage in a brief discussion regarding the general rules of state responsibility as a matter of both CIL and as put forth by the ILC in the ARS to ensure that the proper foundation for this study is established.

The idea of state responsibility has existed for as long as there have been states.[111] The ILC attempted to codify the existing CIL in the ARS as the ILC believed "it was important to do more than codify the law; it was "necessary to change and adapt traditional law so that it will reflect the profound transformation which has occurred in international law.... and to bring the 'principles governing State responsibility' into line with international law at its present stage of development."[112] The ILC's work, however, is a reflection of existing CIL as it was understood by its authors from its inception in 1953 to its completion in 2001. However, one failing of the ILC's work is that the ILC created a static representation of CIL which is forever evolving.

---

110 *Id*.

111 Edith Brown Weiss, *Invoking State Responsibility in the Twenty-First Century*, 96 Am. Soc. I'ntl L. 798, 798 (2002). ("The Peace of Westphalia more than 350 years ago led to the establishment of the classic system of international law, which centered exclusively on sovereign states that had defined territories and were theoretically equal. States made international law and were accountable to each other in meeting international legal obligations. The articles on state responsibility of the International Law Commission (ILC)5 largely reflect this traditional view of the international legal system. They focus on states and the rules they use to hold each other accountable for the substantive obligations to which they have committed themselves.")

112 *Id*. (Internal citations omitted).

It is, therefore, necessary to understand general theories of state responsibility which exist in the ILC's ARS but also as a matter of CIL standing alone. These theories will also be discussed when discussing the ARS and its specific handling of these general theories. This study does so to emphasize the nature of the CIL of state responsibility and to demonstrate that the theories discussed by the ILC ARS exist outside of the ARS standing alone. This study also wishes to emphasise that while the ILC has attempted to codify the CIL of state responsibility, the ARS is but one, albeit highly influential and important, writing on the subject.

The first general principle is that the responsibility of a state for an internationally wrongful act may be owed to another state, multiple states, or "international community as a whole."[113] As a general rule, international law engages states and their interactions with other states. Hence any violation of an international norm giving rise to state responsibility must be on the part of another state or states. In general, the individual non-state actor is not engaged in international law unless the individual actor is acting on behalf of the state as its agent or acting in a private manner but under the direction and control of the state so as to make it a virtual agent of the state. The exceptions to this general rule are put forth in the ARS in arts. two, four, eight, nine and 11 which are discussed infra, chapter three. These exceptions have come about as international tribunals have attempted to link acts of non-state actors to states to ensure that states do not have a mechanism to escape international responsibility by assigning state roles to non-state actors.[114] As a result of the actions by tribunals,and discussion in the contect of the ILC's work on state responsibility, these exceptions to the general rule are now considered part of the CIL of state responsibility.

Second, an internationally wrongful act may be an affirmative act or a failure to act by the state or its agents.[115] This general proposition holds a state responsible as a matter of CIL for those acts it affirmatively takes which violate an international norm but also holds a

113 A/RES/56/10 art. 33.

114 Oona A. Hathaway, et al., *Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors*, 95 Tex. L. Rev. 539, 545-547 (2017).

115 Gordon A. Christenson, *Attributing Acts of Omission to the State*, 23 Mich. J. Int'l L. 312 (1990).

state responsible for the actions it does not take, when the state has a duty to act and fails to do so.[116] An affirmative act on behalf of a state may be anything from conduct that fails comply with the provisions of an international treaty or an illegal use of force or a violation of CIL. An omission, however, may be a failure to control vigilantes, prevent pollution, stop terrorist acts, of preventing a state sanctioned execution when international norms have been violated.[117] Determining when an omission has occurred is a much more difficult proposition as a state may not necessarily be aware that it owed a duty of care to another state in which an omission occurred. It is important to recognize though for the purposes of this study that a state may accrue international responsibility either through an affirmative act or an omission.

It is important to note that the obligation a state owes to another state is not a static or uniform concept. Individual state's obligations to another state may depend upon factors specially impacting the state and which other states are not exposed to. In the cyber context, a state with a large, sophisticated cyber infrastructure and heavy reliance upon the Internet for all aspects of social, military, and government activity will be impacted differently than a state with minimum reliance on cyber infrastructure. A more sophisticated state might be required to do more under applicable due diligence obligations (e.g. the obligation to prevent harm) than a less sophisticated state. In addition, the more sophisticated and dependent the state is in regards to its cyber abilities, the more it is impacted by malicious cyber-attacks, the more its actions in regards to those cyber-attacks and its actions in regards to cyber related acts, in general, may form the basis for state practice and opinio juris over non-sophisticated states as international law will view the sophisticated state as a specially situated state, as was discussed supra.

Third, a state must affirmatively demonstrate that the accused state is responsible for the violation in question. This general principle of CIL seems simple prima facie that a state must demonstrate that the accused state is responsible for an act or omission in which the accused state violated its international obligation. This general principle is the source of

116 Ian Brownlie, 1 System of the Law of Nations State Responsibility 132-150 (1983).

117 *See*, Christenson, *supra* at 314.

some confusion in international law and questions of evidence or the weight of evidence needed to prove an act or omission or the involvement of relevant actors are not addressed by the ARS. This question is addressed in-depth in this study in sec. 3.6.2. et seq.

This study will now analyze the ILC ARS' general provisions regarding the basic principles of state responsibility found in Arts. 1 - 3 of the ILC ARS. This study will then turn to the issue of attribution of malicious cyber-attacks found in Arts. 4 to 11 in chapter three, infra.

2.4.1.1. The ILC's Work on State Responsibility

The ILC first began the study of state responsibility for codification in 1953[118] and finally submitted the ARS for consideration to the UNGA in 2001.[119] Even after the work of the ILC, the issues the ILC addressed are not, per se, settled, in that the ARS is a representation of the CIL at the time of the ILC's writing. While the ARS was being drafted, customs and warfare changed very little in international law. However, after the ARS was published in 2001, the ARS has seemingly become, ever so slightly, out of step with the changes in warfare and technology that happened after the ARS was submitted and approved by the UNGA.[120]

This non-digital distinction regarding the ARS is important as it may be argued that the ARS is representative of the CIL for kinetic, non-digital events, as it did not envision the digital world. This is not to say the ARS is inapplicable to the issues involving malicious cyber-attacks; this is to say that custom may have evolved with respect to malicious cyber-attacks for the purpose of state responsibility and attribution other than as posited in the ARS. When the ARS was submitted to the UNGA, only ~8% of the world population had Internet connectivity; as of June 2015, that number had risen to ~44%[121] and is expected to

118 A/RES/56/10 at 29 ¶ 30.

119 A/RES/56/10 at 42 ¶ 72.

120 U.N.G.A. res. 56/83 (12 Dec. 2001).

121 Internet Growth Statistics, *The Global Village Online* (15 Sept 2015), http://www.internetworldstats.com/emarketing.htm

grow exponentially in the coming years. As access to, and dependence upon, the Internet and cyberspace have grown, so has the state practice (and arguably the *opinio juris*) of states' acts in cyberspace. As such, custom may have sprung or is forming, concerning cyberspace since the UNGA approved the ARS.

It must be noted, in support of the above proposition, that the ARS is entirely a pre-cyber document with no reference to cyberspace, the Internet, information systems, information warfare, or even computers. However, the ARS is not alone in this distinction, the main judicial bodies for international law, the ICJ and the ICC, have not yet, as of writing, heard any cases involving cyber warfare, cyber-attacks, or any iteration thereof.

Moreover, international law is reactive. As Professor Michael Schmitt has said, "[l]aw tends to be reactive and responsive to factual context in which it operates. Obviously, this is the case for customary international law, which relies, *inter alia*, on state practice…"[122] This reactivity comes into play when events and technology outpace the evolution of the law, forcing the law to regulate ex-post facto. This creates a system of law which relies, in part, on the reactive nature of state practice, yet individual state practice changes as the state reacts to external threats and other stimuli, thus making its application to the issue of state responsibility for malicious cyber-attacks difficult, as states' practice varies; states themselves change practice depending upon the state they hold responsible for the accused cyber-attack. A prime example of this diverse handling of malicious cyber-attacks is the United States response to disparate cyber-attacks blamed upon Chinese hackers. The United States has sought to hold the purported Chinese hackers individually criminally liable, under domestic United States federal law,[123] and hold China as a state responsible in international law by applying sanctions against Chinese officials and state-owned corporations.[124] The United States practice, if it follows through with sanctions against

122 Michael N. Schmitt, *Counter Terrorism and the Use of Force*, 5 Marshal Center Papers 2 (2002). Mark A. Drumbl, *Pluralizing International Criminal Justice*, 103 Mich. L. Rev.1295, 1304 (2005).

123 Shane Harris, *U.S. Poised to Indict China's Hackers for Cyber Blitz*, The Daily Beast, Sept. 9, 2015, http://www.thedailybeast.com/articles/2015/09/09/u-s-poised-to-indict-china-s-hackers-for-cyber-blitz.html.

124 Ellen Nakashima, *U.S. Developing Sanctions Against China Over Cyberthefts*, Wash. Post, Aug. 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-

China, is seemingly at odds with the ILC's ARS, as no direct attribution of malicious cyber-attacks has been demonstrated to date.[125]

Lastly, prior to discussing the ILC's ARS, a general principle of the traditional understanding of state responsibility needs to be discussed. This traditional understanding of state responsibility is simple: a state is responsible for its own acts, the state's own nonfeasance, and the actions and nonfeasance of a state's agents. CIL has created exceptions, recognized by the ILC's ARS, to this rule through case law from the ICJ, tribunals, and arbitral decisions which, will be discussed infra. However, international law has recognized that due to evolving circumstances, this baseline of state responsibility may be expanded as a matter of international law as discussed previously. This applies to the issues discussed herein; as technology evolves so does the laws governing it.

It is these exceptions to the general rule which are of importance to this study. The difficulty is identifying the exceptions to the general rule and finding adequate legal support for the exceptions so as to argue that the exceptions apply to the issue of malicious cyber-attacks. To do this, this study, in Chapters Four through Seven, steps away from the ILC's ARS to identify and discuss applicable rules from other sources of international law and soft law, which, it is argued, assist in developing a framework for holding states responsible for cyber-attacks that originate from within their territory. It should be understood that these exceptions may exist in CIL without impacting the rules put forth in the ILC's ARS.

This study will turn now to discuss the regime of state responsibility as put forth in the ILC's ARS. This study utilizes the work of the ILC in the ARS as the ARS has been recognized as part of the corpus of CIL on state responsibility, particularly chapters I-II which this study relies upon. This study will, where necessary, go behind the work of the ILC and discuss germane ICJ case law to assist in the understanding of the instant issue.

---

sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

125 The United States is seemingly relying upon "circumstantial attribution" to attribute the cyber-attacks to China. *See*, Jason Healey, *Concluding Assessment* 273-278, in A Fierce Domain: Conflict in Cyberspace 1986 to 2012 (2013 Jason Healey ed.) (Discussing circumstantial attribution for cyber-attacks.)

It is important to note that the ILC's ARS posits general secondary rules for state responsibility. The ILC's ARS does not discuss the primary rules or the evidence needed to show a violation thereof. This means that one needs to identify the primary norm being violated and discern how the violation occurred and what evidence is needed to prove the same. Once these elements are met, then the secondary rules of state responsibility are engaged. This precluded the ILC from having to address the multitude of disparate primary norms and their standards of proof. It should be noted that a single incident, particularly in the cyber context, may violate a multitude of primary norms. As such, each norm standing on its own should be analyzed independently, and the secondary rules of state responsibility applied after one discerns the needed rules of proof and violation thereof for the specific primary norm.

This chapter will begin with a general discussion on the ARS and state responsibility. Once this study completes its discussion concerning the general principles of state responsibility, this study will move to an in-depth discussion on attribution and technical attribution in chapters three and four.

2.4.1.2. The Draft Articles on Responsibility for Internationally Wrongful Acts: General Provisions on State Responsibility

The ILC's ARS Chapter I sets forth two principles: (1) that states may be responsible for internationally wrongful acts and (2) the superiority of international law. The ARS elements are accepted *arguendo,* as no contrary position has been found for the purposes of this study. The ILC ARS Art. 1, "states the basic principle underlying the articles as a whole…"[126] Art. 1 holds that "[e]very internationally wrongful act of a state entails the international responsibility of that state."[127] ARS Art. 1 establishes a "basic principle"[128] that carries throughout the principles of state responsibility. This, in turn, means that for a

126 A/RES/56/10 Art. 1, cmt. 1.

127 A/RES/56/10 Art. 1.

128 G.A. Res. 56/83 Art. 1, cmt. 1, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001). ("Article 1 states the basic principle underlying the articles as a whole, which is that a breach of international law by a State entails its international responsibility...")

state to be held responsible for cyber-attacks, those cyber-attacks must violate international law, i.e., those cyber-attacks must constitute an internationally wrongful act.

The commentary to Art. 1 establishes that:

> An internationally wrongful act of a state may consist of one or more actions or omissions or a combination of both. Whether there has been an internationally wrongful act depends, first, on the requirements of the obligation which is said to have been breached and, secondly, on the framework conditions for such an act…[129]

This raises the first issue that this study needs to address, under what circumstances and what type of attacks, constitute an internationally wrongful act as required by Art. 1 of the ARS. This issue is addressed in section 2.4.3. of this study and in chapters five through seven herein. It is posited for the purposes of this section that a cyber-attack is an internationally wrongful act when a cyber-attack violates international law. To wit, when a state acts in a manner inconsistent with international law and utilizes cyberspace to commit an internationally wrongful act, that wrongful act engages the offending state for the purposes of state responsibility. This proposition is supported by Rule 6 of the *Tallinn Manual*, which holds that "[a] state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[130] However, not every cyber-attack will rise to the level of an internationally wrongful act e.g., certain acts of cyber-espionage may not violate international law. Just because an act happens in cyberspace does not instantly make the act unlawful, if that act does not violate international law in the kinetic realm it may not violate international law because it is in the cyber realm. Those cyber-attacks which rise to the level of an internationally wrongful act may be a violation of an international obligation, a violation of the UN Charter, a violation of international humanitarian law, a violation of *jus cogens* norms, etc.

This is explored in-depth infra sect. 2.4.1.3.

Not every malicious act in cyber-space will engage a state for the purposes of state responsibility. De minimis attacks, those attacks which are not enough to engage the state

---

129 *Id*. cmt. 1.

130 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, R.6, p.29 (Michael N. Schmitt ed. 2013).

itself or do not constitute a harm to a state, will be an issue for a state's domestic law. If the cyber-attack fails to engage international law, it is a matter not covered by the ILC or this study. However, a series of de minimis attacks may eventually progress to the point where the incidents in toto amount to a violation of international law which engages the state. Such attacks may take a variety of forms such as cyber-vandalism, prolonged spam campaigns, small-scale continuous DDoS attacks, etc. It is up to the injured state to determine when such incidents bloom into a violation of international law and then demonstrate as such.

Lastly, in respect to an internationally wrongful act, an internationally wrongful act arises against another state "immediately between the two states…"[131] That is, as soon as a state commits an internationally wrongful act against another state. International Courts and Tribunals have repeatedly stressed this fact,[132] the arbitrators in the Rainbow Warrior case held that "any violation by a state of any obligation, of whatever origin give rise to state responsibility…"[133] this state responsibility blooms upon the violation of the obligation in question. So, in respect to the instant issue, state responsibility blooms as soon as the malicious cyber-attack violates a state's international obligation.

The ILC's ARS establishes that in addition to the existence of an internationally wrongful act, the wrongful act must be attributable to the state accused of the internationally wrongful act. Art. 2 of the ARS states that "[t]here is an internationally wrongful act of a state when conduct consisting of an action or omission: (a) is attributable to the state under international law; and (b) constitutes a breach of an international obligation of the state."[134]

131 A/RES/56/10 Part I, cmt. 2, citing, Phosphates in Morocco, Judgment, 1938, P.C.I.J., Series A/B, No. 74 p. 10, at p. 28

132 A/RES/56/10 Part I, cmt. 2.

133 Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair, XX Rep. Int'l Arbitral Awards 215 (30 Apr. 1990).

134 A/RES/56/10 Art.2.

Where Art. 1 establishes that international responsibility begins with a state's wrongful act, Art. 2 establishes that an internationally wrongful act is composed of two distinct elements, attribution and a breach of international law consisting of an act or omission. This means, for example, that in the case of malicious cyber-attacks, an internationally wrongful act may consist of a state initiating a malicious cyber-attack or failing to stop a malicious cyber-attack that it has knowledge of. Traditionally, under the ILC, this conduct by the state must be an act by the state or its agents or acts on behalf of the state by a non-state actor or agent, where the non-state actors act as virtual agents of the state (as will be discussed infra) or be conduct that the state "adopts" after the act.[135] The act or omission must be violative of an existing international obligation, that is, that a state may not be held responsible ex-post facto for acting in a manner inconsistent with a future obligation.[136] Attribution is discussed in-depth infra chapters three and four. It is important to note that attribution is in the opinion of this study the keystone to state responsibility for malicious cyber-attacks. As is discussed infra, attribution of malicious cyber-attacks is difficult, if not impossible, due to numerous factors explored in chapter three and four.

This study will argue that true attribution of malicious cyber-attacks is virtually impossible given the current state of cyberspace and the technology utilized therein. While some argue that attribution is getting easier, this study will argue that due to the focus on attribution by states and their internal law enforcement and security apparatus, attribution is actually getting more difficult. This difficulty stems from the fact that until recently, those engaging in cyber-attacks for whatever reason did not have to worry about those attacks being attributed back to the originating actor as the technology to do so was lagging. However, with the advent of new technology which may assist in technical attribution, malicious actors and authors are now actively working to thwart attribution. Something that has not necessarily been true in the past. This focus by malicious actors in making their malicious code untraceable is adding a new dimension to the issue of attribution.

In addition, state responsibility requires that attribution be such as to directly link the alleged internationally wrongful act to the state or the state's agent. Computer systems are

135 A/Res/56/10 Art. 11.

136 A/RES/56/10 Art.2. cmt. 1.

such as to make this link virtually impossible to demonstrate. Under existing rules of attribution, a victim of malicious cyber-attack must demonstrate that the state or its agent initiated or authored the malicious cyber-attack. This study posits that such a linkage is virtually impossible in the cyber domain as establishing such a linkage would require the injured state to have the computer(s) utilized to author or initiate the cyber-attack or evidence of a state agent initiating the attack, such as the state agent executing the code to initiate the attack. The rules of state responsibility were established when direct evidence of another state's internationally wrongful act was relatively easy to establish. It is one thing to demonstrate that another state's military forces present unlawfully on another state's sovereign territory, but it is entirely different to establish that a state's cyber infrastructure was attacked by another state.

Art. 3 of the ARS establishes the supremacy of international law when defining an internationally wrongful act. Art. 3 holds that "[t]he characterization of an act of a state as internationally wrongful is governed by international law. Such characterization is not affected by the characterization of the same act as lawful by internal law."[137] Art. 3 eliminates the defense by states that their actions are legal under domestic law and therefore no state responsibility could apply. This idea, while accepted in international law since the early 1900s,[138] has been reinforced by the ICJ in post-ARS cases such as the case concerning *Avena and Other Mexican Nationals* (Mex. v. U.S.),[139] which found the United States had committed an internationally wrongful act for an individual domestic state (Texas), breaching Art. 36 of the Vienna Convention by not promptly notifying the Mexican consulates of the arrest of Mexican citizens. The acts by Texas did not violate domestic state law but did violate international law.[140] Therefore, the focus for determining

137 A/RES/56/10 Art.3.

138 A/RES/56/10 Art.3, cmts. 1-9.

139 *Avena and Other Mexican Nationals* (Mex. v. U.S.A), Judgment, 2004 I.C.J. Rep. 12.

140 The United States Supreme Court later found that the *Avena* decision was not directly enforceable on individual states within the United States due to domestic law. This created a paradox for the federal government of the United States where the United States was bound by international law but due to domestic constitutional law of the United States, could not force individual states to act in accordance on issues of a purely internal state question even though it potentially violated international law. *See*, *Medellín v. Texas*, 552 U.S. 491 (2008).

the legality of an international act is international law. This is important to bear in mind as states may interpret the legality of actions in cyberspace differently with the primary focus on domestic laws. Hence, states may be less likely to act against non-state actors within their domestic territory if the act is not a violation of domestic law.

Finally, it must be understood that the internationally wrongful acts posited in the ARS are not addressed either subjectively or objectively by the ARS. The act itself is addressed through the lens of international law as such an internationally wrongful act may be objectively or subjectively measured depending upon the violation claimed.

2.4.1.3. Cyber-Attacks as Internationally Wrongful Acts

As discussed above, an internationally wrongful act arises whenever a state breaches an international obligation. What constitutes an internationally wrongful act is dependent upon the primary international obligation violated. This would appear straightforward in most circumstances, e.g., illegal use of force is an internationally wrongful act because it violates U.N. Charter Art. 2(4).. A kinetic use of force is relatively easy to quantify when conducted by elements of a state. Evidence of one state invading another state is usually straightforward and easy to demonstrate. Other kinetic harms such as damage done to crops by airborne pollution may not be as easy to demonstrate, but may be proven through scientific observation and common sense and thus holding one state responsible for the harm is a relatively easy process as demonstrated by the *Trail Smelter* arbitration.[141]

An internationally wrongful act consists of a violation of "treaty or non-treaty obligations…"[142] The breadth of which includes "any violation by a state of any obligation…"[143] and includes "non-execution of international obligations…acts

141 In addition to scientific evidence considered by *Trail Smelter*, one could hypothesize that the common law rule of *res ipsa loquitur* could apply in some circumstances of attribution of wrongful conduct. *Res ipsa loquitur* "the thing speaks for itself" may apply in attribution when, as in *Trail Smelter*, there is only one legally and scientifically possible source of the harm.

142 A/Res/56/10 Art 2. cmt. 7.

143 *Id.*

incompatible with international obligations…violation of an international obligation…or breach of an engagement."[144]

The *Tallinn Manual,* in the comments to Rule 6 advances that:

> [i]n the realm of cyberspace, an internationally wrongful act can consist of, *inter alia*, a violation of the United Nations Charter…or a violation of a law of armed conflict obligation…[or] [a] breach of peacetime rules not involving conflict…[145]

As the *Tallinn Manual* is concerned with the issues surrounding cyber-attacks and the use of force, it is necessary to look beyond it to ascertain how malicious cyber-attacks fall within the purview of international law and how cyber-attacks may be considered an internationally wrongful act. As internationally wrongful acts spring from the CIL or treaty violated, it is not possible to address all the potential means of creating an internationally wrongful act via malicious cyber-attacks. However, this study will propose a general rule for internationally wrongful acts premised upon the unlawful harm inflicted by a state's action upon another state. A malicious cyber-attack standing alone may violate international law, or a series of de minimis attacks may collectively violate international law if those attacks either singularly or collectively rise to the level of an internationally wrongful act. The malicious cyber-attack standing alone may not be unlawful per se, but the harm caused by the malicious cyber-attack creates the internationally wrongful act; i.e., the intrusion upon a state's cyber infrastructure in itself may not be an internationally wrongful act, but the harm caused after the intrusion by malware or other act resulting in harm may be of such a magnitude in itself to be an internationally wrongful act.

This study puts forward three theories regarding malicious cyber-attacks as internationally wrongful acts:

1. The general duty of a state to not allow its territory to be utilized to the detriment of

---

144 *Id.,* citing, *Reparation for Injuries Suffered in the Service of the United Nations*, Advisory Opinion, 1949 I.C.J. Rep. 174, 184.

145 *Tallinn Manual on the International Law Applicable to Cyber Warfare* R.6, cmt. 3 (Michael N. Schmitt ed. 2013). (Internal parentheticals omitted).

another state, as put forth in the *Trail Smelter* arbitration, as recognized by the ICJ in the *Corfu Channel* case, and recognized as a general principle of international law.

2. The theory of strict liability for ultra-hazardous activities is applied to such activities as space launches, oil transportation, and nuclear reactor operation, and may also apply to malicious cyber-attacks as states may be under notice of the potential harm resulting from malicious cyber-attacks originating from within their sovereign territory.

3. The theory that malicious cyber-attacks may violate the principle concerning the duty not to intervene in matters within the domestic jurisdiction of any state and the principle of sovereign equality of states (collectively "unlawful political intervention") as stated in the *Declaration on Principles of International Law concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations*.[146] These theories are utilized to illustrate how the two above posited theories may apply.

This study does not hold that the theories posited above are the only CIL prohibitions that may be available to states to demonstrate malicious cyber-attacks as internationally wrongful acts. This study presents these theories as a means to demonstrate the depth of CIL available to states as a method to combat malicious cyber-attacks through the international law framework, thus minimizing the risk of kinetic overflow. This study does not address potential treaty law violations or IHL violations. These areas within themselves are subjects of scholarly debate and are worthy of individual, in-depth study, standing alone. This study seeks to demonstrate how CIL may be utilized as an effective and timely tool for holding states responsible for malicious cyber-attacks originating from within their sovereign territory.[147]

---

146 U.N.G.A. Res 2625, U.N. Doc. A/Res/25/2625 (24 Oct. 1970). *See also*, U.N. Charter Art. 2(1).

147 *See e.g.*, Oona Hathaway et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817-885 (2012). (Discussing the application of international treaty law, domestic state law, and the law of war to the issue of cyber-attacks.) *See also*, Michael Gervais, *Cyber Attacks and the Laws of War* (2011). https://ssrn.com/abstract=1939615.) Rex Hughes, *A Treaty for Cyberspace*, 86 Int'l Aff. 523 (2010). (Discussing the need for a cyber treaty after the cyber-attacks on Estonia.) Jeffrey T. G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 Mich. L. Rev. 1427 (2008). (Discussing the application of IHL to the issue of malicious cyber-attacks.)

The importance of utilizing CIL to define an internationally wrongful act may be demonstrated by the recent agreement between the United States and China[148] to prohibit economic espionage via cyberspace between the state parties.[149] Espionage, per se, is not prohibited by CIL,[150] nor has economic espionage fallen within the purview of international law. However, China and the United States recently entered into a bilateral agreement making economic espionage a wrongful act between the parties. By agreeing that economic espionage is a wrongful act, China and the United States may be creating new CIL that may bind parties not subject to the agreement. While it is too early to claim that economic espionage, as it currently stands, is an internationally wrongful act, economic espionage may rapidly become a violation of CIL if other states ascribe to the belief and practice, as custom may form as discussed *supra*.

2.5. Conclusion

State responsibility has evolved through the CIL process and is still evolving despite the attempts to codify it by the ILC. The evolution of state responsibility is a positive though as it allows the CIL of state responsibility to adapt to changing norms and technology. The issue of state responsibility for malicious cyber-attacks is such an event which challenges existing CIL and the rules of state responsibility. Malicious cyber-attacks are covered by both the CIL of state responsibility and the codified rules put forth by the ILC. However,

148 Kim Zetter, *US and China Reach Historic Agreement on Economic Espionage*, Wired (Sept. 25, 2015), http://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/. (US President Barack Obama stated: we [China and the United States] have agreed that neither the US or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. We'll work together and with other nations to promote other rules of the road.)

149 Ellen Nakashima, *The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace*, Wash. Post. (Sep. 25, 2015), https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9edce8a2a2a679_story.html?Wpisrc=al_alert-COMBO-world%252Bnation. Comments of President Barack Obama, *Joint Press Conference by President Barack Obama of the United States and President Xi Jinping of China* (25 Sep. 2015), http://www.cctv-america.com/2015/09/25/full-text-of-presidents-obama-and-xis-joint-press-conference-during-state-visit.

150 *But Cf.*, Russell Buchan, *Cyber Espionage and International Law, in*, Research Handbook on International Law and Cyberspace (Nicholas Tsagourias & Russell Buchan eds., 2015). (Buchan argued that cyber-espionage is an internationally wrongful act but acknowledges that the matter is not settled.)

this study argues that such a fit is far from perfect and leaves too many gaps for states or non-state actors to exploit. As such this study set out the basis for state responsibility in general and demonstrated how a malicious cyber-attack is an internationally wrongful act. However, the theories regarding malicious cyber-attacks as an internationally wrongful act as posited by this study are not the only means to ascertain state responsibility for malicious cyber-attacks. To paraphrase the ILC, any internationally wrongful act on behalf of a state gives rise to the states international responsibility.[151] Therefore, there are multiple ways in which a malicious cyber-attack may incur the international responsibility of the state from which it was initiated. This study selects three for reference and discussion.

As discussed supra, an internationally wrongful act is any breach on behalf of a state of the state's international obligation. The second element of an internationally wrongful act is that the act is attributed to the state. This issue, that of attribution is discussed infra chapters three and four. A breach may be an affirmative act or an omission. It is up to the injured state to determine when a breach has occurred. Such determination may be through objective or subjective means and is based on the international norm in question. A state's internal domestic law plays no role in the determination. At its simplest, a malicious cyber-attack may breach an international obligation by either being an affirmative act by the state (initiating an attack) or by an omission (not preventing an attack). Each state will be impacted differently and as such the state remains the arbitrator for the determination.

It is important to remember that while the ILC ARS is a pre-cyber document and is not, in the opinion of this study, a good fit for determining state responsibility for malicious cyber-attacks; the ILC ARS is still the baseline for discussion and determination of state responsibility. This study relies in great part on Chapters I-II of the ARS for discussion and application. However, this study seeks to go beyond the ILC ARS and posit original and creative methods for determining state responsibility for malicious cyber-attacks and attribution thereof.

Lastly, state responsibility may not lie without proper attribution. In the opinion of this study, the issue of attribution is arguably the most vexing issue facing the international

151 A/Res/56/10 Part 1, cmt. 3.

community with respect to state responsibility for malicious cyber-attacks. This study will now turn to the issue of attributing malicious cyber-attacks to the responsible state. This issue is explored in-depth infra chapters three and four.

Chapter Three: Attribution of Malicious Cyber-Attacks and Questions of Evidence

3. Introduction

This study now turns to the first issue of legal attribution for the purposes of state responsibility. This study divides attribution of malicious cyber-attacks into two separate but interrelated issues. First is the issue addressed in this chapter, that of legal attribution; the second interrelated issue is that of technical attribution, which will be addressed in Chapter Four. This study addresses these issues individually as the attribution of malicious cyber-attacks depends upon both types of attribution to establish state responsibility. This chapter will begin with a discussion regarding the issue of legal attribution in general as put forth by the ARS. This chapter will then address issues regarding the burden of proof associated with legal attribution of malicious cyber-attacks and the burden of proof for theories put forth in this study.

Malicious cyber-attacks present unique issues in both legal attribution and technical attribution. Malicious cyber-attacks are difficult to link to the authors responsible for the attack and even more difficult to prove the authorship and responsibility therefor.[1] There are several pertinent factors that impact the legal and technical attribution of malicious cyber-attacks:

1. The volume of malicious cyber tools, the variety of attack payloads (malicious code), and attack vectors. An estimated 225,000 new malware strains are discovered each day.[2]
2. Malicious cyber-attacks may be launched from any Internet-connected machine in the world, and as will be discussed in Chapter Four, numerous methods and techniques are

---

1 Neil C. Rowe, *The Attribution of Cyber Warfare*, in, Cyber Warfare: A Multidisciplinary Analysis 61-72 (James A. Green ed., 2015).

2 Panda Security, *Panda Security Detects Over 225,000 New Malware Strains Per Day in the First Quarter of the Year*, May 28, 2015, http://www.pandasecurity.com/mediacenter/press-releases/panda-security-detects-over-225000-new-malware-strains-per-day-in-the-first-quarter-of-the-year/. (Please note that the estimated number of malware strains discovered vary greatly between researchers.)

available to disguise the launch location. In addition, attacks may be transmitted without an Internet connection.[3]

3. The attack payload of malicious cyber-attacks, composed solely of computer code, may not have any information that will identify the author or the author's location, unlike those found in kinetic attacks.[4] In addition, the computer code utilized in the attack payload may be written in such a way as to lay a false trail of attribution to an innocent actor. Malicious payloads may also be reutilized by numerous distinct actors with relative ease.[5]
4. Malicious cyber-attack payloads may linger for months to years on an infected system waiting to be activated remotely or upon a specific date, time, or event.[6]
5. There is a high degree of crossover of malicious payloads; that is, the tools utilized in various types of attacks may be re-used for different attacks.[7]
6. A majority of the evidence gathered in a malicious cyber-attack will be circumstantial in nature and will not normally meet the evidentiary burden, discussed *infra*, needed for the legal attribution of state responsibility.[8]
7. The need to show that a state had effective control over the non-state or state actors responsible for a malicious cyber-attack in order for state responsibility to lie, is an almost unachievable evidentiary burden for a state injured by malicious cyber-attacks.

The "attribution problem,"[9] as many commentators refer to it, is one of the most difficult issues to overcome with regard to establishing state responsibility for malicious cyber-

---

3 Rowe, *id*. at 62.

4 *Id.*

5 *See*, *infra*, ch. 4.

6 *Id.*

7 *Id.*

8 *Id.*

9 David D. Clark and Susan Landau, *Untangling Attribution*, 25 Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010). *See also*, Robert K. Knake, *Untangling Attribution: Moving to Accountability in Cyberspace*, Subcommittee on Technology and Innovation, Committee on Science and Technology, United States House of Representatives 2nd Session, 111th Congress (July 15, 2010); Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council Issue Brief (2011).

attacks. As explained in Chapter One, this study argues that due to the nature of the existing CIL requirements for legal attribution to the state and the need to show that a state has effective control over any non-state actors behind a cyber-attack, legal attribution for malicious cyber-attacks fails as a matter of CIL. This failure is based upon both legal and technical issues. The existing limits on technical attribution make attributing cyber-attacks to the responsible actor difficult, if not impossible; and the evidentiary burden imposed by CIL makes it nearly impossible to hold states accountable for state malicious acts in cyberspace. Due to the technical limitations of computer science, legal attribution for malicious cyber-attacks is virtually impossible; and when possible, it is labor intensive and time-consuming. Even when there is sufficient technical data to attribute a malicious cyber-attack to a state, the legal requirements for attribution are such as to make it virtually impossible to link a state to a malicious cyber-attack to establish state responsibility.

This issue concerning the attribution problem is present in the examples discussed in Chapter One. To date, of the selected attacks discussed in Chapter One, only the Sony hack has been "attributed" to a state; the United States publicly held that North Korea was responsible. The veracity of this attribution has been highly debated by both technical and legal commentators.[10] Professor Jack Goldsmith stated that "[o]ne hears a lot in cybersecurity circles that the [U.S.] government has 'solved' the attribution problem. The evidence presented today (concerning the attribution of the Sony hack) shows why it has not come close to solving it."[11] Again, it must be noted that no scholarly article or technical brief has demonstrated adequate attribution of any malicious cyber-attack to a state, nor has

---

10 Kim Zetter, *The Evidence That North Korea Hacked Sony Is Flimsy*, Wired (Dec. 17, 2014), https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/ (Discussing the lack of evidence for the attacks and stating:

> Attribution in breaches is difficult. Assertions about who is behind any attack should be treated with a hefty dose of skepticism. Skilled hackers use proxy machines and false IP addresses to cover their tracks or plant false clues inside their malware to throw investigators off their trail. When hackers *are* identified and apprehended, it's generally because they've made mistakes or because a cohort got arrested and turned informant. Nation-state attacks often can be distinguished by their level of sophistication and modus operandi, but attribution is no less difficult… And even when an attack appears to be nation-state, it can be difficult to know if the hackers are mercenaries acting alone or with state sponsorship...)

11 Jack Goldsmith, *The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance*, LAWFARE (Dec. 19, 2014), https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance.

any international tribunal held a state responsible for any type of malicious cyber-attack. The attribution of the Sony hack to North Korea is more likely a product of circumstantial attribution, a combination of intelligence gathering, computer traceback techniques, computer forensics, and guesswork. As of this writing, no evidence has been produced by the United States to link North Korea to the Sony hack,[12] nor has the United States demonstrated that North Korea had effective control over those alleged to have committed the hacks or other malicious acts against Sony.

Therefore, this study argues that international law needs a mechanism for state responsibility that recognizes the deficiencies of technical attribution and fills the void as to prevent states from freely utilizing cyber-attacks in violation of international law.

This chapter will engage in a general discussion regarding legal attribution for malicious cyber-attacks for the purpose of state responsibility, with a specific focus on two issues: (1) which are the applicable primary rules, and (2) how the ILC framework for attribution applies to the issue of malicious cyber-attacks.

This study argues that a state may be implicated through either an act or omission when the state or its agent participates in malicious cyber-attacks against another state; or for omissions on behalf of the state, in not taking the steps necessary to stop its cyber territory from being utilized for malicious cyber-attacks.[13] This study also addresses the issue of non-state actors which utilize a state's domestic cyberinfrastructure to facilitate or launch malicious cyber-attacks. This study argues that the issue concerning state responsibility for hacktivists/proxies is one of particular importance of which the CIL does not adequately address. Both of these issues, that of attributing malicious cyber-attacks to a state and that of attributing the conduct of a non-state actor to a state, will be discussed herein.

---

12 *Id.*

13 International Law Commission, *Draft Articles of Responsibility of States for International Wrongful Acts*, art.2, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001). *See also*, Luigi Condorelli and Claus Kress, *The Rules of Attribution: General Considerations*, *in* The Law of International Responsibility 221 (James Crawford, Alain Pellet, and Simon Olleson ed. 2010).

The legal attribution of malicious cyber-attacks is a complex problem. The legal paradigm for attribution and state responsibility has developed through the CIL process. As the CIL for attribution was developed, the theory of attribution was based upon a mode of governing and warfare that may still exist in part but does not accurately reflect the modern means of conducting warfare or that of governing states.[14] States have evolved and embraced the digital age as a means of facilitating governance, delivering state services, conducting warfare, conducting espionage and asymmetric warfare, and as an adjunct to traditional warfare. However, the ILC, ARS, and CIL, in general, still operate based on a pre-cyber age understanding of attribution and state responsibility.

As the cyber-age, has developed, states have embraced the reality that patriot hackers/hacktivists and proxies are useful tools to conduct malicious cyber-attacks, as was alleged in both the Estonia and Georgia cyber-attacks. The use of proxies to conduct malicious cyber-attacks that are not attributable to the states under customary rules of state responsibility creates a means for states to act without potential repercussions due to the inability to attribute such cyber-attacks to the state. This inability to attribute malicious cyber-attacks has resulted, in part, from the slow adaptation of CIL regarding attribution in the cyber age. This slow adaptation process has left a legal framework which is ill-suited for dealing with the issues related to state responsibility for malicious cyber-attacks. To put it bluntly, states under the existing ARS cannot be held responsible for cyber-attacks, as direct technical attribution to the state is virtually impossible; the existing paradigm for legal attribution does not take into account the reality of technical attribution, and the effective control test discussed *infra* creates a bar to state responsibility for malicious cyber-attacks initiated either by the state or its proxies. Accordingly, the ability to legally attribute any form of cyber-attacks to a state without a "smoking gun"[15] is difficult at best and impossible at worst.

---

14 *Cf*. Michael C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 422, 440-448 (2011).

15 "Incontrovertible incrimination." William Safire, *The Way We Live Now: On Language: Smoking Gun*, New York Times, January 26, 2003, http://www.nytimes.com/2003/01/26/magazine/the-way-we-live-now-1-26-03-on-language-smoking-gun.html.

Attribution of wrongful conduct is the cornerstone of state responsibility. It is axiomatic that without attribution there can be no state responsibility. As a general rule, under the existing CIL of state responsibility, only those acts of a state or its agents (with certain narrow exceptions) are attributable to a state.[16] However, the ARS recognizes that "[i]n theory, the conduct of all human beings, corporations or collectivities linked to the state by nationality, habitual residence or incorporation might be attributed to the state, whether or not they have any connection to the Government."[17] However, such a theory of attribution has not been adopted in modern times[18] and has not been implemented due to policy considerations.

Another aspect of attribution that needs to be addressed is the proof needed to link the responsible party to the state and the state to the internationally wrongful conduct in international law. The ARS avoids discussion of proof and evidence.[19] The ARS focuses on the theory of attribution while ignoring the realities of attribution. In addition, international tribunals have laid down "generic rules"[20] for the standards applied for the burden of proof with regard to justifying the use of force.[21] This study will address the issue of attributing malicious cyber-attacks to a state, attributing the acts of non-state actors to a

16 International Law Commission, *Draft Articles of Responsibility of States for International Wrongful Acts*, arts. 2-10, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

17 ARS, Ch.2, cmt. 2.

18 Jan Arno Hessbruegge, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. Int'l L. & Pol. 265 (2003-2004). *See also*, Lassa Oppenheim, *International Law: A Treatise* vol. 2 § 164, p. 262 (Kindle ed. 2010) (Discussing state responsibility for private individuals).

19 International Law Commission, *Draft Articles of Responsibility of States for International Wrongful Acts*, Ch. III, cmts. 2 - 4, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001) ("Questions of evidence and proof of [ ] a breach of an international obligation fall entirely outside the scope of the [ARS].").

20 *Cf*. Nicholas Tsagourias, *Cyber-attacks, Self-Defence and the Problem of Attribution*, 17 J. Conflict & Security L. 234 (2012) ("International law does not lay down any specific standards of evidence with regard to issues involving the use of force or self-defence. The only generic threshold that perhaps exists is that 'claims against a State involving charges of exceptional gravity must be proved by evidence that is fully conclusive. The same standard applies to the proof of attribution for such acts.")

21 *Id.*

state, and the burden of proof in attribution. It will also attempt to discern the quantum of proof needed to link a state to cyber-attacks.

3.1. Attribution v. Imputability

Prior to delving into the grist of the instant issue, a brief discussion concerning the terminology utilized by the ARS is necessary. When the ARS discusses attribution, attribution does not necessarily mean imputability or vice versa. However, the terms should not create confusion as they both operate within the legal framework posited. The argument concerning the choice of term is largely academic. Brownlie posited that attribution should not be confused with imputability as the "major issue in any given situation is whether there has been a breach of duty: the content of imputability will vary according to the particular duty, the nature of the breach, and so on."[22] To support this proposition, Brownlie cited the second report of the ILC concerning the progress of codification of the CIL of state responsibility by Robert Ago, in which Ago discusses Anzilotti's work and definition regarding imputability versus attribution. In pertinent part, Anzilotti equated imputability to simply linking the wrongful act to the actions or omission of a state.[23] As Brownlie put it, "[t]o speak of imputation to a state, therefore, merely indicates that the international legal order must be able to regard the action or omission concerned as an act of the state."[24] Based upon the scholarship on the topic and at a base level, there is very little difference between the two terms. However, the debate was carried over into the final version of the ARS.

While Ago's version of the ARS differs significantly from Crawford's final version of the ARS, the distinction between imputability and attribution is carried into the final version of the ARS with the ARS seemingly adopting Brownlie's argument that the focus is on the determination of whether the wrongful act was that of a state.[25] In addition, the ILC adopted

---

22 Ian Brownlie, *System of the Law of Nations State Responsibility (Part I)* 36 (1983).

23 *Id.* at 37.

24 *Id.*

25 Ian Brownlie, *System of the Law of Nations State Responsibility (Part I)* 36 (1983). International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts,* ch.

the term attribution versus imputation "in order to avoid any suggestion that the legal operation of connecting conduct to the state involved a kind of fiction."[26] However, the terminology does not necessarily have any impact on the operation of the legal theory of linking a wrongful act to a state irrespective of the academic arguments put forth in favor of one term or another.[27] This debate, however, is presented, in part, to demonstrate the continued scholarly debate concerning almost every facet of the ARS and its representation of custom.

Attribution under the ARS has been described as a restrictive normative process in which attribution operates as a matter of law but not fact.[28] This idea that attribution is not based upon the fact of the matter has resulted in much academic debate regarding whether attribution may operate without a fact-based test.[29] The ARS's focus is solely on attribution as a legal principle and does not concern itself with the issues related to the violation of the primary norm.

The ARS posits that:

> [w]hether responsibility is 'objective' or 'subjective' in this sense depends on the circumstances, including the content of the primary obligation in question. The articles lay down no general rule in that regard. The same is true of other

---

II, cmt. 4, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

26 Luigi Condorelli and Claus Kress, *The Rules of Attribution: General Considerations, in* The Law of International Responsibility 233 (James Crawford, Alain Pellet, and Simon Olleson ed. 2010).

27 *Id.*

28 Luigi Condorelli and Claus Kress, *The Rules of Attribution: General Considerations, in* The Law of International Responsibility 221-225 (James Crawford, Alain Pellet, and Simon Olleson ed. 2010). *See also*, International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, ch. II, cmt. 4, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001). ("[A]ttribution of conduct to the State as a subject of international law is based on criteria determined by international law and not on the mere recognition of a link of factual causality. As a normative operation, attribution must be clearly distinguished from the characterization of conduct as internationally wrongful. Its concern is to establish that there is an act of the State for the purposes of responsibility. To show that conduct is attributable to the State says nothing, as such, about the legality or otherwise of that conduct, and rules of attribution should not be formulated in terms which imply otherwise.")

29 Luigi Condorelli and Claus Kress, *The Rules of Attribution: General Considerations, in*, The Law of International Responsibility 221, 225 (James Crawford, Alain Pellet, and Simon Olleson ed. 2010).

> standards, whether they involve some degree of fault, culpability, negligence or want of due diligence. Such standards vary from one context to another for reasons[,] which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation.[30]

The ARS allows for the primary rule violated to dictate all facets of the means to attribute an act. Therefore, attribution under the ARS must be addressed in a case-by-case manner depending on the primary obligation violated and the circumstances of the violation. This application of attribution may cause a host of issues, particularly with regard to the standards of evidence needed to support proper attribution depending upon the primary norm violated. This issue of the requisite degree of proof required for an act to be attributed to a state will be addressed *infra*.

Two initial issues need to be addressed prior to a doctrinal discussion regarding the ILC's ARS. The first is how an internationally wrongful act on behalf of a state occurs, and the second is whether the issue of mens rea operates within the issue of attribution.

How an internationally wrongful act on behalf of a state occurs is important in that a state as an entity does not act; the human actors within the state entity act in its stead. As such, only natural persons acting on behalf of a state may commit an internationally wrongful act.[31] Therefore, an internationally wrongful act may only occur when an individual actor with an identifiable relationship with the state commits an internationally wrongful act, or when a state adopts an internationally wrongful act after the fact.[32] This necessarily means that for full attribution under the ARS, the act must be attributable to an individual actor who has an identifiable relationship with the state.[33] This, in the context of attributing

---

30 International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, art. 2 cmt. 3 p.34, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

31 Constantine Antonpoulos, *State Responsibility in Cyberspace, in,* Research Handbook on International Law and Cyberspace 55, 58 (Nicholas Tsaqourias and Russell Buchan, eds. 20015).

32 International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, art. 11, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001). United States Diplomatic and Consular Staff in Tehran, Judgment, 1980 I.C.J. Rep. 3, 29, ¶90 (24 May).

33 *Id*. at 59.

malicious cyber-attacks based upon current technical attribution practices, is virtually impossible.

The second issue is whether the ARS includes a mens rea element for the individual actor within the state committing the internationally wrongful act. The simple answer is no; as a general rule, the ARS does not require any mens rea or intent for the purposes of attribution.[34] The focus is solely on proving that the accused state is responsible for an internationally wrongful act based on the primary norm violated. As such, this study will address the question of "proof" based on the specific primary norms discussed in this study.

This chapter will begin in Section 3.2 with a discussion regarding legal attribution as set forth by the ARS, followed by a discussion regarding the effective control test which establishes the needed control a state must have over other actors for responsibility to lay. This study will then turn to the issue of proof to ascertain the evidentiary burden that an injured state bears to prove state responsibility for an injury in cyberspace. After concluding this discussion, Chapter Four will focus on technical attribution with a discussion of general attribution techniques, an overview of cyberspace, and conclude with a discussion regarding how the posited rules apply to the examples discussed in Chapter One.

3.2. Responsibility of States for Internationally Wrongful Acts: Attribution

The ARS focus is on the attribution of an internationally wrongful act to the state. The ARS does recognize that a state may be responsible for the acts of non-state actors, but only within narrowly defined parameters. Art. 4-11 of the ARS elucidates how an act may be attributed to a state. Art. 4-7 discusses the conduct of a state's organs[35] while Art. 8 discusses acts directed or controlled by the state. Art. 10 discusses the acts of insurrectional or other movements and Art. 11 discusses those acts which the states may adopt after the

35 James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* 94 (2002). *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art 4 para. 1.

fact. This study will discuss the applicability of the ARS to cyber-attacks in general to demonstrate the issues with applying the ARS to the instant issue.

Art. 4 addresses the issue of attributing acts to the state by the organs of that state. The ARS states that "[t]he conduct of any state organ shall be considered an act of that state under international law…"[36] The ARS applies this to state acts as a whole, irrespective of the internal role the organ plays within the state; however, the state's internal law dictates whether that organ or person[37] is considered an organ of the state. Comment 1, to Art. 4 posits that ""State organ" covers all the individual or collective entities which make up the organization of the State and act on its behalf…"[38] The focus for determining the existence of a state organ will be the states internal law and the actions of the state in regard to the entity in question. The reference to a state organ in Art. 4 should be viewed in the most general sense.[39] The term organ

> is not limited to the organs of the central government, to officials at a high level or to persons with responsibility for the external relations of the State. It extends to organs of government of whatever kind or classification, exercising whatever functions, and at whatever level in the hierarchy, including those at provincial or even local level.[40]

The ARS does not distinguish between the act of a "superior [or] a subordinate;"[41] instead, the focus in Art. 4 is solely on the organ as part of the state.[42] The difficulty arises when a state does not specify the powers that one of its organs possesses or whether the organ

---

36 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art 4. Para. 1.

37 *Id*., at 4(2).

38 *Id.* cmt. 1.

39 U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art 4, cmt. 6.

40 *Id.*

41 Art. 4, *id*., at cmt. 7.

42 Those having status under the internal law of the state. Cf., *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), 2007 I.C.J. para. 285 et seq. (Feb. 26)

acting on behalf of the state is actually an organ.[43] In order to prevent a state from denying that an organ is actually empowered by the state to act, Art. 4, para. 2, defines an organ to "include[] any person or entity which has that status in accordance with the internal law of the states."[44] Thus a state will be held responsible for all acts that appear to be from its agent or organ based upon the appearance of exercising public authority, unless "the act had no connexion [sic] with the official function and was, in fact, merely the act of a private individual[.]"[45]

While not explicitly mention in the ARS, the ICJ has held that de facto organs fall within the purview of Art. 4.[46] De facto organs are those entities which "are not legally part of the State apparatus, [however,] they factually operate as an organ of the state since they have no real autonomy from the State."[47] Simply put these organs have no formal link to the state but operate as an organ carrying out specific state functions. De facto organs should not be confused with parastatal organs discussed in Art. 5 which have governmental authority although normally serving the state indirectly. Parastatal entities or organs are empowered to exercise elements of the state's authority, albeit, normally in limited situations.[48] James Crawford described parastatal organs as "being empowered, even if only in an exceptional and limited way, to perform certain functions that are related to those normally exercised by State bodies…"[49] Thus, parastatal organs are distinct in that they

---

43 *Id.* at cmt. 11 – 13.

44 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art 4. para. 2.

45 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art 4. para. 2, cmt. 13.

46 Sten I. Verhoeven, *International Responsibility of Armed Opposition Groups* 285-303, in, Responsibilities of the Non-State Actor in Armed Conflict and the Market Place: Theoretical Considerations and Empirical Findings (Noemi Gal-Or, Cedric Ryngaert, and Math Noortmann eds., 2015).

47 *Id.* at 300.

48 Vanessa Ballesteros Moya, *The Privatization of the Use of Force Meets the Law of State Responsibility*, 30 Am. U. Int'l L. Rev. 795, 796 (2015).

49 *Id.* Citing, Special Rapporteur, First Report on State Responsibility, Int'l L. Comm.at 39 U.N. Doc. A/CN.4/490 and Add.1-7 (1998)

have a formal link to the state even though they may be non-state actors under a state's internal laws. Parastatal organs are discussed infra.

It is important to distinguish between the test for determining a de facto organ under Art. 4 and the test for determining when a state is responsible for the actions of non-state actors under Art. 8. The ICJ has elucidated two tests, the "complete dependence and control" test for de facto organs, and the "effective control" test for non-state actors. The complete dependence and control test will be discussed infra in respect to the instant discussion on Art. 4 and the effective control test will be discussed along with Art. 8, infra.

The ICJ in *Bosnia Genocide* addressed how to test for whether an individual is to be considered an organ of the state when the ICJ asked

> whether it is possible in principle to attribute to a State conduct of persons — or groups of persons — who, while they do not have the legal status of State organs, in fact, act under such strict control by the State that they must be treated as its organs for purposes of the necessary attribution leading to the State's responsibility for an internationally wrongful act.

The ICJ answered this question, stating

> that, according to the Court's jurisprudence, persons, groups of persons or entities may, for purposes of international responsibility, be equated with State organs even if that status does not follow from internal law, provided that in fact the persons, groups or entities act in "complete dependence" on the State, of which they are ultimately merely the instrument. In such a case, it is appropriate to look beyond legal status alone, in order to grasp the reality of the relationship between the person taking action, and the State to which he is so closely attached as to appear to be nothing more than its agent: any other solution would allow States to escape their international responsibility by choosing to act through persons or entities whose supposed independence would be purely fictitious... However, so to equate persons or entities with State organs when they do not have that status under internal law must be exceptional, for it requires proof of a particularly great degree of State control over them, a relationship which the Court's Judgment quoted above expressly described as "complete dependence."[50]

50 *Bosnia Genocide*, *id*, para. 392-393.

The test for complete dependency and control therefor becomes a question of autonomy on behalf of the group or individual.[51] A de facto organ will have no autonomy and will be completely dependent upon the state. The test does not look to the formal relationship between the state and the de facto organ, the test solely focuses on the autonomy of the de facto organ and whether the de facto organ is completely dependent upon the state in question. This is an extremely high bar to meet in order to demonstrate that an individual or group is a de facto organ. In *Bosnia Genocide*, the ICJ held that "to equate persons or entities with state organs when they do not have status under internal law must be exceptional, for it requires proof of a particularly great degree of state control over"[52] the person or entity. Simply put the individual or entity must for all purposes be virtually indistinguishable from a state organ to be considered a de facto organ of the state.

Demonstrating complete dependence and control is difficult enough in the kinetic realm, so demonstrating complete dependence in the cyber realm will be even more difficult. It will be difficult in the cyber-realm to demonstrate that an individual actor will be completely dependent upon the state for the purposes of attributing the individual's acts to the state under art. 4. It may be easier to demonstrate that the individual actor was acting under the direction and control over the state as needed under art. 8, as discussed infra. As the ICJ notes, the equating of an individual actor as a state organ is an exceptional act and requires a much greater demonstration of the control over the individual than that which is needed under the effective control test needed to attribute the act under art. 8.[53] The effective control test standing alone is an extremely challenging test making the complete dependence test even more burdensome. As such this study would argue that demonstrating complete dependence or control over a non-state actor so as to attribute the acts as that of a state organ is virtually impossible in cyberspace.

This study would argue that in practice, the disavowing of state acts by claiming that the actor was not empowered to act on behalf of the state and that the actor is not wholly

51 Verhoeven, *id.*, at 300.

52 Bosnia Genocide, *id*., at para. 393.

53 *See generally, id.*

dependent upon the state, particularly in cyberspace, is a serious obstacle to overcome for attributing state responsibility. States too often create clandestine intelligence operations to act on their behalf with the sole purpose of acting without the appearance of state involvement at any level. Gaining evidence to link the state with clandestine intelligence operations is difficult in kinetic operations, and with advances in operational security, it is almost impossible in the virtual world. While it has been alleged[54] that the United States' intelligence apparatus has the means to crack such acts in cyberspace, it must be recognized that most intelligence operations will utilize alternative methods of communication to avoid potential interception by another state for clandestine activities.[55] In other words, states combine old methods with new technology in order to avoid attribution of conduct for their clandestine activities.

Demonstrating complete dependence may prove particularly difficult when combined with the burden of proof necessary to meet the required burden of proof for attribution. This study argues that most attribution to a state will not be by direct attribution, but will instead be circumstantial in nature. While there is nothing wrong with circumstantial evidence in and of itself, circumstantial evidence is too malleable in the context of cyberspace, and as will be discussed *infra*, circumstantial attribution does not meet the evidentiary burden needed for attribution and state responsibility.

As briefly discussed supra, the issue of parastatal entities or organs is discussed in ARS Art. 5 which states:

> [t]he conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under

54 See disclaimer, *supra* p. ii.

55 *See, e.g., Back in Time: Russian Agency Seeks Typewriters for Secret Documents*, Spiegel Online International (July 11, 2013), http://www.spiegel.de/international/world/russian-intelligence-seeks-typewriters-for-secret-documents-a-910677.html (Discussing the potential purchase of German-made typewriters by the Russian Federal Guard Service in an attempt to protect internal communications from electronic intercept.)

international law, provided the person or entity is acting in that capacity in the particular instance.[56]

The ARS justifies such attribution by positing that when the person or entity is empowered by the state, their acts are then the state's own acts as the state "has conferred on the entity in question the exercise of certain elements of governmental authority."[57] The ARS again looks to the domestic law of the state to ascertain the standing of the person or entity in reference to the state. The issue of parastatal groups and state responsibility is of growing import as states continue the trend of utilizing parastatal entities to perform functions that were traditionally under the purview of the state.

Art. 5 allows for the acts of groups such as computer emergency response teams (CERT) to be attributed to the state if acting in their official capacities on behalf of the state; those groups may be established by law, and they often consist of private individuals or entities.[58] Art. 5 holds that when a state empowers "a person or entity"[59] with powers normally reserved to the state, the state will be responsible for the acts of the person or entity. If that same CERT group is acting on behalf of a private organization and not the state, then no state responsibility would attach. However, the ARS does not delineate the "scope of governmental authority for the purposes of attribution of the conduct of the entity to the state."[60] Instead the ARS looks at the circumstances and role of the state and its legal traditions to ascertain the cope of authority. Thus, creating a broad general standard which may be applied to various circumstances.

---

56 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 5.

57 *Id*. cmt. 5.

58 Tallinn Manual on the International Law Applicable to Cyberwarfare 33, R. 6 n. 13 (Michael N. Schmitt ed., 2013).

59 *Id*. n. 45, *supra.*

60 U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 5, cmt. 6.

Art. 6 and 7 of the ARS may prove even more burdensome for use in attributing cyber-attacks to a state. According to Art. 6, any internationally wrongful act by the organ will be attributed to the parent state "if the organ is acting in the exercise of elements of the governmental authority of the state at whose disposal it is placed."[61] In the instant issue, Art. 6 would apply in the cyber context if, hypothetically, the United States loaned elements of the National Security Agency (or other government agency or organ) to the Israeli government in order for Israel to launch a cyber-attack on another state's nuclear infrastructure. In that case, where the NSA element is an organ of the U.S. Government, Israel would be responsible for the internationally wrongful act if the act was attributable to Israel under international law and if the NSA element "was placed at the disposal"[62] of the state of Israel and the NSA element "act[ed] with the consent, under the authority of and for the purposes of the" state of Israel.[63] However, gathering the required evidence to attribute the cyber-attack to Israel and then gathering the evidence sufficient to prove the United States' involvement is a difficult proposition.

Art. 7 deals with the issue of when a state's organ, person, or entity empowered to act on behalf of the state exceeds the authority it was granted, resulting in an internationally wrongful act.[64] Any act of an empowered organ, individual, or entity which is acting in an

---

61 *Id*. at n.49 art. 6.

62 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 6, cmt. 1 *et seq.*

63 *See id*., cmt. 5. ("There are two further criteria that must be met for article 6 to apply. First, the organ in question must possess the status of an organ of the sending State; and secondly its conduct must involve the exercise of elements of the governmental authority of the receiving State. The first of these conditions excludes from the ambit of article 6 the conduct of private entities or individuals which have never had the status of an organ of the sending State. For example, experts or advisers placed at the disposal of a State under technical assistance programmes do not usually have the status of organs of the sending State. The second condition is that the organ placed at the disposal of a State by another State must be "acting in the exercise of elements of the governmental authority" of the receiving State. There will only be an act attributable to the receiving State where the conduct of the loaned organ involves the exercise of the governmental authority of that State. By comparison with the number of cases of cooperative action by States in fields such as mutual defence, aid and development, article 6 covers only a specific and limited notion of "transferred responsibility". Yet, in State practice the situation is not unknown.")

64 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 7.

official capacity and exceeds that authority or acts *ultra vires,* is still attributable to the state.[65] The ILC adopted such a position based on the idea that a state should not be able to hide behind its internal laws relating to the powers granted to an authorized party on behalf of the state. To do so would allow states to deny responsibility for the majority of its agents' acts. This rule is "firmly established in this sense by international jurisprudence, state practice and the writings of jurists."[66] While this study cannot demonstrate such an act as envisioned by Art. 7 in cyberspace, it is easy to theorize situations where an agent or individual takes a malicious act in cyberspace.[67]

Under the ARS, a state may empower private corporations to take countermeasures in cyberspace. Garrie and Reeves recognized that under such a scenario, a state would be responsible for not only the approved countermeasures but also for any unapproved acts by such empowered corporations.[68] In addition, states are likely to contract out the production of malicious cyber tools to private corporations as a means to avoid technical attribution or circumstantial attribution to the states. In that scenario, a state will be responsible for any unauthorized or *ultra vires* acts taken by the contractor, and responsible for any use of such tools with state approval. Arguably, once such a cyber weapon is released, if the code for the cyber weapon is modified and re-used, the original state may still bear responsibility for the harm caused by its creation.

Art. 8 deals with the situation where a person or a group (non-state actors) not affiliated by law to the state acts at the "instruction of, or under the direction or control of, the state."[69]

---

65 *Id.*, cmt. 1.

66 *Id*., cmt. 4.

67 Daniel Garrie and Shane R. Reeves, *So You're Telling Me There's a Chance: How the Articles on State Responsibility Could Empower Corporate Responses to State-Sponsored Cyber Attacks*, Harv. Nat. Sec. J. 10-12 (Dec. 17, 2015), http://harvardnsj.org/2015/12/so-youre-telling-me-theres-a-chance-how-the-articles-on-state-responsibility-could-empower-corporate-responses-to-state-sponsored-cyber-attacks/.

68 *Id.* at 10.

69 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 8.

This may be seen when a state engages non-state actors (hacktivists or proxies) to perform an act in cyberspace which amounts to an internationally wrongful act. The purpose of Art. 8 is to prevent a state from avoiding its responsibility in international law by engaging non-state actors to perform the act.[70]

The attribution of responsibility to the state under Art. 8 is challenging and has a high evidentiary burden to meet. The ICJ has held in *Military and Paramilitary Activities in and against Nicaragua* (Nicar. v. U.S.) (*Nicaragua*), that for state responsibility to lie for the acts of a non-state actor it must "be proved that that state had effective control of the…operations in the course of which the alleged violations were committed…"[71] To ascertain exactly what the effective control test is, it is necessary to look at the facts of *Nicaragua* and understand the acts of the United States.

The United States, through its external intelligence agencies (mainly the Central Intelligence Agency), financed, trained, armed, and advised contras rebels in the Nicaragua civil war from circa 1980-1986. The ICJ found that:

> it is in the Court's view established that the support of the United States authorities for the activities of the contras took various forms over the years, such as logistic support, the supply of information on the location and movements of the Sandinista troops, the use of sophisticated methods of communication, the deployment of field broadcasting networks, radar coverage, etc. The Court finds it clear that a number of military and paramilitary operations by this force were decided and planned, if not actually by United States advisers, then at least in close collaboration with them, and on the basis of the intelligence and logistic support which the United States was able to offer, particularly the supply aircraft provided to the contras by the United States.[72]

70 Collin S. Allan, *Attribution Issues in Cyberspace*, 14 Chi-Kent J. Int'l & Comp. L. 56, 64 (2014).

71 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J. 14, 64-65 (June 27).

72 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J. 14, 61 ¶106-107 (June 27).

The ICJ found that the United States openly funded the contra rebels and made the contras a cornerstone of United States policy in the region.[73] The ICJ, therefore, asked:

> whether or not the relationship of the contras to the United States Government was so much one of dependence on the one side and control on the other that it would be right to equate the contras, for legal purposes, with an organ of the United States Government…[74]

The ICJ ultimately found:

> despite the heavy subsidies and other support provided to them by the United States, there is no clear evidence of the United States having actually exercised such a degree of control in all fields as to justify treating the contras as acting on its behalf.[75]

The ICJ in *Nicaragua* looked at the aid and actions of the United States and the contras in its totality, without focusing on any one type of assistance or acts on behalf of the United States vis-à-vis the contras. The ICJ established that to attribute the acts of non-state actors to a state, (1) the state must have effective control based upon the totality of the evidence presented and (2) the non-state actors must be almost completely dependent upon the sponsoring state to the point that it is almost impossible to differentiate the non-state actor from an organ of the sponsoring state.

The test elicited by the ICJ in *Nicaragua* to hold a state responsible for the acts of a non-state actor is different than the test elucidated by the ICJ in the *Bosnia Genocide* case to determine if the acts of a non-state actor may be equated as the acts of a state organ as discussed supra, in the discussion on art. 4. The ICJ explained the different tests as thus

> [t]he [effective control] test thus formulated differs in two respects from the test—described above [art. 4, supra] — to determine whether a person or entity may be equated with a State organ even if not having that status under internal law. First, in this context it is not necessary to show that the persons who performed the acts alleged to have violated international law were in general in a relationship of "complete dependence" on the respondent State; it has to be proved that they acted in accordance with that State's instructions or under its

---

73 *Id.* p. 61 ¶109.

74 *Id*. at p.62.

75 *Id.*

> "effective control". It must however be shown that this "effective control" was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.[76]

In addition, the ICJ held that the effective control test was to be used irrespective of the internationally wrongful conduct alleged.[77] Therefore whether it be genocide or malicious cyber-attacks, to attribute the acts of non-state actors to a state the effective control test is the test to utilize. If one alleges that the acts were such as to make the non-state actor an organ of the state the test to be utilized is the complete dependence test. The focus of the effective control is not the relationship per se of the actors but whether the non-state actors acted on the instructions of the state and then demonstrated that the state had effective control over the non-state actors as described supra.

In the context of this study, attributing the acts of non-state actors in cyberspace to the sponsoring state is virtually impossible given the difficulties of technical attribution and the difficulties of showing effective control on behalf of the state over the non-state actors. Indeed, a state may fund groups, supervise groups, choose the group's targets, and even give the groups the tools and training necessary and state responsibility will not lie. This is demonstrated by the ICJ in *Nicaragua* as the United States had done all these things for the Contra rebels and yet the acts of the Contras were not attributed to the United States.

In the opinion of this study, the effective control test creates a virtual bar for attributing the acts of hacktivists and proxies to the state. As such, it is theorized that states may be more likely to utilize such groups for malicious acts in cyberspace when a modicum of deniability on behalf of the state is needed. Hence, even given the evidence of the DDoS attacks

---

76 *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), 2007 I.C.J. para. 285 et seq. (Feb. 26)

77 *Id.* para. 401. ("The rules for attributing alleged internationally wrongful conduct to a State do not vary with the nature of the wrongful act in question in the absence of a clearly expressed *lex specialis*... This is the state of customary international law, as reflected in the ILC Articles on State Responsibility.")

originating from Russia against Estonia and Georgia, the DDoS attacks cannot be legally attributed to Russia under the ARS/ICJ rules.

However, a state's involvement with hacktivists and proxies may constitute an internationally wrongful act in itself without attribution of conduct to the state. If the state provides the tools for hacktivists to use against a common foe, then per the *Tallinn Manual*, the state has committed an internationally wrongful act in supplying the tools. Proving authorship of cyber tools is not as difficult as technically attributing a cyber-attack, but it is not straightforward either, for the best authors will know the forensic techniques utilized to delineate who produced the tools. As such, the better the author, the less likely direct technical attribution of the tool will be.

ARS Art. 9 addresses the "exceptional"[78] case of when a state will be responsible for the acts of a person or persons acting in place of a state's authority. When the state, for whatever reason, is unable to fulfill the role itself, and a person or persons act in "absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority,"[79] the state will be responsible for those actions. Art. 9 is fundamentally different from Art. 8 even though in both respects the acts in question are performed by non-state actors. In Art. 8, the state is only responsible if effective control over the non-state actors is demonstrated; no such finding is necessary under Art. 9. This is due to the exceptional circumstances which give rise to the non-state actor's actions.

The ARS uses the term "exceptional" to set Art. 9 apart from the other articles and to illustrate the distinct circumstances that must exist for the acts of non-state actors to be seen as those of a state. The ARS puts forth the theory that exceptional circumstances will only occur during "during revolution, armed conflict or foreign occupation."[80] The theory

78 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 9.

79 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 9.

80 *Id*. cmt. 1.

behind Art. 9 is based upon the "*levee en masse*, the self-defense of the citizenry in the absence of regular forces;"[81] that is, citizens defending their states when the state itself is incapable of acting. Such incidents may occur in cyberspace when a group or individual launches a cyber-attack against a foreign state which has knocked out that state's ability to respond. Another example is if the state cannot "exercis[e] their function in some respect,"[82] such as if a state's defense infrastructure is disabled and individuals or groups initiate cyber-attacks because the state is unable to do so itself.

The state under Art. 9 must have knowledge of the acts in question and must not object to the actions by the non-state actors. In addition, those actions must be undertaken by the non-state actors because the circumstances must call for action.[83] That is, private individuals take actions that would otherwise be undertaken by the state as the situation dictates that such actions be taken. This is the idea of citizens acting in self-defense against an invader where traditional military forces are not available and "just as citizens have the right to collective self-defense in absence of regular forces… they may assume government functions where the government is absent"[84] These acts, which implicate the state, are actions that normal state functionaries would take and in their absence individual actors undertake to fill a role otherwise filled by a state actor as there is a lack, for whatever reason, of state actors to do these roles.

Therefore, if the acts of the individual or group would violate the authority of the organ they are acting on behalf of, the act would not be attributable to the state. This caveat is to protect against the acts of insurrectional groups being attributed to the state,[85] which is dealt with in ARS Art. 10.

---

81 *Id.* cmt. 2.

82 *Draft Articles on Responsibility of States for Internationally Wrongful Acts 38*, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 9, cmt. 5.

83 *Id.* cmt. 6.

84 Jan Arno Hessbruegge, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. Int'l. L. & Pol 265 (2004). *See also*, *Id.*

Art. 10 sets forth three principles: (1) the acts of an insurrectional group may be attributed to the state if the insurrectional group is recognized as a state in international law;[86] (2) that the acts of insurrectional or other groups that establish a new state "in part of the territory under its administration" shall be attributed to the new state;[87] and (3) the insurrectional group that forms a new state is not prejudiced as to the attribution of any conduct under the ARS. Again, the ARS deals with attribution such as this as a "special" circumstance[88] much like Art. 9. However, both Art. 9 and 10 labor under the technical attribution problem as much as the legal attribution problem. The linking of acts in cyberspace to a group is as difficult as linking the acts to a state. In fact, it may be even more difficult as it has been argued that states utilize multiple intelligence methods, not just technical attribution, in an attempt to attribute malicious cyber-attacks to a state. As Matt Tait explained:

> [t]he intelligence community [of a state] has powers and capabilities that far exceed that of the private sector for [circumstantial] attribution, and do not suffer from the same conflicts of interest. Whereas private sector attribution tends to rely on technical forensics of the malware and infrastructure used by the hackers, the [Intelligence Community] is able to draw upon a much more diverse set of capabilities—such as financial intelligence, human intelligence, and counter-intelligence—to bring together a wider set of facts with narrower bands of uncertainty than the private sector would normally have at its disposal.[89]

However, such intelligence may not be available for rebel groups, insurrections, or other such groups, making it difficult to attribute acts in cyberspace to the new state.

---

85 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 9. Cmt. 6.

86 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 10(1).

87 *Id*. at 10(2).

88 *Id.* cmt. 1.

89 Matt Tait, *On the Need for Official Attribution of Russia's DNC Hack*, Lawfare (July 28, 2016), https://www. lawfareblog.com/need-official-attribution-russias-dnc-hack.

Finally, Art. 11 discusses ex-post facto attribution based on the adoption of conduct by the state:

> [c]onduct which is not attributable to the state under the preceding articles shall nevertheless be considered an act of that state under international law if and to the extent that the state acknowledges and adopts the conduct in question as its own.[90]

Art. 11, like Art. 10, is an exception to the rules posited by the ARS in Chapter II, where only the acts of the state are attributable to the state.[91] The conduct attributed to the state under Art.11 is normally that of a non-state actor.[92] This exception to the attribution of conduct to the state for the acts of a non-state actor is based, in large part, on the ICJ decision in the *United States Diplomatic and Consular Staff in Tehran* (Iran Hostage case).[93]

The Iran Hostage case was brought by the United States against Iran after the United States Embassy and two consulates in Iran were overrun and occupied by student protesters[94] who took American diplomatic and consular staff as hostages on November 4, 1979. Under the customary interpretation of state responsibility, such acts by the students could only be attributed to Iran "if it were established…that they were, in fact, acting on [Iran's] behalf…"[95] However, due to Iran's failure to act to protect the American Embassy and its staff, the ICJ found that Iran was "in clear and serious violation of the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations."[96] This

---

90 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 11.

91 *Id*. cmt. 1.

92 *Id.* cmt. 2.

93 United States Diplomatic and Consular Staff in Tehran (U.S.A. v. Iran), 1980 I.C.J. Rep. 3 (24 May).

94 Id. at ¶56.

95 Id. at ¶58.

96 United States Diplomatic and Consular Staff in Tehran (U.S.A. v. Iran), 1980 I.C.J. Rep. 3, 32 ¶67 (24 May).

violation was ongoing; while the ICJ heard the instant case, the Iranian government allowed and encouraged the students' actions. Further, it took no action to bring Iran into compliance with treaties and CIL in place even though Iran conceded that the state of Iran was "duty bound to safeguard the life and property of foreign nationals."[97] Instead, the Iranian government expressed approval of the students' actions. This approval was given at almost every level of the Iranian government, including the judiciary and executive, with Ayatollah Khomeini endorsing "both the take-over of the Embassy and Consulates and of the detention of the Embassy staff as hostages."[98] The Ayatollah went so far as to order his representatives not to meet with the American representatives attempting to negotiate the release of the hostages. The government of Iran made its approval of the students' acts official when the Ayatollah issued an official decree on November 17, 1979, where he:

> expressly to declare[d] that the premises of the Embassy and the hostages would remain as they were until the United States had handed over the former Shah for trial and returned his [the Shah's] property to Iran. This statement of policy the Ayatollah qualified only to the extent of requesting the militants holding the hostages to 'hand over the blacks and the women, if it is proven that they did not spy, to the Ministry of Foreign Affairs so that they may be immediately expelled from Iran.' As to the rest of the hostages, [the Ayatollah] made the Iranian Government's intentions all too clear: 'The [sic] noble Iranian nation will not give permission for the release of the rest of them. Therefore, the rest of them will be under arrest until the American Government acts according to the wish of the nation.'[99]

This policy was almost uniformly endorsed at all levels of the Iranian government as a means to compel the United States to accept the Iranian demands. Thus:

> [t]he approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible.[100]

---

97 United States Diplomatic and Consular Staff in Tehran (U.S.A. v. Iran), 1980 I.C.J. Rep. 3, 33-35 ¶¶ 69-74 (24 May).

98 *Id*. at ¶71.

99 *Id*. at ¶73.

100 United States Diplomatic and Consular Staff in Tehran (U.S.A. v. Iran), 1980 I.C.J. Rep. 3, 35 ¶74 (24 May).

The acts of the students in the Tehran Hostage case became the acts of the state of Iran due to the presence of an internationally wrongful act, the prevention of that act by the state, and the state's support, acquiescence to, or adoption of, the act, where the act of the state was in contravention of an international obligation. The adoption by the state must be based upon actions at the highest level of the state and must be more than mere statements in support or endorsement.[101] The adoption by the state must also be widespread to the point that the act resembles an act of the state itself. The state must also be open about the adoption; that is, the state, in its comments or acts, must readily adopt the acts with a degree of affirmation as seen as an official act of the state.

For application to malicious cyber-attacks, a state may adopt the actions of non-state actors in cyberspace if, after the fact, the state endorses those acts at the highest levels, encourages the actions as a matter of official policy, and does not take action to stop the attacks if they are ongoing. This rule is for attribution only; state responsibility will not lie unless the adopted act itself is an internationally wrongful act.

As to the examples presented in the study, none of the examples discussed have been adopted after the fact. While some media reports indicate that a Russian official acknowledged the engagement of hacktivists against Estonia and Georgia, a single comment by a state official is not enough for the state to adopt the acts. A state may adopt acts in cyberspace after the fact and be responsible for the attacks under this rule, but none of the examples discussed in this study have met the criteria necessary for after-the-fact adoption.

101 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 11, cmt. 6.

3.2.1. Analysis: The Articles on Responsibility of States for Internationally Wrongful Acts and Attribution

The ARS, in its simplest form, may be seen as a model of agency law: the superior is only responsible, with limited exceptions, for the acts of its agents and employees. The theory is based on the fact that the agency conveys its powers to act to its agents, just as a state may only act through those real persons who have the ability to act.[102] This distinction is important to remember as we discuss an abstract idea of the "state" as being responsible for an action; in reality, we are discussing individuals who wield the power of the state under the guise of state authority. Too often, the literature sets off the state as an independent actor while forgetting that it is composed of individuals working to achieve its objective.[103]

The ARS was an attempt to codify the CIL of state responsibility. It suffers from the drawback that the CIL for state responsibility is continually evolving in response to technological changes.[104] This is important, as will be discussed *infra*, as international law, in general, has been slow to embrace the cyber evolution that has arguably taken over the world. The ARS has been impacted by the evolution of cyber-related technology in particular and its impact upon the notions of sovereignty and state control.

The ARS posits that "[i]n theory, the conduct of all human beings, corporations or collectivities linked to the state by nationality, habitual residence or incorporation might be attributed to the state, whether or not they have any connection to the Government."[105] Such a method of attribution is avoided by the ARS, however, as the ARS strives to maintain

---

102 André Nollkaemper, *Concurrence Between Individual Responsibility and State Responsibility in International Law*, 52 Int'l Comp. L. Q. 615, 616 (July 2003) ("Traditionally, international law attributes acts of individuals who act as [S]tate organs, exclusively to the [S]tate. Although in factual terms [S]tates act through individuals…").

103 *Id.*

104 *See e.g.*, David D. Caron, *The ILC Articles on State Responsibility: The Paradoxical Relationship Between Form and Authority*, 96 Am. J. Int'l L. 857, 858 (2002) ("The difficulty of concluding the ILC's work on state responsibility suggests that the Commission's adoption of the articles is not the end of the story.") *See also id*, at 860. (Discussing the unwanted "rigidity" that the codification of customary international law may "inject.").

105 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), ch 2, cmt. 2.

both the autonomy of the state and that of the individual. The ARS adopts "the general rule [] that the only conduct attributed to the state at the international level is that of its organs of government, or of others who have acted under the direction, instigation or control of those organs."[106]

The ARS allows an exception to this general rule: a state may be responsible for the acts of a private individual or group if the state adopts the acts of the individual or groups as those of its own.[107] This exception, based on the *Tehran Hostage Case*,[108] applies "to the extent that the state acknowledges and adopts the conduct in question as its own."[109] The ARS does not recognize state responsibility for private acts of individuals or groups outside this narrow exception. The ARS is at odds with current state practice regarding the responsibility of states for the acts of private individuals and groups as discussed *supra*, where it was demonstrated that state practice has recognized, in limited circumstances, the responsibility of states for the acts of private individuals and groups for the purposes of attribution. This once again illustrates the fragility of the ARS as a codification of CIL: it is inflexible in the face of ever-changing state practice. This study will return to this idea *infra*, but it is important to bear this in mind as this study goes forth.

The ARS establishes that a state is responsible for the acts and omissions of any of its organs.[110] Organs include individuals and groups that "make up the organization of the state and act on its behalf."[111] It does not matter what the organ's role within the state is,[112] the "level of principle,"[113] or whether the organ is of the central government or local

106 *Id.*

107 *Id.* at art. 11.

108 United States Diplomatic and Consular Staff in Tehran Case, (USA v. Iran), 1980 I.C.J. 1 (24 May).

109 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 4.

110 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 4.

111 *Id.* cmt. 1.

112 *Id.* cmt. 6.

113 *Id.* cmt. 7.

government.[114] This principle is aptly demonstrated with the United States bearing responsibility for the state of Texas's acts in applying the death penalty to Mexican citizens who had been denied consular notification rights. While domestic United States law made it impossible for the United States to prevent Texas from acting, the United States nonetheless was responsible for the breach of international law where the acts of Texas were attributable to the United States.[115]

The ARS extends the agency principle to those individuals or groups who are "empowered by law of that state to exercise elements of the governmental authority…"[116] These parastatal organs are not directly controlled by the state, but they still wield some modicum of state power. Under the ARS, they may implicate the state through their acts. These parastatal organs may be individuals or collectives working under charter or grant for the state as independent corporations, yet they are authorized by domestic law to carry out acts on behalf of the state. Such parastatal entities may involve military contractors, railway operators, and private penal institutions.

Their acts are attributable as if they were state actors, but the ARS narrows the scope to only those acts which are:

> in that capacity in the particular instance."[117] That is the parastatal entity is acting within the scope of powers granted to it by the State. This is a narrow exception specifically for those parastatal entities as any act of a State organ shall be considered an act of the State under international law if the organ, person or entity acts in that capacity, even if it exceeds its authority or contravenes instructions.[118]

---

114 *Id.* cmt. 8.

115 *See,* Case Concerning Avena and Other Mexican Nationals (Mex. V. USA), 2008 Gen. List 139 (16 July).

116 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 5.

117 *Id.*

118 *Id.* at Art. 7.

The ARS also allows for attribution when the "[c]onduct [is] carried out in the absence or default of the official authorities."[119] This exception covers acts of individuals and groups acting in a manner normally reserved for a state alone (e.g., waging combat operations against another state) without or outside of "governmental authority"[120] to do so. The ARS "envisions"[121] such conduct to "occur only rarely"[122] as in times of "revolution, armed conflict, or foreign occupation."[123] This form of attribution could implicate cyber-attacks if "a person or group… perform government functions though they are doing so on their own initiative"[124] during times of conflict.

This concept may implicate cyber-attacks like those carried out by hacktivists or proxies: those individuals or groups who, absent explicit governmental authority to do so, launch attacks against states to support an ongoing conflict or to show disapproval for another state's conduct vis-à-vis their home state. Such patriot hacker group phenomena have been blamed for the cyber-attacks against both Estonia and Georgia. However, the ARS establishes two additional elements that must be met for attribution under this rule in addition to the *actus reus* posited *supra*. First, the actions of the private actors or groups must be in the "absence or default of"[125] government authority or oversight. The ARS posits that such acts would be present in the "partial-collapse or a loss of control"[126] over parts of a state's territory.[127]

---

119 *Id.* at *Art*. 9.

120 *Id.*

121 ARS, Art. 9, *id.* at cmt. 1-2.

122 *Id.* at cmt. 1.

123 *Id.*

124 *Id.* Art. 9 at cmt. 4.

125 *Id.* Art. 9 at cmt. 5.

126 *Id.*

127 *Id.*

Second, the state itself must "call[] for"[128] individuals or collectives to act in its absence and at its request. The ARS states that the act of calling for individuals or collectives to act does not have to be for the same conduct the individual or collective later takes.[129] Such acts, while *ultra vires* of the original rights granted to the individual or collective, still implicate the granting state.

These additional elements create issues in attributing the acts of hacktivists and proxies to states. This is particularly difficult when the state engages in willful blindness to the activities of such groups or, as alleged by some commentators in regards to the Georgia cyber-attacks, the state gives tacit approval so as to not implicate itself. The ARS addresses activities of private individuals and groups, positing:

> 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.[130]

In order to find a link between the state and the individual or group, the ARS adopted the effective control test. The effective control test was first put forth by the ICJ in the *Nicaragua* case, where:

> the Court ha[d] to determine…whether or not the relationship of the *contras* to the United States Government was one of dependence on the one side and control on the other that it would be right to equate the *contras*, for legal purposes, with an organ of the United States Government, or as acting on behalf of that Government.[131]

The ICJ held that to attribute the acts of the contras to the United States "would in principle have to be proved that that state had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.''[132] The effective

---

128 *Id.* Art. 9 at cmt. 6.

129 *Id.*

130 *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), art. 8.

131 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Merits), 1986 I.C.J. Rep. 14, ¶ 109.

132 *Id.* at ¶ 115.

control test is the ICJ's means of analyzing whether a state controlled independent actors to the point where they may be considered state actors or organs. The ICJ held that to meet the threshold needed for an actor to be considered under the control of the state; the state must "direct[] or enforce[] the perpetration of the acts."[133] The effective control test establishes an extremely high level of control that a state must have over independent actors before the acts may be attributed to the state.[134]

The *Nicaragua* case and the effective control test have faced criticism within international law. Cassese, for example, posited that the ICJ's decision was not rooted in CIL, nor is the ICJ following the three elements posited by ARS Art. 8.[135] The effective control test was challenged by the ICTY in its *Tadić* decision where the tribunal adopted a less restrictive test to find state responsibility. In *Tadić*, the ICTY put forth the overall control test in which the tribunal held "for the attribution to a state of acts of these groups; it is sufficient to require that the group as a whole be under the overall control of the state."[136] The tribunal explained that:

> [i]n order to attribute the acts of a military or paramilitary group to a State, it must be proved that the State wields overall control over the group, not only by equipping and financing the group but also by coordinating or helping in the general planning of its military activity. Only then can the State be held internationally accountable for any misconduct of the group.
>
> It should be added that courts have taken a different approach with regard to *individuals or groups not organized into military structures.* With regard to such individuals or groups, courts have not considered an overall or general level of

133 *Id.* ("The Court has taken the view that United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua. All the forms of United States participation mentioned above, and even the general control by the respondent State over a force with a high degree of dependency on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State.") *See also*, Antonio Cassese, *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 Eur. J. Int'l L. 649, 653 (2007).

134 Cassese, *id.* at 654.

135 *Id.* at 651.

136 Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment of the Appeals Chamber ¶ 120 (Int'l Crim. Trib. for the Former Yugoslavia 15 Jul 1999).

> control to be sufficient but have instead insisted upon specific instructions or directives aimed at the commission of specific acts, or have required public approval of those acts following their commission.[137]

The tribunal explained that there is support in previous ICJ cases such as *Tehran* to justify a lesser level of control for the actions of paramilitary organizations and those of less organized groups and individuals.[138] The tribunal uses differing levels of control over groups and individuals. The tribunal stated:

> international rules do not always require the same degree of control over armed groups or private individuals for the purpose of determining whether an individual not having the status of a State official under internal legislation can be regarded as a *de facto* organ of the State. The extent of the requisite State control varies. Where the question at issue is whether a *single* private individual or a *group that is not militarily organised* has acted as a *de facto* State organ when performing a specific act, it is necessary to ascertain whether specific instructions concerning the commission of that particular act had been issued by that State to the individual or group in question; alternatively, it must be established whether the unlawful act had been publicly endorsed or approved *ex-post facto* by the State at issue.[139]

Lastly, the tribunal posited that international law recognized a third test for state responsibility. The tribunal put forth the assimilation test which "is the assimilation of individuals to state organs *on account of their actual behavior within the structure of a State*."[140] The tribunal explained that individuals:

> acting within the framework of, or in connection with, armed forces, or in collusion with State, authorities may be regarded as *de facto* State organs… it follows that the acts of such individuals are attributed to the State, as far as State responsibility is concerned, and may also generate individual criminal responsibility.[141]

The assimilation test as put forth by the ICTY would, in the opinion of this study, greatly simplify the difficulties of attributing malicious cyber-attacks to states. In addition, such a test would square with the ILC's adoption of ARS Art. 11 and comport better with the ICJ's

---

137 *Id.* at ¶¶ 131-132. (Emphasis in original).

138 Prosecutor v. Tadic, *id.* at ¶¶ 133-134.

139 *Id.* at ¶ 137 (emphasis in original).

140 Id. at ¶ 174.

141 *Id.* at ¶ 144.

decision and the facts in the *Tehran Hostage Case*. The assimilation test would have created an objective test based upon the role of the actor similar to public function theory in United States constitutional law as put forth in *Evans v. Newton*, 382 U.S. 299 (1966).[142] In *Newton*, the United States Supreme Court stated: "that [c]onduct that is formally 'private' may become so entwined with governmental policies or so impregnated with a governmental character as to become subject to the constitutional limitations placed upon state action."[143] In doing so, the private acts may be attributable to the state, particularly "where a State delegates an aspect of the elective process to private groups."[144] By performing acts normally reserved to states, such as malicious cyber-attacks, espionage, and any act that implicates national security, a state may become responsible for these acts under the assimilation test, just like the test in *Newton*.

However, the ICJ revisited the issue of attribution and state responsibility in the *Bosnia Genocide* case[145] where the ICJ rejected the overall control test (and the assimilation test) in favor of its effective control test. The ICJ reasoned that the ICTY "was not called upon in the *Tadic´* case, nor is it in general called upon, to rule on questions of State responsibility, since its jurisdiction is criminal and extends over persons only."[146] While the ICJ avoided ruling that the overall control test was invalid for determining state responsibility, the ICJ stated the overall control test broadened the "scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say, the conduct of persons acting, on whatever basis, on its behalf"[147] and as such, the ICJ reaffirmed the use of the effective control test.

---

142 382 U.S. 296, 299 (1966). *See also*, James Daily, *Is Batman a State Actor?* Law and the Multiverse (Nov. 30, 2010), http://lawandthemultiverse.com/2010/11/30/is-batman-a-state-actor/. (Discussing the theoretical application of *Evans. v. Newton* to the comic book character Batman.)

143 *Evans v. Newton*, 382 U.S. 296, 299 (1966).

144 *Id.*

145 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 2007 I.C.J. Rep. 43 (26 Feb. 2007).

146 *Id.* at ¶ 403.

147 *Id.* at ¶ 406.

The ICJ then stated that an individual might implicate a state for the purposes of state responsibility if the individual conduct is an international wrong that was attributable to the state via ARS Art. 8. It then applied Art. 8 to the facts of the case before it.[148] The effective control test demands a showing of control that may not be evidenced in malicious cyber-attacks, as the digital evidence of such attacks will not necessarily support such a finding. Add to this the decentralized nature of cyber-attacks and the ability for private actors to engage in such acts, then hacktivists and proxies may act in the state's stead without the state fearing any "legal" recourse. Thus, the ICJ established a virtual bar to attribution of a majority of malicious cyber-attacks to states irrespective of the entity responsible for the attacks. As such, international law needs alternative mechanisms for holding states responsible for acts in cyberspace initiated from the state's sovereign territory.

Returning to the issue of this study, that of attributing malicious cyber-attacks to a state for the purposes of state responsibility, the question, therefore, is how one attributes a cyber-attack to the responsible state given the issues of technical attribution discussed *infra* Chapter Four, combined with the high level of control demanded by the effective control test. Attribution is further compounded by the issue of states allowing hacktivists or proxies to act in support of states' objectives either with the acquiescence of the state or through willful blindness. It is difficult to envision adequate attribution under the existing ARS. This problem will be assessed briefly.

If a state suffers a malicious cyber-attack of any type that is serious enough to invoke international law, the injured state faces two challenges ab initio: (1) collecting the needed digital evidence to link the attacks to a state (or group or individual); and (2) proving that the actor or actors responsible for the attacks were or were not state agents or organs. If they are not state agents or organs, the challenge becomes determining whether the state had effective control over the group's acts.

The evidence available to the injured state will depend, in large part, upon the skill of the authors of the malicious cyber-attacks and the skills of those conducting the investigation

148 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 406 (26 Feb. 2007).

on behalf of the injured state. The available digital evidence will most likely not contain direct evidence of state involvement; at best, it may contain cryptic references that may be either evidence or a false trail intended to lead forensic analysts astray.[149] If the injured state is lucky enough to have a "smoking gun"[150] that digitally proves that a state created a cyber weapon, that alone does not attribute the attack to the state under existing CIL. The nature of malicious cyber-attacks, combined with the ability of individuals with a modicum of technical know-how to launch a cyber-attack, means that the injured state will be hard-pressed to find enough evidence to attribute the malicious cyber-attacks. It is posited herein that any state that is accused of launching a malicious cyber-attack need not fear the attack being attributed to it as a matter of international law; given the nature of the internet, it is easy for a state to simply blame a non-state actor, and without contrary proof, it becomes a simple case of finger-pointing by states without any legal recourse.

The ICJ's adherence to the effective control test may be plausible for kinetic attacks where physical evidence is available, and intelligence regarding an attack is more readily attainable, but it fails in respect to malicious cyber-attacks. The evidence needed to link an attack to a state that demonstrates the requisite control needed for attribution will not, in a majority of cases, be present. The *Tallinn Manual* offers no assistance in this matter as it adopts the effective control test in Rule 6 without offering clarification. Since cyber-attacks of all types exist in international law, they constitute a near blameless weapon for states to utilize. As such, this study now turns to alternative theories for attribution outside of the ICJ/ARS paradigm to seek a means of holding states responsible for malicious cyber-attacks.

149 *See*, John Markoff and David E. Sanger, *In a Computer Worm, a Possible Biblical Clue*, N.Y. Times (Sept. 29, 2010), http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=all&r=0 (Discussing biblical references found within the computer code of the worm later named Stuxnet).

150 "A piece of physical or documentary evidence that conclusively impeaches an adversary on an outcome-determinative issue." Black's Law Dictionary 1516 (9th ed. 2011).

3.3. The Question of Proof: Attributing Actions to the Responsible State

The ARS does not concern itself with the rules of proof or evidence related to either a breach of a primary obligation or attribution. The ARS focuses on the secondary rules of attribution alone, creating a symbiotic relationship in which a host of varying primary obligations determines the quantum of proof needed for finding a breach of a primary obligation. This was sensible on the part of the ILC as it did not have to attempt to formulate a set of primary rules that could encompass the disparate primary norms in existence in international law. However, this refusal to address the issue of proof and evidence creates a tension between reality and scholarship: to be of practical use; the ARS needed to establish a minimum baseline since no such baseline of proof or evidence has been fully enunciated.

With the focus of the ARS solely on the breach of the primary obligation, the ARS allows the injured state to subjectively determine when and to what extent harm has occurred. This allows the state to subjectively determine both the quantum of proof and whether that burden has been met. One must remember that while the ICJ may proclaim one thing, the common law theory of stare decisis does not apply. States are free to decide actions based upon the individual matter at hand and not necessarily what the ICJ has previously stated, leaving the injured state free to respond as it deems necessary. CIL may be difficult to distinguish for the given matter, and without further guidance, a state will decide its actions based on practicality and politics rather than on international law. In short, by disregarding the issue of proof, the ARS has created a gray area within international law that allows states to act as they seem while still claiming the protection of the law.

For the purposes of discussing attribution and proof, this study addresses two primary sources. The first issue addressed concerns the prohibitions contained in U.N. Charter Art. 2(4) and the second concerns those prohibitions contained within the *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*.[151] This study utilizes these prohibitions as a means to demonstrate that the required proof of violations of the U.N. Charter Art. 2(4) which are arguably the gravest violations of international law and require

[151] G.A. Red. 2625 (XXV), U.N. GAOR, 25th Sess., U.N. Doc. A/RES/25/2625 (24 Oct. 1970).

a degree of proof higher than any other. This study will address the issues of proof as an element of the prohibition on the use of force, the non-intervention theory, and the *Principles of International Law concerning Friendly Relations*. This study discusses the non-intervention theory and the legal principles contained in the *Principles of International Law concerning Friendly Relations* as this study believes that the non-intervention theory is one of the most violated norms by malicious cyber-attacks. It must be noted that while this study does not, per se, address those cyber-attacks that violate the U.N. Charter Art. 2(4), Art. 2(4) is discussed herein so as to establish a baseline for the proof needed to demonstrate an internationally wrongful act to a state for purposes of attribution. U.N. Charter Art. 2(4) UN Charter establishes the baseline for comparison to all other lesser acts.

Second, the issue of CIL will be discussed in regards to the idea that malicious cyber-attacks may be seen as analogous to prohibited transboundary pollution and transboundary harm.[152] As such, the needed proof to demonstrate violations of the transboundary harm theory needs to be addressed. Transboundary harm is well established in CIL and lends itself well to the issue at hand. It is posited that by discussing both charter law and CIL, a general theory on the burden of proof and evidentiary standard for both areas may be discerned. It is recognized that this is a small sample of possible violations and is not offered to be dispositive for all potential charter law or CIL violations. This discussion is offered for demonstration purposes, and to stimulate for future conversations.

It must be reiterated that this study concerns malicious cyber-attacks that remain below the level of a use of force described in U.N. Charter Art. 2(4). However, as the majority of scholarship regards the use of force and cyber-attacks, this study will utilize the Art. 2(4) paradigm to illustrate the issues involved with attribution of cyber-attacks and proof thereof. This study will then utilize the lessons learned by analogy to the issue of malicious cyber-attacks. This study will discuss the quantum of proof needed to attribute violations of the impacted primary obligation, as delineated by the primary obligation involved, prior to discussing the current CIL regarding attribution and state responsibility.

152 *See*, Eric Talbot Jensen, *State Obligations in Cyber Operations*, (April 2, 2014). Baltic Y.B. Int'l L. forthcoming. Available at SSRN: http://ssrn.com/abstract=2419527 (cited with author's permission).

3.4. Proof and the UN Charter Article 2(4)

The U.N. Charter Art. 2(4) states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." The requisite evidentiary burden for demonstrating the use of force and the violation of art. 2(4) is a matter of some debate.

Proof or evidence of the use of force is not addressed within Art. 2(4), and the available ICJ case law is more concerned with defining force rather than the evidence or proof needed to demonstrate it.[153] Tsagourias summed up the issue of evidence for the use of force as "th[e] standards concerning the availability and probity of evidence in cases involving armed attacks, uses of force or interventions are rather lax."[154] This in part may be related to the traditional understanding of force; that is, force involves a kinetic event, which is an event that involves a physical, observable cause and effect. After a kinetic event, the impacted state could present proof gained through traditional criminal and intelligence services to demonstrate what state was responsible for the event. The question of state responsibility for a kinetic attack is normally a relatively straightforward proposition (with the exceptions of terror attacks or the involvement of non-state actors in kinetic attacks, which are more difficult as to matters of proof and attribution.) In this manner, an injured state merely needed to link a kinetic event in which force was utilized to the purported state believed to have used force before the injured state could legally respond in self-defense.[155]

153 *See*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) 1986 I.C.J. 14 (June 27) (The ICJ goes to great lengths to explain what does and does not constitute force, but says nothing about the evidence needed except to say that a right to self-defense was a subjective interpretation on behalf of the victim state. It must be noted that the ICJ in *Nicaragua* held that the right to self-defense was reserved only for use of force incidents attributed to state actors, a distinction that has been thoroughly repudiated by state practice and emerging CIL.)

154 Nicholas Tsagourias, *Cyber-attacks, Self-defence and the Problem of Attribution*, 17 J. Conflict & Security L. 235 (2012). *Cf.*, Michael N. Schmitt, *Responding to Transnational Terrorism Under the Jus ad Bellum* 83, *in*, Essays on Fault and War at the Fault Lines (2012) ("[I]nternational law contains no express evidentiary standard governing the quality of the information upon which States may resort to force in self-defense.")

155 Subject to the constraints of UN Charter Art. 51 and customary rules on *jus ad bellum*/*jus in bello*.

The evidence or proof of an attack needed for a state to respond in self-defense is subjective; it depends on the victim state's assessment of the attack. If an attack is of great enough magnitude to meet or exceed the scale and effect test[156] and be considered an armed attack, the injured state may respond in self-defense under art. 51 of the U.N. Charter, however, the injured state will bear the responsibility to demonstrate to a high degree of confidence of who was responsible and that the attack met the threshold to be considered an armed attack thus necessitating an action in self-defense. The focus of the needed evidence is on the attack itself, evidence of a subjective nature need not be demonstrated, the focus is solely on the objective nature of the attack.

Proving or delineating evidence of a cyber-attack that amounts to force is a different problem. Due to the nature of cyber-attacks, which is discussed in detail, infra, chapter four, there will be limited digital evidence of an attack, and depending on the state's interpretation of whether the cyber-attack constitutes a use of force, there may or may not be a kinetic effect from the attack. At present, there is no clear test or threshold for when a cyber-attack will rise to the level of force, how to identify those behind the attacks, and how to prove who is responsible for such an attack. One could adopt a mechanism similar to the strict liability approach for malicious cyber-attacks, in that any use of cyber-based weapons with a kinetic impact may equate to force; however, this only answers part of the question. The matter of proof, evidence, or attribution remains.

---

156 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) § 195, 1986 I.C.J. 14 (June 27). ("In the case of individual self-defence, the exercise of this right is subject to the State concerned having been the victim of an armed attack...There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also 'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (*inter alia*) an actual armed attack conducted by regular forces, "or its substantial involvement therein". This description, contained in Art. 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces. But the Court does not believe that the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the interna1 or external affairs of other States**.** It is also clear that it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked…")

The ICJ has stated that the greater the claim of wrongfulness against a state, the greater the degree of evidence that is needed to prove the wrongful conduct.[157] This idea also applies to cyber-attacks but may be difficult to implement in cyberspace where the majority of evidence will be indirect or circumstantial. In an ideal world, a state would only respond to cyber-attacks that amount to force if the injured state had clear and convincing evidence that the authors of an attack were state X, could prove the attacks originated from state X, and could legally attribute the attacks to state X. However, as a pragmatic argument, this idea of proof or evidence of the highest magnitude would only be effective before an international tribunal because states will respond to acts of force against them based on multiple factors, including a degree of evidence they alone deem necessary.

This study argues that, at a minimum, a state must possess clear and convincing evidence that a state is responsible for a cyber-attack prior to taking acts against that state in self-defense. As Professor Michael Schmitt stated:

> [c]lear and convincing evidence is a level more probative of the issue at hand than ‘‘preponderance of the evidence,’’ which simply means that the evidence makes the matter more likely than not. It is, on the other hand, less probative than the ‘‘beyond a reasonable doubt’’ standard typically required for a guilty finding in a criminal case. Used in the context of justifying a use of force, clear and convincing evidence of a forthcoming armed attack is evidence that would convince a reasonable State to act defensively in same or similar circumstances.[158]

Schmitt justified the clear and convincing evidentiary standard for the use of force and self-defense by positing that "[i]n light of the near universal characterization of OEF [Operation Enduring Freedom] as lawful, it appears that the international community accepts 'clear

---

157 Case Concerning Application of the Convention on Prevention and Punishment of the Crime of Genocide (Bos. & Herz. v. Serbia /Montenegro), 2007 I.C.J. 43, 90 – 91 § 208-210.

> ("[T]he Court requires proof at a high level of certainty appropriate to the seriousness of the allegation…The Court has long recognized that claims against a State involving charges of exceptional gravity must be proved by evidence that is fully conclusive…The Court requires that it be fully convinced that allegations made in the proceedings, that the crime of genocide or the other acts enumerated in Article III have been committed, have been clearly established. The same standard applies to the proof of attribution for such acts...")

158 Michael N. Schmitt, *Responding to Transnational Terrorism Under the Jus ad Bellum* 84, in, Essays on Fault and War at the Fault Lines (2012).

and compelling' as an appropriate evidentiary standard in self-defense cases."[159] Schmitt premised his belief on the UN Security Council's acceptance of United States Ambassador John Negroponte's statement regarding the September 11th terrorist attacks to the Security Council, in which Ambassador Negroponte stated that the United States had "obtained clear and compelling information that the Al-Qaeda organization, which is supported by the Taliban regime in Afghanistan, had a central role in the attacks."[160]

Given that the majority of evidence in malicious cyber-attacks will be circumstantial, a higher burden of proof would be unreasonable. A higher evidentiary burden, proof beyond a reasonable doubt, requires that the proof "precludes every reasonable hypothesis except that which it tends to support"[161] or simply, that there is no plausible explanation that another state could be responsible for the attack. For instance, this is the burden of proof adopted by the International Criminal Court as the necessary burden of proof for a criminal conviction.[162] However, such a burden of proof cannot work for cyber-attacks; first, the forensic abilities of computer science for technical attribution cannot, in the majority of

159 *Id.*

160 *Id.* quoting, Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, UN Doc. S/2001/946 (October 7, 2001). *See also*, Black's Law Dictionary 635 (9th ed. 2011). ("Clear and convincing proof" is that the "[e]vidence indicating that the thing to be proved is highly probably or reasonably certain."). *Cf. Microsoft v. i4i Ltd*., 131 S.Ct. 2238 (2011) (Thomas J. Concurring) n.4 -5 (Discussing the terms clear and convincing and burden of proof). *See also*, *Santosky v. Kramer*, 455 U.S. 745, 756 (1982) ("This Court has mandated an intermediate standard of proof—'clear and convincing evidence'—when the individual interests at stake in a state proceeding are both 'particularly important' and 'more substantial' than mere loss of money.")

161 Black's Law Dictionary 1334 (9th ed. 2011). *See also, Miles v. United States*, 103 U.S. 304 (1881) ("The evidence upon which a jury is justified in returning a verdict of guilty must be sufficient to produce a conviction of guilt, to the exclusion of all reasonable doubt..."). Rome Statute of the International Criminal Court art. 66(3) U.N. Doc. A/CONF.183/9 (as corrected 12 July 1999) ("In order to convict the accused, the Court must be convinced of the guilt of the accused beyond reasonable doubt."). *But cf.* Tony Gerdwin-Meyer, *What Probability is Involved in "Beyond Reasonable Doubt" in Criminal Trials?* Kings College London (2014), http://www.ucl.ac.uk/ ~ucgbarg/doubt.htm (Arguing that the "beyond reasonable doubt" threshold be based upon the theory that "the probability of guilt, is a Bayesian probability: it is the degree of belief that the facts could have arisen consistent with innocence [i.e., broadly, that the defense account is plausible]. If this proposition is capable of reasonable belief, above some low threshold probability, then the jury should acquit—even if it may appear much more likely that the evidence arose through guilt.").

162 Rome Statute of the International Criminal Court art. 66(3) U.N. Doc. A/CONF.183/9 (as corrected 12 July 1999).

cases, find such evidence for cyber-attacks, and second, because this is not a question of criminal liability.[163]

It is recognized that the application of the clear and convincing burden of proof is highly malleable depending upon the victim state's interpretation of the facts. However, by elucidating a standard for the burden of proof, it enables a baseline for the minimum proof needed to invoke the right to self-defense and for the purposes of attributing a use of force to a state. It also establishes a baseline of evidence needed to attribute cyber-attacks and the needed burden of proof for the implementation of any other form of liability. The clear and convincing burden should not be viewed as the maximum level of proof a state must possess, but as the minimum evidence needed. The greater the proof, the more justified the response to a cyber-attack.

3.5. Proof of Unlawful Political Intervention: General Discussion

For the purposes of this study, the principle of unlawful political intervention is based on principles elucidated in the *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, the U.N. Charter art. 2(1), and CIL.[164] Together, these sources form the basis for the theory of unlawful political intervention as discussed within this study. This study will address unlawful political intervention as a general matter for the purposes of the discussion on proof and will discuss the *Principles of International Law concerning Friendly Relations* in specific, infra. This study discusses these ideas separately to demonstrate that the ideas behind unlawful political intervention exist in international law in multiple forms.

While non-intervention[165] is often cited in UNGA debate, Security Council resolutions and some treaties, the exact boundaries of what may or may not be unlawful political

---

164 U.N.G.A. Res. 2635 (XXV) (24 Oct. 1970), U.N. Doc. A/Res/25/2625 (1970).

165 The terms unlawful political intervention and non-intervention are used in the same manner by many commentators, this study utilizes the term unlawful political intervention to distinguish the issue from that of unlawful intervention which may also encompasses the use of force which is not part of the instant discussion, however where commentators use the term non-intervention it is

intervention has yet to be truly delineated.[166] Jamnejad and Wood posited that unlawful political intervention consists of "[t]wo elements...First, there must be an 'intervention' by one state in the affairs of another. Second, the intervention must bear on 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely."[167]

Oppenheim believed that such intervention as posited by the first element *supra* must be dictatorial in nature.[168] Oppenheim described dictatorial intervention:

> [i]ntervention is dictatorial interference by a State in the affairs of another State for the purpose of maintaining or altering the actual condition of things. Such intervention can take place by right or without a right, but it always concerns the external independence or the territorial or personal supremacy of the respective State…[169]

Jamnejad and Wood noted that intervention, as used in the term non-intervention is misunderstood and ill-defined, stating that "[w]hat constitutes an 'intervention' is nowhere set out clearly" in international law.[170] Jamnejad and Wood utilized the term to denote "cases where coercive action is taken by one state to secure a change in the policies of another."[171] Hence a violation of non-intervention principle equates to unwanted or illegal coercion on behalf of a state.[172] However, it must be recognized that not all intervention is

---

not changed within this study. Some commentators also refer to this idea as "non-interference in domestic affairs" *see*, Michael Wood, *Non-Intervention (Non-Interference in Domestic Affairs), in*, Encyclopedia Princetoniensis (2017), https://pesd.princeton.edu/?q=node/258.

166 Maziar Jamnejad and Michael Wood, *The Principle of Non-Intervention*, 22 Leiden J. Int'l L. 345-348 (2009).

167 *Id.* at 347 (internal citations omitted).

168 1 Lassa Oppenheim, *International Law: A Treatise. Peace* § 134 (2 ed. 1912, Kindle ed. 2012). *See also, Id.* (quoting Oppenheim).

169 1 Lassa Oppenheim, *International Law: A Treatise. Peace* § 134 (2 ed. 1912, Kindle ed. 2012). *See also, Id.* (quoting Oppenheim).

170 Maziar Jamnejad and Michael Wood, *The Principle of Non-Intervention*, 22 Leiden J. Int'l L. 345, 347 (2009).

171 *Id.* at 348, citing *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations*, G.A. Res. 26/25 (XXV), UN Doc. A/Res/2625(XXV) (24 Oct. 1970) ("No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from its advantages of any kind.").

172 *Id.*

illegal or unwanted. Oppenheim suggested that a third state may take certain actions which may be considered as intervention but for lawful purposes. Oppenheim argued that it may be lawful for a third state to act by intervening in a conflict to spur negotiations or seek a peaceable end to a conflict.[173] Oppenheim puts forth various types of intervention that are not dictatorial in nature and are to the benefit of a state that does not amount to an unlawful act.[174]

The ICJ stated in *Nicaragua* that non-intervention equated to unlawful coercion in some areas, such as those sovereign dealings in "political, economic, social and cultural system[s], and the formulation of foreign policy."[175] In addition, the court "held that the [non-intervention] principle forbids all states or groups of states to intervene directly or indirectly in the internal or external affairs of a state."[176]

One may posit that the principle of non-intervention may be viewed as a continuum ranging from minor infractions to major infractions. Thus, if one is to follow the ICJ suggestion on evidentiary weight, the evidentiary burden grows with the claimed level of wrongdoing. Or, one could view the principle in which any violation of the principle could be a violation, thus invoking a set standard for evidentiary purposes. Prior to discussing this dichotomy and the evidentiary weight needed to prove a violation of the CIL regarding non-intervention, this study must first discuss non-intervention in the context of malicious cyber-attacks to establish whether a malicious cyber-attack may rise to the level of prohibited non-intervention.

---

173 1 Lassa Oppenheim, *International Law: A Treatise. Peace* 211-214 (2 ed. 1912, Kindle ed. 2012).

174 1 Lassa Oppenheim, *International Law: A Treatise. Peace* 211-214 (2 ed. 1912, Kindle ed. 2012).

175 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) § 205, 1986 I.C.J. 14 (June 27). Maziar Jamnejad and Michael Wood, *The Principle of Non-Intervention*, 22 Leiden J. Int'l L. 345, 348 (2009).

176 *The Tallinn Manual on the International Law Applicable to Cyber Warfare* 144, cmt. 7 (Michael N. Schmitt ed. 2013). *See also*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) § 205, 1986 I.C.J. 14 (June 27).

3.5.1. Malicious Cyber-Attacks and Unlawful Political Intervention: Defining the Problem

The *Tallinn Manual* states that "[i]f [] cyber operations are intended to coerce [a] government (and are not otherwise permitted under international law), the operation may constitute a prohibited 'use of force.'"[177] However, even those cyber operations that do not rise to the level of force may violate the principle of non-intervention. The *Manual* suggests as much in the commentary to Rule 10:

> [t]he fact that a cyber operation does not rise to the level of a use of force does not necessarily render it lawful under international law. In particular, cyber operations may constitute a violation of the prohibition on intervention. Although not expressly set out in the United Nations Charter, the prohibition of intervention is implicit in the principle of the sovereign equality of States as laid out in Article 2(1) of the United Nations Charter…[178]

Such acts of non-intervention, those that arguably do not meet the use of force threshold,[179] have already occurred, most notably with the cyber-attacks on Estonia and Georgia. There, malicious cyber-attacks (DoS/DDoS attacks) that were never legally attributed (but widely believed to be acts taken by patriot hackers on behalf of Russia) were carried out to punish a sovereign state (Estonia) and as an adjunct to kinetic warfare (Georgia). Both acts standing alone constitute a violation of the principle of non-intervention / unlawful political intervention in that the cyber-attacks were meant to coerce a sovereign state, in an attempt to force a state to take another course of action in its internal political considerations (Georgia) and punish a state for a domestic act (Estonia).

As CIL emerges and evolves in regard to the use and impact of malicious cyber-attacks, this study will posit that the impact and effect of malicious cyber-attacks will prompt a reassessment of what constitutes prohibited non-intervention / unlawful political intervention. An argument may be made that malicious cyber-attacks or militarized cyber-attacks prompted by states or acquiesced to by states, will be seen as violating the CIL of

177 *The Tallinn Manual on the International Law Applicable to Cyber Warfare* 17 (Michael N. Schmitt ed. 2013).

178 *Id.* at 44, cmt. 6.

179 As used in this example, the use of force threshold would be an attack resulting in kinetic impact and causing kinetic damage.

non-intervention. In addition, such acts as cyber-espionage, DDoS attacks, and even widespread spamming of computer systems could potentially rise to the level of unlawful intervention by a state. However, this idea of malicious cyber-attacks as violating the non-intervention principle creates a circular problem. If the original concept of non-intervention is ill-defined and poorly understood, then positing that cyber-attacks, which themselves are ill-defined and poorly understood, violate the concept of non-intervention creates an issue without clear definition or solution.

As such, this study will discuss how one may define the parameters of the principle of non-intervention in regard to malicious cyber-attacks. To understand the concept of non-intervention, one needs to understand the relationship of non-intervention and the concept of sovereignty. The *Tallinn Manual* relates non-intervention to the UN Charter Art. 2(1), concept of sovereignty, without discussion of either Art. 2(1) or how one is to understand what sovereignty involves.[180] For the purposes of this study, sovereignty in international law may be understood as those rights and privileges inherent within an independent state; simply put, sovereignty is the state itself at its simplest.[181]

Cyber-attacks may take numerous forms ranging from minor incidents to full-blown use of force events with kinetic impact or effect. While a full range of cyber-attacks may violate the non-intervention principle as discussed *supra*, it is the lesser forms of attacks—those not reaching the use of force level—that may constitute a violation of the non-intervention principle and are of importance herein. Any state-sponsored malicious cyber-attack which is launched with the objective intent to interfere with the sovereignty of a state would violate the non-intervention principle, whether directly attributable to a state or to a non-state actor. In this respect, the non-intervention principle would cover a variety of malicious cyber-attacks judged solely by the objective intent and application of the attack. For example, the DDoS attacks against Estonia, where the attacks objectively happened in retaliation for a decision by Estonia to remove a statue of a Russian soldier and were

180 *The Tallinn Manual on the International Law Applicable to Cyber Warfare* 17 (Michael N. Schmitt ed. 2013).

181 *See*, Black's Law Dictionary 1524 (9th ed. 2011) (Defining sovereignty as "1. [s]upreme dominion, authority or rule. 2. The supreme political authority of an independent [S]tate. 3. The [S]tate itself.").

arguably launched to punish and make Estonia reconsider its actions, violate the principle of non-intervention. The DDoS attacks were meant to coerce or punish a state for an act which was solely under the jurisdiction and sovereignty of the state.

The range of malicious cyber-attacks that may be used by a state to violate the principle of non-intervention is only restricted by the technical ability and imagination of those who are using cyberspace to influence the political activities within a sovereign state. As such, a true definition of malicious cyber-attacks that may violate the non-intervention principle would be impossible to propagate. However, this study would posit the following elements that need to be present in order to claim a violation of the non-intervention principle via malicious cyber-attacks: (1) computer code is used by a state via cyberspace or other vector with the objective intent to (2) unlawfully interfere with the internal affairs of a sovereign state[182] or attempt to coerce a sovereign state (3) regarding the acts and powers reserved to a sovereign state (4) based upon an objective observer's understanding of the act.

This study argues that the theory of non-intervention/ unlawful political intervention should be understood as prohibiting states from attempting to impose their political will upon another state through actions within the state's sovereign territory whether physical or cyber. As Oppenheim related, it is the dictatorial[183] nature of the intervention that makes it wrongful. Dictatorial should be understood as forceful, unfair, overbearing, or unwanted in content and nature. Hence, malicious cyber-attacks that are more than nuisance attacks, but that fall short of force and are launched to either prevent a state from taking action or for the purpose of punishing a state for an act are dictatorial.

3.5.2. The Burden of Proof and Unlawful Political Intervention

The burden of proof for the non-intervention principle suffers from the same issues like those associated with proving who is responsible for use of force incidents; that is, no clear standard of proof has been elucidated. Given the subjective nature of the non-intervention

182 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) § 186, 1986 I.C.J. 14 (June 27).

183 Lassa Oppenheim, *International Law: A Treatise. Peace* 211-214 (2 ed. 1912, Kindle ed. 2012).

principle, a clear theory of proof must be formulated prior to assessing how a state is to be held responsible for violating said principle.

From the outset, this study argues that any proof needed to demonstrate a violation of the non-intervention principle must be based on an objective standard, i.e., how an independent reasonable person would prima facie interpret the acts of the offending state. Too often states "wear their feelings on their sleeves" in response to any perceived slight or interference with domestic politics, creating a motive to turn a slight into a greater issue than it is. Add to this, the internal politics of a state, and it is likely that any perceived subjective intervention may be used for domestic political reasons. It is recognized that this proposition is at odds with the ICJ's decision in *Nicaragua*, where the court held that the use of force was a subjective interpretation by the victim state.[184] However, unlike kinetic force in which the evidence of an attack is readily visible, unlawful intervention via cyberspace is more difficult to demonstrate. A state should bear the burden of demonstrating to an objective standard how the principle of non-intervention was violated.

One may determine that any objective evidence of a violation of the principle of non-intervention is enough to demonstrate a violation of the principle. Simply stated, there is no true demarcation in international law of when the violation blooms; there is a violation, or there is not. If a state acts contrary to the rights of another state within the elements posited, then the state is responsible for said actions. In this manner, the intent of the offending state is irrelevant, and mens rea need not be demonstrated. It is not necessary to prove that a state intended to intervene; only that it has intervened contrary to the rights and wishes of the victim state.

If we approach the burden of proof utilizing the sliding scale principle,[185] much as the ICJ has in its jurisprudence, the continuum of international wrongs would have non-intervention below the use (or threat of the use) of force. One could argue that the burden

184 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) § 186, 1986 I.C.J. 14 (June 27).

185 Fredric L. Kirgis, *Custom on a Sliding Scale*, 81 Am. J. Int'l L. 146 (1987). Case Concerning Application of the Convention on Prevention and Punishment of the Crime of Genocide (Bos. & Herz. v. Serbi. /Montenegro), 2007 I.C.J. 43, 129 ¶ 209-210.

of proof then is of a lesser order than that of use of force. One could further argue that a burden of proof akin to the simple preponderance of the evidence, in which a rational arbiter of fact simply assesses the evidence based upon what is most convincing,[186] would suffice to show that a state has violated the principle of non-intervention. However, this is an arguably insufficient a policy; while the policy of non-intervention is a lesser charge as it was, it is a serious breach of CIL and one that arguably may lead to even greater violations of international law up to and including the use of force.

Lastly, it is argued that the ICJ jurisprudence on the issue of the burden of proof has led to much confusion on the subject and allows for too much subjective interpretation of the facts and law on behalf of states and the court. As such, it is argued herein that the clear and convincing burden should be adopted as the minimum standard of proof for any violation.

The clear and convincing standard of proof creates a minimum basis of evidence needed for the proper attribution of state responsibility for violation of the principle of non-intervention via a malicious cyber-attack. As malicious cyber-attacks are difficult to properly attribute to a state or a third party, a set standard of proof is needed. Clear and convincing evidence would set a standard that is fair to the accused and to the victim. The clear and convincing standard allows for the objective decision maker to assess the likelihood of a state being responsible for a malicious cyber-attack. It "precludes every reasonable hypothesis except that which it tends to support."[187] This standard recognizes the difficult nature of evidence-gathering in cyber-attacks and allows the decision maker reviewing the proffered evidence a method of fairly assessing the proof thereof.

---

186 Black's Law Dictionary (9th ed. 2011) ("The greater the weight of the evidence, not necessary established by the greater number of witnesses testifying to a fact but by evidence that has the most convincing force; superior evidentiary weight that, though not sufficient to free the mind wholly all reasonable doubt, is still sufficient to incline a fair and partial mind to one side of the issue rather than the other.").

187 Black's Law Dictionary 1334 (9th ed. 2011). *See also*, *Miles v. United States*, 103 U.S. 304 (1881) ("The evidence upon which a jury is justified in returning a verdict of guilty must be sufficient to produce a conviction of guilt, to the exclusion of all reasonable doubt..."). Rome Statute of the International Criminal Court art. 66(3) U.N. Doc. A/CONF.183/9 (as corrected 12 July 1999) ("In order to convict the accused, the Court must be convinced of the guilt of the accused beyond reasonable doubt.").

3.6. Proof and the Principles on International Law Concerning Friendly Relations

This study now turns to specific principles set forth in the *Principles on International Law concerning Friendly Relations*, which malicious cyber-attacks may violate when those attacks are less than the use of force but are utilized by another state to intervene with domestic policy questions or equal rights and self-determination of a people or state. This study utilizes specific principles to demonstrate this issue. Specifically:

- The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter…
    - No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention **and all other forms of interference** or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law…
    - No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State…
    - Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State.[188]
- The principle of equal rights and self-determination of peoples
    - By virtue of the principle of equal rights and self-determination of peoples enshrined in the Charter of the United Nations, all peoples have the right freely to determine, without external interference, their political status and to pursue their economic, social and cultural development, and every State

[188] *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations*, G.A. Res. 26/25 (XXV), UN Doc. A/Res/2625(XXV) (24 Oct. 1970). (Emphasis added).

> has the duty to respect this right in accordance with the provisions of the Charter.[189]

These principles, which are derived from charter law and exist as CIL, could arguably, be the most violated prohibition with regard to malicious cyber-attacks. Particularly in cases such as Estonia and Georgia when the malicious cyber-attacks were directed at the personality of the state for actions the state had taken in furtherance of its own domestic agenda and political self-determination. Any malicious cyber-attack which violates the principles contained within the friendly relations principles would constitute an internationally wrongful act. Establishing when this occurs will be discussed infra.

3.6.1. Establishing a Violation of the Legal Principles Contained in the Principles of International Law Concerning Friendly Relations

Establishing when a malicious cyber-attack violates the legal principles contained in the *Principles of International Law Concerning Friendly Relations* for the purposes of establishing an internationally wrongful act is theoretically straightforward. However, it is much more of a challenge for an injured state to demonstrate a violation of the friendly relations principles as opposed to the use of force prohibition. As discussed above, the demonstration of a kinetic impact irrespective of its cause is much easier than demonstrating a wholly digital harm.

In theory, it is easy to imagine how a malicious cyber-attack could unlawfully interfere with international peace and security or violate the principles of friendly relations. For example, one could argue that any substantive malicious cyber-attack is violative of the principles of friendly relations. However, the actual demonstration of such an event is difficult. While this applies to the majority of cyber-attacks as a whole, other types of malicious cyber-attacks may be easier to demonstrate and to comprehend.

189 *Id.*

As with all evidentiary issues, the onus of demonstrating the violation is upon the state making a claim. The better a state may demonstrate the harm suffered; the more likely the claim will be accepted. Ideally, the injured state would ab initio be able to demonstrate a clear and convincing level of evidence demonstrating the harm that has been suffered and how the harm is an internationally wrongful act. This may be the case when the harm suffered is the result of a large-scale malicious cyber-attack, particularly where recursive traceback demonstrates that the IP address from which the attack was initiated is a government controlled IP address.[190] However, even then, it is difficult to link the IP address to a state agent for the purposes of attribution. Such straightforward attacks are not the norm.

Individual malicious cyber-attacks that do not constitute internationally wrongful acts by themselves may progress over an extended timeframe and reach the needed scale or effect overall to constitute an internationally wrongful act. This complicates the issue of proof, as each malicious cyber-attack may have been launched from disparate IP addresses linked to the same state or multiple states. This difficulty combined with the possibility that the malicious cyber-attacks may originate from spoofed IP addresses may make it extremely difficult for a state to demonstrate that it has suffered an internationally wrongful act. As such, states may have to take a totality of the circumstances approach, utilizing circumstantial evidence alone in an attempt to demonstrate the internationally wrongful act and attribution of the same. Demonstrating the proof of such an act will be discussed in the next section.

3.6.2. Proof of Violations of the Friendly Relation Principles

Much like the other charter law prohibitions discussed *supra*, it is arguable that a violation of the friendly relations principles is one of the most serious offenses in international law. This proposition is supported by the idea that a violation of the friendly relations principles is an act against the very purpose of the UN Charter and an affront to the very heart of

190 *Cf.* Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, (Feb. 2013), http://intelreport.mandiant. com/Mandiant_APT1_Report.pdf. (Discussing the attribution of cyber-attacks and cyber-espionage to the Chinese military, in part due to the originating IP addresses being under the sole control of the Chinese government).

international law. As such, it may be argued that the violation thereof is a most serious violation, and the proof needed to demonstrate such an internationally wrongful act "appears to be considerably higher, shifting toward clear and convincing."[191] As discussed *supra*, clear and convincing proof of a violation would require a higher burden of proof, particularly when those violations involve more serious allegations against states and/or, as posited by Geiß and Lahmann, touch upon state responsibility.

The violation of the friendly relations principles is subjective in that the violation is to be determined by the injured state. Complicating this, as with all malicious cyber-attacks, is the problem of finding objective proof of the violation. The evidence of a malicious cyber-attack will be based upon digital evidence obtained after the fact; server log files, IP router tables, or user log files may be utilized to help traceback the malicious cyber-attack to the initial IP address. Computer algorithms and other technical means of attempting traceback may also be utilized. However, these methods are subject to the issues of any other forms of evidence where bias, tampering, spoliation, and numerous other issues may impact the validity of the digital evidence acquired. Also, the authors of the attacks may utilize techniques to obfuscate the evidence or lay a false trail to invite reprisal against an innocent party. Thus, as a theoretical exercise, the gathering of evidence of sufficient quantity and veracity to satisfy the clear and convincing burden will be extremely challenging for injured states.

3.7. Proof and Violations of Customary International Law

This study now shifts focus from charter law and the issues of proof to the issue of proof relating to violations of CIL, two distinct paradigms in international law. This section will discuss the required proof needed to demonstrate violations of CIL. As there may be multiple possible violations of CIL relating to malicious cyber-attacks, this study will address the general prescription of "every state's obligation not to allow knowingly its

191 Robin Geiß and Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus Away from Military Response Toward Non-Forcible Countermeasures and Collective Threat-Prevention*, 621, 624, *in,* Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy (Katharina Ziolkowski ed. 2013).

territory to be used for acts contrary to the rights of other states."[192] This obligation consists of two interrelated ideas: the first, "the obligation to not knowingly injure another state (*sic utere tuo ut alienum non laedas*),"[193] use your own property in such a way that you do not injure other peoples';[194] and second, the state's duty to prevent harm.[195] The court in the *Corfu Chanel* case recognized this obligation as a "general and well-recognized principle[]"[196] of CIL.[197] As discussed *infra* Chapter Five, malicious interstate cyber-attacks that cause harm in another state may violate this CIL prohibition.[198] This interstate prohibition on harm is one method for a state injured by a malicious cyber-attack to seek justice before the ICJ.

As Jensen posited, a state has an affirmative duty to prevent its cyberinfrastructure from being utilized by state or non-state agents to cause harm to another state.[199] Sklerov stated that "[i]t is a long established principle of international law that a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another

---

192 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9).

193 Michael Waibel, *Corfu Channel Case*, Max Planck Encyclopedia of Public International Law (2015), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690e118?rskey= ryWdZN&result=1&prd=EPIL.

194 Oxford Dictionary of Law, *Sic Utere Tuo ut Alienum Non Laedas* (7ed., Jonathan Law and Elizabeth A. Martin eds. 2014). http://www.oxfordreference.com/view/10.1093/acref/9780199551248.001.0001/acref-9780199551248-e-3646.

195 Corfu Channel, at 22.

196 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9).

197 Trail Smelter Case (U.S. v. Can.), 3 Rep. Int'l Arb. Awards 1905, 1965 (11 Mar. 1941). ("Under the principles of international law…no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein…"). *See also, id.* at 1963 *quoting* Clyde Eagleton, *Responsibility of States in International Law* 80 (1928) ("A State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction."). *See also*, Corfu Channel Case (U.K. v. Alb.) Judgment, 1949 I.C.J. Rep. 4, 22 (April 9).

198 Eric Talbot Jensen, *State Obligations in Cyber Operations*, (April 2, 2014). Baltic Y.B. Int'l., forthcoming. Available at SSRN: http://ssrn.com/abstract=2419527 (cited with author's permission).

199 *Id.*

nation or its people."[200] A state has a duty to prevent harm to another state irrespective of the source of the harm.[201] The duty to prevent harm is discussed in depth *infra* Chapter Six. This section will briefly address the proof needed to demonstrate a violation of these principles, beginning with a brief discussion of what harm is in relation to malicious cyber-attacks.

3.7.1. The Concept of Harm Relating to Malicious Cyber-Attacks

In the instant context, it is necessary to distinguish the concept of harm from that of internationally wrongful conduct. To put it simply, under the ARS, an internationally wrongful act does not have to result in actual harm. The internationally wrongful act itself is what engages the ARS for the purposes of establishing international responsibility. However, other theories of CIL which will be discussed *infra* require a harm to engage the state for purposes of holding the state accountable for those actions. For example, the duty to do no harm theory requires a harm for the CIL prohibition to engage as a matter of international law and for the purposes of the violation being an internationally wrongful act.

This study will briefly discuss the idea of harm so as to demonstrate its applicability to the issue presented, as the evidence of harm may be necessary to link the internationally wrongful act to a state. Evidence of harm caused by state A to state B may be needed to engage a specific rule of CIL; the violation of that rule on behalf of a state may then be seen as an internationally wrongful act. This discussion will serve as a means of clarification to ensure a better-shared understanding and to establish a baseline of understanding going forward.

The harm from malicious cyber-attacks is wide-ranging, from economic harm to physical harm, and it may include harm to private and public property. Malicious cyber-attacks that

200 Matthew J. Sklerov, *Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 20 Mil. L. Rev. 1, 14 (2009).

201 *See*, International Law Commission, *Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities*, gen. cmt. § 1-5, U.N. GAOR, 53rd Sess. at 148, U.N. Doc. A/56/10 (2001).

cause harm cover a wide spectrum of potential malicious cyber-attacks. The range of malicious cyber-attacks may encompass such items as common spam emails that cost businesses money and productivity, to commercial cyber-espionage and traditional cyber-espionage against a state that causes economic or physical harm.

Harm is the key element for finding violations of the CIL regarding the duty to do no harm. Attribution questions aside, the issue is at what level the harm from cyber-attacks violates this prohibition. To answer this question, this study will look at malicious cyber-attacks and the theory of transboundary harm. The ILC, *Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities* (PTHHA) hold that the harm must be significant.[202] The PTHHA holds that the harm may be to "person[s], property, or the environment."[203] The PTHHA, as a pre-cyber document does not address the issue of cyber-attacks in any form. Instead, the PTHHA limits its coverage to harm that causes physical damage. As such, cyber-attacks with a kinetic impact would be covered under the PTHHA, while malicious cyber-attacks are in doubt. As the PTHHA has not been updated since 2001, this study must hypothesize that malicious cyber-attacks could fall within the PTHHA definition of transboundary harm if the PTHHA were brought into the cyber age. This hypothesis is supported by the comments to Art. 1 of the PTHHA in which the PTHHA promulgates a cause and effect test for determining transboundary harm. The PTHHA states that a "link must connect the activity with its transboundary effects. This implies a connection of a very specific type—a consequence which does or may arise out of the very nature of the activity or situation in question."[204]

Although the PTHHA was discussing a physical link, a link may be demonstrated between a malicious cyber-attack and the corresponding transboundary harm; i.e., the consequence

---

202 *Id.* at art. 1. *Cf.*, Alexendre Kiss and Dinah Shelton, *Strict Liability in International Environmental Law*, GWU Legal Studies Research Paper No. 345; GWU Law School Public Law Research Paper No. 345, http://ssrn.com/abstract=1010478.

203 International Law Commission, *Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities*, art. 2(b), U.N.GAOR, 53rd Sess. at 148, U.N. Doc. A/56/10 (2001). (This study would broaden this classification to encompass digital and/or cyber damage without a kinetic impact, thus allowing cyber-attacks to be considered transboundary harm.)

204 International Law Commission, *Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities*, gen. cmt. §17, U.N.GAOR, 53rd Sess. at 148, U.N. Doc. A/56/10 (2001).

of the malicious cyber-attack arises out of the very nature of the states using malicious cyber-attacks, or allowing non-state actors to carry out malicious cyber-attacks, or by not preventing the same. Thus, it is argued that malicious cyber-attacks may constitute harm.[205] This idea is supported by the fact that malicious cyber-attacks do cause physical harm due to the costs associated with the damage done. The damage may be digital, but the loss is physical in regard to the monetary damage suffered and the costs to rectify the damage after the fact. It is therefore argued that malicious cyber-attacks are a harm that a state has an affirmative duty to prevent as long as the harm is significant, impacts persons, property, and/or the environment, and there is a link between the malicious cyber-attack and the transboundary harm.

The proof needed to link the harm resulting from a malicious cyber-attack to a state was put forth in the *Trail Smelter* arbitration. In *Trail Smelter*, the arbitrators adopted the United States common law burden of clear and convincing evidence needed to link transboundary evidence of pollution to the offending state. The tribunal stated that "to control the conduct of one state at the suit of another, the threatened invasion of rights must be of serious magnitude, and it must be established by clear and convincing evidence."[206] While the tribunal was applying United States case law to the issue at hand, it qualified this adoption by stating, "no contrary rule prevails in international law and no reason for rejecting such precedents can be adduced from the limitations of sovereignty inherent in the Constitution of the United States."[207]

Since the adoption of this rule by the tribunal, the effects and widespread impact of transboundary pollution have grown.[208] With the growth, the debate over the evidentiary requirements to prove transboundary pollution has also been called into question. D'Amato

---

205 *Id.*

206 Trail Smelter Case (U.S. v. Can.), 3 Rep. Int'l Arb. Awards 1905, 1964 (11 Mar. 1941). (Discussing *Kansas v. Colorado*, 185 U.S. 125(1902) and *Missouri v. Illinois*, 200 U.S. 496 (1906)).

207 *Id. See also*, Thomas W. Merrill, *Golden Rules for Transboundary Pollution*, 46 Duke L. J. 931 (1997) (Discussing the clear and convincing rule in transboundary pollution cases).

208 *Cf.* Anthony D'Amato, *Transboundary Pollution* (2001), http://anthonydamato.law.northwestern.edu/IELA/Intech08-2001-edited.pdf.

discussed Kirgis' "modified standard of proof approach,"[209] which may be stated as the greater the harm done, the less the burden of proof. This approach, while viable for transboundary pollution where evidence is more easily obtainable, is not ideal regarding malicious cyber-attacks where a single incident may trigger a catastrophic event and yet be completely anonymous. As such, prior to acting in such an incident, a state must possess a higher degree of objective evidence. This study would hold that the standard first elucidated by the *Trail Smelter* tribunal of clear and convincing evidence is needed to attribute a malicious cyber-attack to a state or non-state actor for a violation of customary international and the duty to do no harm.

209 *Id.* at 113.

Chapter Four: Technical Attribution of Cyber-Attacks

This study now turns to an in-depth discussion concerning the technical aspects of the Internet and cyber-attacks. This study does so as to demonstrate the difficulties involved with attributing cyber-attacks and to discuss the Internet and cyberspace as a shared common. This study undertakes this discussion to ensure that the issue of legal attribution of malicious cyber-attacks is viewed through the understanding of how the digital commons works and the difficulties that malicious cyber-attack attribution poses to computer science. This study operates on the premise that legal theory alone is not enough to deal with the instant issue of this study and must be taken in context along with the technical realities.

Once this study concludes the discussion regarding the technical aspects of malicious cyber-attacks, this study will engage in a discussion regarding hybrid attribution or what some commentators refer to as circumstantial attribution. This form of attribution is probably the most prevalent form of attribution utilized by states when dealing with the attribution of cyber-attacks. This study uses the term probably as states have not disclosed their methods of attributing cyber-attacks. But, as Goldsmith argued,[1] states most likely use a hybrid form of attribution; utilizing traditional intelligence, cyber-forensics, IP traceback, or other various techniques to attribute attacks. It is debatable whether this type of attribution is enough to establish state responsibility. In addition, for this form of attribution to work, states must disclose the means and methods and the evidence derived therefrom for attribution to be accepted by either the public or juridical bodies; information states will be loath to disclose lest potential advisories learn a state's cyber capabilities.

This study utilizes the term "technical attribution" to ensure compliance with terminology utilized in computer science.[2] Both computer science and legal scholarship utilize the term

[1] Jack Goldsmith, *The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance*, LAWFARE (Dec. 19, 2014), https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance. *Cf.* Jack Goldsmith, *Yet More Thoughts on the DNC Hack: Attribution and Precedent*, LAWFARE, (July 27, 2016), https://www.lawfareblog.com/yet-more-thoughts-dnc-hack-attribution-and-precedent. *Bears in the Midst: Intrusion into the Democratic National Committee*, CrowdStrike (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[2] *See*, Andrew Nicholson, *et al.*, *A Taxonomy of Technical Attribution Techniques for Cyber Attacks* 188, European Conference on Information Warfare and Security (Jul. 2012). (Discussing technical attribution techniques for attributing cyber-attacks.).

attribution in similar but distinct ways. To avoid confusion between the different types of attribution, this study refers to attribution as used by computer science as "technical attribution" and legal attribution as "attribution." For the purposes of this study, the definition put forth by Wheeler and Larsen,[3] which defined technical attribution "as determining the identity or location of an attacker or an attacker's intermediary," is adopted.[4]

4. Cyberspace and the Attribution Problem

Clark and Landau referred to the instant issue as the attribution problem.[5] Simply stated, the attribution problem refers to the inability of a state that has been the victim of a cyber-attack to technically attribute the attack due to the inabilities of technical attribution techniques, thus creating an inability to attribute the attacks due to technical and legal

---

3 David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* 1, Institute for Defense Analysis, IDA Paper P-3792 (October 2003). *See also*, Jeffrey Hunker, Bob Hutchinson, and Jonathon Marqulies, *Role and Challenges for Sufficient Cyber-Attack Attribution* 5, Institute for Infrastructure Information Protect (I3P) (January 2008).

4 *Id. See also*, Alan Cook, *et al*., *Attribution of Cyber Attacks on Industrial Control Systems* 2, ICST Transactions (Preprint) (2017). ("Attribution of cyber[-]attacks lacks a universally accepted definition. Proposed definitions have often been limited in their approach, confining each to subsets of attribution...")

5 David D. Clark and Susan Landau, *Untangling Attribution*, 25 Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010). *See also*, Robert K. Knake, *Untangling Attribution: Moving to Accountability in Cyberspace*, Subcommittee on Technology and Innovation, Committee on Science and Technology, United States House of Representatives 2nd Session, 111th Congress (July 15, 2010); Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council Issue Brief (2011). *Cf.* Michael C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 422 (2011). (Terming the issue as the "attribution challenge.") *See also*, Nicholas Tsagourias, 17 J. Conflict & Security L. 230 (2012) (Describing technical attribution as an attempt "to trace back the cyber-attack to its source and ascribe it to an author against whom action can be taken.") Jeffrey Carr, *Responsible Attribution: A Prerequisite for Accountability* 1, Tallinn Paper No. 6 (2014). ("Attribution in cyberspace remains an ongoing challenge due to a series of complicating factors such as the ability of an unknown aggressor to mimic the tools, techniques, and procedures of a better-known aggressor…") *Cf., James Scott, It's the Russians…Or Is It? Cold War Rhetoric in the Digital Age*, ICIT (Dec. 13, 2016), http://icitech.org/its-the-russians-or-is-it-cold-war-rhetoric-in-the-digital-age/. ("Western systems lack the security and resiliency to withstand foreign compromise. Moreover, Incident Response techniques and processes are not comprehensive or holistic enough to definitively attribute an incident to a specific threat actor….")

reasons.[6] Attribution of cyber-attacks is both a technical and a legal question which does not necessarily work well together. The ability of an injured state to technically attribute a cyber-attack is both technically challenging and time intensive and will most often result in failure[7] without the accused state's assistance in tracking the attacks.[8] If the state from which the attack is suspected of originating does not cooperate, then the ability to attribute a malicious cyber-attack adequately is low to nil. Even if a state is able to technically attribute an attack to a state, this alone is not enough to establish state responsibility as discussed in Chapter Three *supra*.

The ability to attribute malicious cyber-attacks both legally and technically is beset with issues that this study will briefly address. This study operates under the premise that the international legal community must work in conjunction with the computer science community to better solve this ongoing issue of malicious cyber-attacks, or absent a solution, mitigate the attacks to the best extent possible. This study looks at both technical and legal attribution in an attempt to meld a working theory of attribution that will serve as a means of attributing malicious cyber-attacks while balancing the inherent rights of the individual users of cyberspace to the right of anonymity and freedom of speech without undue state interference,[9] while allowing a victim state to respond to malicious cyber-attacks within the existing paradigm of international law.

---

6 *See*, Dimitar Kostadinov, *The Attribution Problem in Cyber Attacks*, INFOSEC Institute (1 Feb 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/. ("[A]ttribution of activities carried out through the internet is extremely difficult and, in many cases, impossible to achieve.") *Cf*., William C. Banks, *Developing Norms for Cyber Conflict *3*, in, Research Handbook on Remote Warfare (Forthcoming), (J. Ohlin ed, 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736456. ("Prompt attribution of an attack and even threat identification can be very difficult.")

7 Jeffrey Hunker, Bob Hutchinson, and Jonathon Marqulies, *Role and Challenges for Sufficient Cyber-Attack Attribution* 5, Institute for Infrastructure Information Protect (I3P) (January 2008).

8 *Cf*. Matthew J. Sklerov, *Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 20 Mil. L. Rev. 1, 8 (2009). ("The current legal paradigm, which requires attribution to a state or its agents, perpetuates the response crisis because it is virtually impossible to attribute a cyberattack during an attack. Although states can trace the cyberattack back to a computer server in another state, conclusively ascertaining the identity of the attacker requires an intensive, time-consuming investigation with assistance from the state of origin.")

9 For the purposes herein, it is accepted that the right to freedom of speech and information provided by access to the Internet is a protected human right. *Cf.* Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/20/L.13 (June 29, 2012); U.N.G.A., *Information and Communication Technologies for Development*, G.A. Res. 66/184,

This study argues that the current CIL for attributing conduct in cyberspace to a state for the purposes of ascertaining state responsibility is unworkable for the purpose of attributing malicious cyber-attacks to the responsible state. While the core tenants of state responsibility, as put forth in the ARS[10] apply, the evidence needed to attribute the attack to the state or non-state actor is virtually impossible to meet given the limitations of technical attribution. In addition, this study believes that effective control test[11] as put forth by the ICJ in *Nicaragua* and as adopted by the *Tallinn Manual*[12] and the ARS is unworkable in the cyber context and must be rejected. As will be discussed *infra*, the needed linkage between the perpetrators of a malicious cyber-attack and the state is virtually impossible to make given the current abilities of computer science, without the express help of the state from which the cyber-attacks originate. As such, under the current paradigm for state responsibility, a state rarely, if ever, will be held responsible for malicious cyber-attacks under existing CIL. This study believes that this inability to legally attribute cyber-attacks will increase the likelihood of future malicious attacks and must be addressed as a means to prevent malicious cyber-attacks from escalating into kinetic conflict or to prevent cyber-attacks from creating kinetic damage.

U.N. GAOR, 66th Sess. U.N. Doc. A/RES/66/184 (6 Feb. 2012). ("[R]ecognizing that freedom of expression and the free flow of information, ideas and knowledge are essential for the information society and are beneficial to development…"]

10 G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

11 Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.) (Merits), [1986] I.C.J. Rep. 14, ¶¶ 105 -110.

12 *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Michael N. Schmitt ed. 2013). (It must be noted ab initio that while the information contained within the *Tallinn Manual* may be persuasive as the group of experts involved with its writing should be considered the "most highly qualified publicists, the manual itself is not CIL.")

4.1. Basic Internet Operations

Prior to discussing technical attribution, it is necessary to examine the basic structure and operation of the Internet. The core concept and design of the Internet are responsible for the numerous issues relating to technical attribution of Internet-based cyber-attacks. To understand these challenges, it is necessary to understand the core ideas behind the original founding of the Internet and the core technical concepts behind how the Internet operates. To understand the issues presented in technical attribution, it is necessary to understand the basic operations of cyberspace/the Internet.

The Internet is an "open" system,[13] that is, "the specifications are publicly available."[14] Meaning that the specifications on how the Internet operates and the programming languages needed to operate within the Internet are readily available,[15] thus enabling disparate networks to operate together to allow the Internet to function. However, the Internet's "openness" also allows any individual or state the ability to use the Internet for nefarious purposes. The Internet's greatest strength is arguably its openness and interoperability. These same attributes are also its greatest weakness as these attributes do not allow for identification of end user nor the end user's locations.

The Internet, as originally designed, was never intended to be the global information exchange that it has become.[16] To support this idea, one need only look to the exponential growth of the Internet over its first 25 years of existence, where it went from tens of users to billions of users, while utilizing the same basic infrastructure and programming.[17] This is supported by the fact that the IP address system (Internet Protocol Version 4 [IPV4]) ran

13 Douglas E. Comer, *Internetworking with TCP/IP, Principles, Protocols and Architecture* 2, (5th ed. 2006).

14 *Id.*

15 *Id.*

16 *See generally,* Mark Bowden, *Worm: The First Digital World War* (Kindle ed. 2011). (Discussing the history of the Internet and its lack of security features.)

17 Douglas E. Comer, *Internetworking with TCP/IP, Principles, Protocols and Architecture* 9, fig.1.1 (5th ed. 2006).

out of IP addresses needed to accommodate the exponential growth of Internet-enabled devices.[18] The fact is, the Internet is operating on security features first put in place in its first iteration which cannot be changed without a reshaping of the Internet as a whole.

The Internet as it currently exists[19] is the result of a corroborative effort between computer scientists and the United States Defense Advanced Research Projects Agency (DARPA) in the 1960s, which resulted in the creation of an early Internet called ARPANET (Advanced Research Project Agency Network).[20] The purpose of ARPANET was to allow disparate computer systems to communicate and to allow researchers a means to quickly share information for disparate geographical locations. The ethos of the early Internet was premised upon the free exchange of ideas and information between researchers and institutions.[21] While initially limited in scope, the ARPANET quickly grew beyond the original purpose and became a social tool.[22] ARPANET started to transition to what is now the Internet in 1974 when computer scientists promulgated the idea of data packets and the Transmission Control Protocol (TCP).[23] The TCP has evolved into what is now known as

---

18 For comparison, numerous sources state that the IPV6 theoretically can handle 3.4×10^{38} distinct IP addresses.

19 As used herein, the Internet refers to the current IPV4/IPV6 format. As of this writing, the Internet was in transition from the IPV4 to IPV6. The transition mainly has to do with how IP numbers are assigned, as the Internet under IPV4 had run out of IP addresses and transitioned to a format (IPV6), which enabled virtually unlimited IP addresses to handle the exponential growth of the Internet. While IPV6 has more robust security features most have not been incorporated upon rollout, and the IPV6 format is still based upon technology that was standardized in 1996. *See*, W. Earl Broebert, *A Survey of Challenges in Attribution*, 41-49 Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010). *See also*, ICANN, *A Beginners Guide to Internet Protocol Addresses* (n.d.).

20 Barry M. Leiner, et. al., *Brief History of the Internet*, Internet Society (n.d.), http://www.internetsociety.org/ internet/what-internet/history-internet/brief-history-internet. *See also*, Mark Bowden, *Worm: The First Digital World War* 9-14 (Kindle ed. 2011). Note, DARPA and ARPANET are used interchangeably as they are the same agency, therefore some texts refer to ARPANET as DARPA, *see*, Douglas E. Comer, *Internetworking with TCP/IP, Principles, Protocols and Architecture* 6, (5th ed. 2006).

21 Mark Bowden, *Worm: The First Digital World War* 13 (Kindle ed. 2011).

22 *Id.*

23 *Id.* at 14.

the Transmission Control Protocol/Internet Protocol (TCP/IP) and is the basis for most Internet communications.[24]

Just as the original TCP/IP is in use to drive the Internet today, the security features utilized by the original ARPANET are still in place; that is, virtually no security features. The founders of the Internet focused on the free exchange of information and interconnectivity, but not security. The original security concept was to lock the computer terminals in a room with limited access.[25] When first imagined, the available computers that could operate on the Internet were less than 100, all with trusted and known users. As a result, there was no mechanism built into the Internet that enabled user identity verification. While limited security features have been added, the emphasis is still upon the anonymity of the end user. Anonymity is the keystone of the Internet. Free information exchange depends upon this anonymity. As a result of this anonymity, the Internet has no true means of connecting technical attribution to human attribution.[26] That is, there are no means of linking cyberspace directly to the person who committed the act. At best, technical attribution may demonstrate the IP address from where the act was initiated. This in itself is not dispositive, as multiple systems may at any given time be linked to a single IP address. This inability to attribute to the human level is again linked to the method that information is sent via the Internet (TCP/IP).

TCP/IP is used to create a packet-switched network.[27] Packet-switched networks utilize data packets[28] to drive the information exchange between networks and users. When data is sent via the Internet, it is broken down into smaller data packets to facilitate the ease of

---

24 *Cf.* W. Earl Boebert, *A Survey of Challenges in Attribution*, 41 Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy (2010).

25 *See generally*, Mark Bowden, *Worm: The First Digital World War* (Kindle ed. 2011). (Discussing the history of the Internet and its lack of security features.)

26 *Id*. at n. 24. (Human attribution refers to the ability to link acts on the Internet to the actual human responsible for those acts.)

27 *Id*. at n. 24. (Packet-switching refers to the TCP/IP which allows information to be sent via small packets of information.)

28 Each packet is between 1,000-1,500 bytes of data (a byte is 8 bits of data, each bit of data in binary code a 0 or a 1). Jonathan Strickland, *How Does the Internet Work*, howstuffworks.com (2014), http://computer.howstuffworks. com/internet/basics/internet2.htm; "Byte" and "Bit", Webopedia (2014), http://www.webopedia.com/TERM/B/.

travel within any given network. Simply stated, data packets are small pieces of information that consist of a header, a payload (computer code), and a footer.[29] Data packets take a large piece of data and break it into smaller data packets to enable quicker transmission through various routers.

The Internet works on the path of least resistance theory.[30] Multiple packets from the same data source may take different routes to the destination depending upon network load, router load, etc. This enables the Internet to share the data transmission load over multiple simultaneous networks enabling greater data transmission speeds. This is enabled by the fact that the header of each packet contains the source IP address and the destination IP address. As the data packet goes from network router to network router, each individual router looks at its internal routing tables for a specific IP range and may select the router with the least data load. When the data packets arrive at the destination computer, the information contained in the footer enables the destination computer to put the information back together in the correct format. This path of least resistance model, however, can create further attribution and sovereignty issues as theoretically a single attack could utilize routers in several countries. This issue will be discussed *infra*.

Many technical attribution problems are due to how data packets are identified via an IP address. While each data packet contains the source IP address, the IP address is not always verified, nor is the IP address always assigned to a specific individual with identifiable information. Instead, the IP address utilized by the end user is assigned by the Internet Service Provider (ISP) to a specific device on its network, and this IP address may change each time the device logs onto a network, depending upon what type of scheme the ISP utilizes to assign IP addresses.[31] While IP addresses are normally assigned to a specific geographical location, at present, any identification beyond a broad general area is

---

29 *What is a Packet?*, Howstuffworks.com (01 Dec. 2000), http://computer.howstuffworks.com/question5251.htm

30 Jonathan Strickland, *How Does the Internet Work*, howstuffworks.com (2014), http://computer.howstuffworks. com/internet/basics/internet2.htm.

31 An ISP may utilize a static IP address where all devices that utilize its network are assigned a "permanent" IP address, or an ISP may use a dynamic IP address where an IP address is temporarily assigned to a device when it logs onto a network, thus enabling a network to provide service to a larger range of devices in a given range of IP addresses, as not all the devices are on the network at a given time. *See, Id*. at n. 24.

impossible without further information. This information is only available via the ISP service provider and falls under the control of the host state and its internal domestic laws. This is further complicated by the issue of mobile computing. Wi-Fi hotspots now allow computer devices to access the Internet at locations that offer free access to the Internet without gaining any identifiable user information and reusing IP addresses so as to complicate locating a single device launching an attack.

Combining these factors, the openness of the Internet; the lack of security features; the need for anonymity; and the lack of true data packet tracking, demonstrates why cyber-attacks have become a cause of concern. The totality of the Internet operates to deny positive technical attribution to the individual creating multiple barriers for positive technical attribution by computer scientists. As such, computer scientists continue to work on positive means of technical attribution but continue to struggle to overcome the multiple barriers that hinder positive attribution.[32]

4.2. Sovereignty and the Internet

One of the many things implicated by the Internet is state sovereignty. The Internet is a "stateless" domain for most purposes.[33] There are no recognizable boundaries within cyberspace; a state's physical locality and its Internet infrastructure are static, but its cyberspace footprint on the Internet may involve multiple other states. This is based on the

32 *See*, Piotr Kijewski, *et al*. *The Never-ending Game of Cyberattack Attribution* 175-177, *in*, Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities (Babak Akhgar and Ben Brewster eds., 2016). *Cf.*, Neil C. Rowe, *The Attribution of Cyber Warfare* 58-68, *in*, Cyber Warfare: A Multidisciplinary Analysis (James A. Green, ed., Kindle ed., 2016). (Discussing technical attribution techniques and the difficulty involved with attributing cyber warfare attacks to a state, as most of the evidence will be circumstantial and not meet the evidentiary burden necessary for legal attribution.) Mary Ellen O'Connell, *Cyber Security Without Cyber War*, 17 J. Conflict Sec. L. 1987 (2012). Quoting David E. Graham and Eric Jensen. ("Given the anonymity of the technology involved, attribution of a cyber attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber attack to a specific server in another state, this can be an exceptionally time consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack.")

33 Zhiqianq Gao and Nirwan Ansari, *Tracing Cyber Attacks from The Practical Perspective* 123, IEEE Comm. Mag. (May 2005). *Cf.*, Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostopoulos, *Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare*, 24 Info. & Comp. Sec. 38, 45 (2016).

fact that a state may have its websites, commercial transactions, government agencies, email servers, etc., located on servers located in a third state. So for example, an attempt to hack a government website may automatically implicate the sovereignty of a third state.

In addition, due to the path of least resistance routing of Internet traffic, a cyber-attack launched by state A against state Z may implicate the sovereignty of states B-Y without the knowledge or acquiescence of those states.

The issue of sovereignty is implicated in that "[i]t is easier to use the cyber infrastructure of a third state than the host/harbor states."[34] This may happen either intentionally, as the attacker may attempt to shift the blame for an attack on a third state by intentionally routing an attack through it, or it may be completely a product of the network-switching utilized by the routers handling the Internet traffic for a given region. If the third state willingly participates, then it "is complicit in the attack."[35] However, as the monitoring of such Internet traffic is difficult, third state complicity is not a factor unless the third state may be shown as a knowing accomplice.[36] This issue is addressed by the *Tallinn Manual* Rule 8 in which a group of experts held that the routing of a cyber-attack through a state's cyberinfrastructure was not enough to attribute the attack to that state.[37] However, this study argues that if the state that the attack is being routed through has knowledge that an attack (a DDoS attack, for example) is utilizing its infrastructure, then the third state has a duty to do everything within its technical capabilities to stop the attack.[38] If the third state lacks the

34 Ashley Deeks, *The Geography of Cyber Conflict: Through A Glass Darkly,* 89 Int'l L. Studies 1, 5 (2013).

35 *Id.* at 6.

36 *Id.*

37 *Tallinn Manual on the International Law Applicable to Cyber Warfare* 36 (Michael N. Schmitt ed. 2013), Rule 8. ("The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State.") *See also*, cmt. 2, *id*., ("[P]ursuant to Rule 5 a State must not knowingly allow its cyber infrastructure to be used for acts adverse to the rights of other States. However, the International Group of Experts was unable to achieve consensus as to whether that Rule applies to States through which cyber operations are routed. To the extent that it does, the State of transit will bear responsibility for failing to take reasonable measures to prevent the transit.")

38 Ashley Deeks, *The Geography of Cyber Conflict: Through A Glass Darkly, 89 Int'l L. Studies* 1, 7 (2013).

technical knowledge needed to monitor its networks or needs other technical assistance, it is free to invite another state to assist.[39]

As a general rule regarding sovereignty, the Internet is "governed by the principle of territorial sovereignty and that neither general international law nor the law of neutrality has become obsolete merely because cyberspace may be considered a fifth dimension or part of the global commons."[40] While delineating the exact boundaries of a state's sovereign territory within the context of the Internet is difficult, it is not impossible. A state exercises jurisdiction and control over the physical infrastructure of the Internet contained within its territory. This may trigger a state's duty to monitor the Internet within its cyber-territory better, so as to monitor for signs of attacks on a third state. As it is a matter of CIL that a state has a duty not to knowingly allow its territory to be used to the detriment of a third state,[41] [42]

4.3. General Issues Regarding Attribution

There are several issues that need to be clarified concerning the topic of attribution. As discussed *supra*, attribution may mean many things to different individuals; "[a]ttribution generally means assigning a cause to an action, this meaning refers to identifying the agent responsible for the action…[and technical attribution means] determining the identity or location of an attacker or an attacker's intermediary".[43] Bishop, Gates, and Hunker defined technical attribution in regards to cyber-attacks as "the ability to determine the origination of an attack."[44] As used herein by this study, legal attribution refers to the assignment of

---

39 Louis Arimatsu, *The Law of State Responsibility in Relation to Border Crossings: An Ignored Legal Paradigm*, 89 Int'l L. Studies 21, 36 (2013).

40 Wolff Heintshel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 Int'l L. Studies 123, 124 (2013).

41 *Corfu Channel*, *supra*. *Trail Smelter* Case (U.S. v. Can.), 3 Rep. Int'l Arb. Awards 1905, 1964 (11 Mar. 1941).

43 David D. Clark and Susan Landau, *Untangling Attribution*, 25 Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010).

44 Matt Bishop, Carrie Gates, and Jeffrey Hunker, *The Sisterhood of the Traveling Packets*, 59 Proceedings of the Workshop on New Security Paradigms (Sept. 2009).

responsibility for an "internationally wrongful act to a state."[45] Attribution may be for an act or an omission of a duty that a state owes to another state.[46] As discussed *supra*, this study utilizes the terms technical attribution as utilized by computer science and legal attribution (or attribution) as used in international law, to create a mechanism for positive attribution of cyber-attacks against states.

Technical attribution is important in that without positive technical attribution, an individual, group, or state may not be held accountable for acts contrary to the rights of another in international law.[47] A means for positive technical attribution has been desired for cyber-attacks by those computer scientists dealing with the problem, but as of this writing this desire for a means of positive technical attribution has not blossomed, nor is it likely to be given the structure of the current Internet. As Tsagourias stated:

> [t]hree particular characteristics of cyberspace make [technical] attribution extremely difficult. The first is 'anonymity' in that cyber attackers can hide their identity; the second is the possibility of launching multi-stage cyber-attacks, in that a number of computers operated by different people and placed in different jurisdictions are infiltrated before an attack is launched; and the third is the speed with which a cyber-attack can materialize.[48]

With these issues in mind, this study now turns to a discussion concerning technical attribution techniques with a focus on recursive traceback techniques. It must be noted that the information presented herein is but a small slice of existing and theoretical attribution techniques and will be discussed in general terms. The information presented by this study in regards to technical attribution is intended to guide the reader through the process so as to better understand the linkage of technical attribution to legal attribution and the difficulties and failures involved with technical attribution in regards to linkage to the author and state.

---

45 *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001), Art.1. *See also*, *id.* art 2, cmt. 12.

46 *Id.* at Art. 2.

47 Matt Bishop, Carrie Gates, and Jeffrey Hunker, *The Sisterhood of the Traveling Packets*, 59 Proceedings of the Workshop on New Security Paradigms (Sept. 2009).

48 Nicholas Tsagourias, *Cyber-attacks, Self-Defence and the Problem of Attribution*, 17 J. Conflict & Security L. 234 (2012).

4.3.1. Technical Attribution: General

Gao and Ansari discussed that "due to the Stateless nature of the Internet and the prevalence of attack tools, it is very easy to mount cyber-attacks."[49] This study fully supports such a belief and will operate under that general premise. This ease of mounting cyber-attacks, as discussed by Gao and Ansari, is enhanced by the difficulty of holding those committing the cyber-attack responsible.[50] The risk/reward dichotomy is strongly within the rewarding realm as the risks associated with conducting cyber-attacks are arguably minimal. This risk-reward dichotomy works for both state and non-state actors.

Computer science utilizes a mixture of attribution techniques and theories to attempt to trace the malicious code utilized in the attack on the author or originating IP address. Multiple techniques and theories abound concerning the attribution of cyber-attacks. This study will briefly discuss common techniques with a focus on recursive traceback techniques to demonstrate what current computer science may and may not accomplish through technical attribution. Finding those responsible for a cyber-attack is one goal of computer science in relation to cyber-attacks which generally utilizes the term "IP traceback"[51] or "stepping-stone detection"[52] (hereafter collectively "traceback") to designate efforts to attribute cyber-attacks.

---

49 Zhiqianq Gao and Nirwan Ansari, *Tracing Cyber Attacks from The Practical Perspective* 123, IEEE Comm. Mag. (May 2005).

50 Florian P. Buchholz and Clay Shields, *Providing Process Origin Information to Aid in Network Traceback*, 1 CERIAS Tech Report 2002-22, Center for Education and Research in Information Assurance and Security (2002).

51 Traceback may be defined simply as "as identifying the actual source of any packet sent across the Internet." Krishan Kumar, A.L. Sangal, and Abhinav Bhandari, *Traceback Techniques Against DDOS Attacks: A Comprehensive Review*, 491 Proceedings 2nd IEEE Int'l Conf. on Computer and Comm. Tech. (2011). *But cf.*, Jeffrey Hunker, Bob Hutchison, and Jonathon Marquilies, *Role and Challenge of Sufficient Cyber-Attack Attribution*, 5 Institute for Information Infrastructure Protection (Jan. 2008). (Holding that traceback techniques should be considered a subsidiary of attribution.) *See also*, Matt Bishop, Carrie Gates, and Jeffrey Hunker, *The Sisterhood of the Traveling Packets*, 59 Proceedings of the Workshop on New Security Paradigms (Sept. 2009). (Discussing attribution via IP traceback schemes.)

52 Matt Bishop, Carrie Gates, and Jeffrey Hunker, *The Sisterhood of the Traveling Packets*, 59 Proceedings of the Workshop on New Security Paradigms (Sept. 2009). (Discussing the use of the term "stepping-stone detection.")

Computer science utilizes various techniques and theories to conduct traceback operations, but they are limited due to the design of the Internet and the lack of inherent security and identification protocols within the Internet.[53] "Given the complexity of the current Internet, it is difficult for the victim of a cyber-attack to ascertain the source of a cyber-attack."[54] As Hunker, Hutchison, and Margulies discussed, cyber-attack attribution suffers from unique challenges in that:

> [a]ttribution cannot…be accomplished strictly through the use of technology [alone]…[t]here are situations that make attribution highly desirable and situations in which attribution would destroy the Internet as a means of communication…[and] [c]yber attacks often cross jurisdictional boundaries; hence attribution techniques require cooperation between jurisdictions, some of whom may not be able to trust one another.[55]

The issue of technical attribution and the use of traceback techniques are complicated by the issue that different cyber-attack methods implicate different traceback and forensic techniques in an attempt to identify the malware utilized in the cyber-attack. This is complicated further by the vector of attack and computer systems implicated, i.e., a DDoS attack will be analyzed using more traditional IP traceback, and the worm that infected the computers that created the zombie-bots[56] will be analyzed utilizing traditional computer forensics in an attempt to discern its creators. A computer virus such as Stuxnet that did not utilize the Internet as a vector of attack would only be analyzed by traditional computer science forensic techniques.

---

53 *Id.* at 4.

54 Zhiqianq Gao and Nirwan Ansari, *Tracing Cyber Attacks From The Practical Perspective* 123, IEEE Comm. Mag. (May 2005). *Cf*., Krishan Kumar, A.L. Sangal, and Abhinav Bhandari, *Traceback Techniques Against DDOS Attacks: A Comprehensive Review*, 491 Proceedings 2nd IEEE Int'l Conf. on Computer and Comm. Tech. (2011). (A review of traceback techniques did not find a single technique that was able to traceback any DDoS attack to its origination.) *See also*, Jeffrey Hunker, Bob Hutchison, and Jonathon Marquilies, *Role and Challenge of Sufficient Cyber-Attack Attribution*, 5 Institute for Information Infrastructure Protection (I3P) (Jan. 2008).

55 Jeffrey Hunker, Bob Hutchison, and Jonathon Marquilies, *Role and Challenge of Sufficient Cyber-Attack Attribution*, 4 Institute for Information Infrastructure Protection (Jan. 2008).

56 A zombie bot is a computer system (typically a Windows-based PC) that has been infected by a worm (a self-replicating computer program that gives access of a PC to another without the owner/user's knowledge) and is then utilized by a botmaster (the individual or organization that has knowledge of the infected zombie bots and then utilizes them for a DDoS attack or to send spam).

The goal of IP traceback techniques is to ascertain the actual location and source of the attacks.[57] For those cyber-attacks that do not utilize the Internet as a vector of attack, e.g., Stuxnet or Ouroboros virus, attribution is even more difficult as it then becomes a matter of computer forensics where the computer code that makes a cyber weapon is taken apart line by line, where the investigator looks for clues within the programming of the code in an attempt to ascertain who wrote the code. Such cyber weapons will be discussed *infra*.

Technical attribution alone though is not sufficient in most incidents to bind a state to a specific cyber-attack for the purposes of state responsibility.[58] An ideal technical attribution scheme would enable an investigator to pinpoint a specific computer/user that could then be held responsible. This, unless it was launched from a state-owned computer or a state-controlled network, is not enough to bind the state to the cyber-attack unless it may be shown that the state had effective control over the individual/group responsible for the attack.

In addition to the inability of technical attribution to necessarily link an attack to a state, one must consider the veracity and level of certainty[59] of the attribution needed for proof. The ICJ has held that the greater the accusation against a state, the greater the burden of proof.[60] This impacts technical attribution in that without a "smoking gun," as it were, a state will deny its involvement and lay the blame at others. These multiple factors complicate the issue of technical attribution.

Technical attribution, it must be noted, is not always a desirable trait within the Internet. So-called non-attribution is an important aspect of the Internet in that those individuals who desire to practice their inherent right to the freedom of speech (or the practice of any other human right facilitated by the Internet that may be subject to state scrutiny and prohibition) may not wish for their identities to be known, hence the ability of non-attribution or

---

57 Zhiqianq Gao and Nirwan Ansari, *Tracing Cyber Attacks From The Practical Perspective* 123, IEEE Comm. Mag. (May 2005).

58 *Cf. Tallinn Manual*, R.6, cmt.6.

59 Matt Bishop, Carrie Gates, and Jeffrey Hunker, *The Sisterhood of the Traveling Packets*, 60 Proceedings of the Workshop on New Security Paradigms (Sept. 2009)

60 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶210.

anonymity is an important factor that must be balanced against the right of a state to find those responsible for cyber-attacks. Any scheme for technical attribution may be utilized for attribution of both good and bad conduct on the Internet as determined by the state. As such, any scheme for attribution must be carefully balanced to ensure that individual rights are respected.[61]

4.3.2. Barriers to Attribution

The ability to properly attribute cyber-attacks is further complicated by technical barriers that individuals may utilize to hinder or prevent technical attribution. These mechanisms that prevent technical attribution may serve a necessary cause to ensure the anonymity of at-risk users who wish to avail themselves of their individual right of free speech while protecting themselves from unwanted government intrusion. However, the same protective technology that may be used to protect individual anonymity may also be used to hide nefarious users. Thus the duality of the problem is how to protect the lawful rights of an individual while ensuring that those nefarious individuals are not able to avail themselves of that protection.

Theoretically, there are as many means of creating barriers to technical attribution as there are means to attempt to attribute technically. The openness of the Internet means that every technical article published on how to attribute an attack technically gives the attacker information on how to overcome that form of technical attribution.[62] This creates an ongoing battle between the attackers and the defenders to vie for supremacy. Just as discussed *supra*, the malware responsible for cyber-attacks are evolving continuously, so

---

61 Jeffrey Hunker, Bob Hutchison, and Jonathon Marquilies, *Role and Challenge of Sufficient Cyber-Attack Attribution*, 4 Institute for Information Infrastructure Protection (Jan. 2008). Matt Bishop, Carrie Gates, and Jeffrey Hunker, *The Sisterhood of the Traveling Packets*, 60 Proceedings of the Workshop on New Security Paradigms (Sept. 2009). Gary D. Brown, *What International Humanitarian Law Gets Wrong About Cyber Warfare*, Seminar Presentation, University of Glasgow (10 June 2014).

62 For an interesting example of how fast cyber-attack authors adapt and utilize new science and techniques *see*, Mark Bowden, *Worm: The First Digital War* 124-125 (2010). (Discussing the second generation of the Conficker worm and its utilizing 4,096 bit-key for its secure hash algorithm encryption, prior to the use of this 4,096 bit-key, the standard used by the U.S. government's Federal Information Processing Standard [as per Bowden, the highest publicly available encryption at the time] was a 1,024 bit-key and the use of a 4,096 bit-key had been theoretical and only discussed as a proposed model for future use.).

to are the means of avoiding technical attribution. A few of the more common and readily available barriers to technical attribution will be discussed to demonstrate the difficulty in overcoming even those barriers that computer science knows about.

Many tools that impede or prevent technical attribution are readily available to end users and take numerous forms. Included in these tools are IP anonymizers, which are either software or Internet-based services that allow a user to establish a connection to a proxy server. Connecting via a proxy server allows the end user to be assigned an IP address which replaces the actual IP address of the end user, which the end user may select by country or location or at random by the software/web service. This allows the end user to avail themselves to the Internet with a greatly reduced risk of technical attribution.

Other software allows the end user to spoof or forge IP addresses;[63] this enables the user to create packet headers with altered IP addresses that may be gibberish or reflect a valid IP address of an innocent individual. IP spoofing is normally utilized to mask the source of DDoS attacks where the attacker need not worry about the packet return,[64] as a DDoS attack focuses on bombarding a server with worthless requests in order to prevent authentic requests from being serviced.

Additionally, "[t]he stateless nature of IP routing, where routers normally know only the next hop for forwarding a packet instead of knowing complete the end-to-end path taken by each packet,"[65] creates an intrinsic barrier to attribution by making attribution more difficult, as each "hop" of a packet must be traced back to the next "hop" and so on. However, this is complicated as routers only keep temporary logs of the packets that pass through them and these logs may be wiped by savvy attackers to mask their attacks, or these logs will be wiped either automatically by the server software or at intervals by the administrator as they take up space on the server; hence the more traffic a router has, the faster it will recycle its logs.

---

63 Krishan Kumar, A.L. Sangal, and Abhinav Bhandari, *Traceback Techniques Against DDOS Attacks: A Comprehensive Review*, 491-492 Proceedings 2nd IEEE Int'l Conf. on Computer and Comm. Tech. (2011).

64 *Id.*

65 *Id.*

The United States has contributed to this issue by creating the Tor browser system which utilizes an "onion routing" system allowing users to share their Internet access from differing locations through "a circuit of encrypted networks."[66] Tor operates a "distributed anonymous network"[67] which enables users' activity to be distributed throughout a series of secure servers before reaching its end point via the secure network. As Tor states:

> [t]o create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.[68]

Thus, Tor is an ideal way to evade IP traceback and mask a cyber-attack, e.g., in the third quarter of 2013, the Security Engineering Research Team (SERT) Quarterly Threat Intelligence Report, found a 350% increase in Tor traffic which SERT linked to the increased use of Tor "to shield botnet traffic and possible attempts to defend against NSA (the United States National Security Agency) surveillance."[69]

Tor was established by the United States Naval Research laboratory as a means of protecting communications with the intention to shield dissident groups, journalists, and law enforcement investigations through secure communication.[70] The irony is that now Tor is used to protect malicious cyber-attacks and its authors, facilitate cybercrime, and provide access to the dark web. This again demonstrates the hazards incorporated through the dual use of Internet services.

---

66 Tor Project, *Tor: Overview* (n.d.), https://www.torproject.org/about/overview.html.en. This issue has potentially gotten worse as computer scientists have developed a HORNET system, a High speed Onion Routing NETwork, which has a much higher bandwidth and more robust anonymity features.

67 *Id.*

68 Id.

69 Digital Forensic Investigator (DFI) News, *Increase in Strange Traffic, Cyber Attacks Utilizing Tor* (Oct. 31, 2013), http://www.dfinews.com/news/2013/10/increase-strange-traffic-cyber-attacks-utilizing-tor.

70 Id. at n.66.

Lastly, as Kostadinov [71] discussed, a savvy attacker will route an attack through as many servers and states as possible to mask the trail of the attack. This creates technical difficulties as discussed above. It also creates international legal issues in that the state that was victim to the malicious cyber-attack must now deal with each individual state's legal system that the malicious cyber-attack utilized, in an attempt to gather information before the evidence that would allow the victim state to piece together the trail of the attack is deleted.

The barriers to technical attribution discussed herein are a mere sampling of the issues that face those attempting to technically attribute any cyber-attack. It is important to bear these issues in mind as this study now turns to traceback techniques. It is important to remember that for each technique or theory discussed herein, there are individuals or states of equal or better education devising mechanisms to thwart the traceback techniques as such a constant cat-and-mouse battle is waged between the white hats and the black hats.[72]

4.4. Attribution Techniques

There are no set categories for attribution techniques. Nicholson et al.[73] in their review of the taxonomy of attribution techniques, identified six classes of attribution techniques.[74] This taxonomy includes manual attribution,[75] traceback techniques,[76] stepping stone

71 Dimitar Kostadinov, *The Attribution Problem in Cyber Attacks*, INFOSEC Institute (1 Feb 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/.

72 *See*, Olivia Solon, *Hacking Group Auctions 'Cyber Weapons' Stolen from NSA*, The Guardian (16 Aug. 2016), https://www.theguardian.com/technology /2016 /aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group. (Discussing a reported theft by hackers of NSA hacking tools.)

73 Andrew Nicholson, et al., *A Taxonomy of Technical Attribution Techniques for Cyber Attacks* 188-198, in, Proceedings of the 11th European Conference on Information Warfare and Security (Eric Filiol & Robert Erra, eds. 2012)

74 *Id*. at 195.

75 *Id*. at 191.

76 *Id.* at 192.

attribution,[77] payload attribution,[78] honeypots,[79] Internet redesign,[80] and what Nicholson et al. referred to as "attribution frameworks" where multiple techniques are used to attribute the attacks.[81]

Rowe [82] placed attribution into three broad categories, attribution of files (forensic examination of malware payload),[83] attribution of network traffic (including "backward [recursive] tracing of files…[and] alternatives to backward tracing")[84] and "attribution to the state."[85] Shamsi, Zeadally, Sheikh, and Flowers[86] broke attribution down to three categories: digital forensics, malware-based analysis, and indirect attribution.[87]

All three of the above-referenced articles discuss similar techniques. This study will combine them into the following three categories (Fig. 1):

77 *Id*. at 193.

78 *Id*. at 194.

79 Nicholson, *Id.*

80 *Id*., at 195.

81 *Id*.

82 Neil C. Rowe, *The Attribution of Cyber Warfare* 58-68, *in*, Cyber Warfare: A Multidisciplinary Analysis (James A. Green, ed., Kindle ed., 2016).

83 *Id*. at 62.

84 *Id*. at 63.

85 *Id*. at 66.

86 Jawwad A. Shamsi, Sherali Zeadally, Fareha Sheikh, & Angelyn Flowers, *Attribution in Cyberspace: Techniques and Legal Implications*, Sec. Comm. Networks (2016), http://onlinelibrary.wiley.com/wol1/doi/10.1002/ sec. 1485/full

87 *Id.* at *4-9.

Technical Attribution	Forensic Attribution	Indirect Attribution
Recursive Traceback	Malware Analysis	Circumstantial Attribution
Stepping Stone	Digital Forensics	Attribution to the state
Honey Pots	Payload Attribution	Multiple attribution frameworks
	Authorship Attribution	
	Attribution of Files	
	Manual Attribution	

Fig. 1.

This study does not include the redesign of the Internet as a means of attribution. The redesign of the Internet lies firmly within the realm of computer science and is a purely theoretical construct which, in the opinion of this study, is cost prohibitive for states, corporations, and individuals at present. In addition, as discussed *supra*, the ability to positively identify an individual on the Internet is not necessarily a positive idea. As such, creating a new Internet, one which has a means to identify the end user positively, militates against the original premise of the Internet: an open and free exchange of information.

No single technical attribution technique or scheme is able to adequately attribute a cyber-attack standing alone. Each attribution technique has its own strength and weaknesses,[88] and the success of the attribution technique is dependent, in part, on the technical skill of the attack author. It has been posited that multiple attribution schemes working in conjunction are the best method of finding the responsible computer for a cyber-attack.[89] Attribution techniques are also dependent upon the besieged computer systems' or networks' ability to identify that the system is under attack and for the ability to identify the type of attack that the system has suffered, as many stealth attacks may lay undiscovered for long periods of time.[90] Even before attempting to attribute the attack, the injured party must identify the tool or method utilized to attack them. This identification, which Rowe called the "attribution of files,"[91] encompasses identifying that a system has or is being

88 David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* 3, Institute for Defense Analysis, IDA Paper P-3792 (Oct. 2003).

89 *Id.*

90 *See e.g.*, Criminal Complaint, *United States v. Su Bin*, Case No. 14-1318M (C. D. Cal. June 27, 2014). (Alleging an ongoing computer infiltration of Boeing aircraft company computers by Su Bin and two alleged co-conspirators from 2009 to 2014. During that time, Boeing allegedly did not know their computer systems were compromised.)

attacked and then identifying the tools being utilized to conduct the attack. This is a matter of computer forensics, where the attack vector or tools are deconstructed in an attempt to identify the authors.

The information gathered from the attribution of files may give clues as to who the potential author may be, or metadata from the code may give clues as to what language the authors utilized, the time zone where the authors lived, and other minor details that may be utilized in tracing the attack tool. This, however, is not always accurate as code and snippets of code are routinely bought and sold or pirated and reused by multiple authors of attack tools. In addition, old attack tools may be re-tooled for new purposes, thus creating confusion as to the identity of the original author. The knowledge gained from such attribution in all likelihood will not demonstrate conclusively who the author is but may be utilized to attribute the attack to a state circumstantially. However, such attribution is of arguable legal worth.[92] And as many attack authors, much like IED engineers, have specific methods of construction, good intelligence may be garnered through the forensic deconstruction of attack tools.

This study will address the three categories of attribution put forward *supra*; this study does so as to demonstrate the known current abilities of computer science and computer science's inability to fully attribute a cyber-attack.

4.4.1. Traceback Techniques for Attribution

The primary method[93] currently utilized for technical attribution of cyber-attacks is the tracing of Internet traffic associated with a cyber-attack from the site of the attack

---

91 Neil C. Rowe, *The Attribution of Cyber Warfare* 62, *in*, Cyberwarfare: A Multidisciplinary Analysis (James A. Green, ed. Kindle ed. 2016).

92 O'Connell, *supra.*

93 Vahid Aghaei-Foroushani and A. Nur Zincit-Heywood, *Deterministic Flow Marking for IPV6 Traceback* *1, Network and Service Management (CNSM), 11th Int'l Conf. on IEEE (2015), https://www.semanticscholar.org/paper/Deterministic-flow-marking-for-IPv6-traceback-DFM6-Foroushani-Zincir-Heywood/ 49c12809fb3776bda0260aef561d3f8924463 517/pdf. ("IP traceback is a mechanism which aims to identify the true source of an IP datagram. However, as many current IP traceback schemes are proposed concerning IPv4 network, they

recursively to the original IP address responsible for the attack.[94] (There are a number of other techniques that may be utilized such as SMTP [Simple Mail Transfer Protocol], Ethernet protocols, and Dynamic Host Configuration Protocol [DHCP][95] traceback techniques) but as the majority of attacks are IP-based, this study will focus on general IP protocol traceback. It must be noted that none of the other mentioned traceback schemes are able to truly technically attribute an attack standing alone, as they suffer from the same or similar limitations of IP traceback. All traceback schemes rely on the attribution of network traffic.

The majority of IP traceback mechanisms are designed to function against DoS/DDoS attacks,[96] such as those suffered by Georgia and Estonia. DoS/DDoS attacks are "flood" attacks, where the operations of a server or information system are severely impacted by a flood of data requests made on the service by spoofed packets.[97] By flooding these systems with spoofed packets, the system cannot reply to legitimate requests, and the systems cease to function as designed. Most famous of these types of attacks are the attacks on Estonia (2007) and Georgia (2008), where large segments of both countries' cyberinfrastructure were impacted by large-scale DDoS attacks over a period of days.

DoS/DDoS attacks are normally one-way attacks, that is, the packets that are requesting bogus services from a system are spoofed with false IP packet headers, so there is no packet data sent back to the author of the attack. In most instances, the author of the attack is far removed from the DoS/DDoS attacks, as the author will normally have set up a botnet which is a collection of zombie computers that have been infected by a worm that allows

---

cannot be directly used in IPv6 network. Implementing those techniques for IPv6 networks require modifications because of the technological differences…)

94 Xinyuan Wang and Douglas Reeves, *Traceback and Anonymity* 5-11 (2015). (Discussing the traceback model.) *See also*, Karanpreet Singh, Paramuir Singh, and Krishan Kumar, *A Systematic Review of IP Traceback Schemes for Denial of Service Attacks*, 56 Comp. & Sec. 111-139 (2016). Neil C. Rowe, *The Attribution of Cyber Warfare* 63, *in*, Cyberwarfare: A Multidisciplinary Analysis (James A. Green, ed. Kindle ed. 2016). (Discussing attack attribution.)

95 David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* 3, Institute for Defense Analysis, IDA Paper P-3792 (Oct. 2003).

96 Naga Mani Tenali and Bala Savitha Jyosyula, *IP Traceback Scenarios*, 19 Global J. Comp. Science Tech.13(E) (2013).

97 *Id.*

the botmaster to use those machines to launch the DoS/DDoS attacks, while limiting the traceback options and exposure to the author of the attack.

Traceback techniques may fall into one of two broad categories: either preventive traceback or reactive traceback.[98] Preventive traceback focuses on preventing spoofed IP addresses or illegitimate IP addresses from accessing specific systems. Preventive traceback, per se, is not a traceback technique as it does not provide the recursive step-back (stepping stone) needed to identify the source of the attacks and as such, fail to provide a basis for identification of the attacker.[99]

Reactive traceback techniques provide the best hope for actually tracing an attack to the source IP address. Reactive traceback techniques such as link testing,[100] work backward from the attacked system, querying each router along the line looking for the router that forwarded the spoofed packets. This is repeated until the source IP of the originating system is located.[101] Other traceback variations rely on algorithms to calculate the path of a packet in which a marker has been inserted into, and others utilize a probabilistic packet marking algorithm.[102]

For non-DoS/DDoS attacks, traceback techniques will attempt to reclusively step-back the attacks throughout the data packet's route to the attacked system in an attempt to identify

98 Naga Mani Tenali and Bala Savitha Jyosyula, *IP Traceback Scenarios*, 20 Global J. Comp. Science Tech.13(E) (2013); Krishan Kumar, A.L. Sangal, and Abhinav Bhandari, *Traceback Techniques Against DDOS Attacks: A Comprehensive Review*, 491 Proceedings 2nd IEEE Int'l Conf. on Computer and Comm. Tech. (2011). (Describing the two different categories of traceback schemes as pro-active and reactive), *but cf.*, David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* 9-11, Institute for Defense Analysis, IDA Paper P-3792 (Oct. 2003). (Discussing both preventive and reactive traceback techniques as a single category of techniques).

99 Tenali, *id.*

100 *Id. See also*, David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* 9, Institute for Defense Analysis, IDA Paper P-3792 (Oct. 2003). (Discussing "[s]tore logs & traceback queries...which is a similar technique to that posited by Tenali and Jyosyula); Ghao Gong, Trinh Le, T. Korkmaz, and K. Sarac, *Single Packet IP Traceback in AS-Level Partial Deployment Scenario* 1817, in Proceedings of the IEEE Globocom (2005).

101 Tenali, *id.* at n.98.

102 *Id.*

the source IP responsible for the attacks. Simply put, computer science will follow the breadcrumbs of the attack from one IP address to the next until they get to the original IP address responsible for the attack. However, this is not sufficient for technical or legal attribution as the malware responsible for installing the payload onto the infected system most likely will have originated from another source. The malware will have to then be analyzed through computer forensic analysis in an attempt to identify the author of the software/payload which may yield clues as to the origin.

Traceback techniques currently in operation appear to be able to trace a cyber-attack, either a DoS/DDoS or direct attack, to the originating IP address, however, this process is time-consuming, and its success has to do with the abilities of the attack author and sheer luck. The IP address that the traceback technique resolves to will be linked to a specific geographic range. The IP address will not normally demonstrate the end user for that address. Thus, additional techniques will be needed to corroborate the findings of traceback techniques and develop a theory of who may be the authors of an attack.

Honeypots are related to traceback techniques but are different in that a honeypot may exist for multiple reasons including identifying an attack event,[103] identifying attack vectors, searching for new types of attacks, and tracking attacks by regions. Honeypots themselves are not necessarily an attribution tool but serve as a mechanism to assist in attribution. A honeypot is "[a] server that is configured to detect an intruder by mirroring a real production system."[104] That is, a honeypot is a device running on the Internet that appears to be a real series of IP addresses that are set up to trap incoming attacks for various purposes.[105] There are two types of honeypots, "[p]roduction honeypots [which] capture only limited information, and are used primarily by companies or corporations; and research honeypots [which] are complex to deploy and maintain, capture extensive information, and are used primarily by researchers, military, or government organizations…"[106] Honeypots' benefits

103 Van-Hau Pharm, *Honeypot Traces Forensics by Means of Attack Event Identification* 1-2, PhD Thesis, Telecom Paris Tech (2009).

104 Shantanu Shukla & Sonal Sinha, *Use of Honeypot and IP Tracing Mechanism for Prevention of DDOS Attack*, 3 Int'l J. Sci. Engineering & Res. 94, 95 (2015).

105 For a visual representation of what honeypot activity is, *see*, map.norsecorp.com.

106 *Id.* at n. 104.

lie in that they only collect malicious attacks and are not prone to false-positives.[107] Honeypots may be used to collect attacks that may then be traced back to the originating IP address,[108] giving researchers a source IP address which may be blacklisted or monitored. Honeypots may also be utilized as a defense against DDoS attacks by identifying zombie IP addresses associated with a DDoS attack and blocking said IP addresses from gaining access to the attack's intended target.

4.4.2. Forensic Attribution

The second category of attack attribution is that of forensic attribution utilizing digital (computer) forensic science. In the instant matter, forensic attribution relates to the analysis of the computer code creating the malware, which was utilized to conduct a cyber-attack, to ascertain evidence of authorship. The evidence obtained may assist an injured state in finding the responsible actor, however, "attributing malicious code is always questionable…"[109] While it is doubtful, in the opinion of this study, that evidence obtained during forensic attribution is enough to attribute an attack to a state standing alone, evidence obtained from an attack may be combined with other elements to attribute an attack. The legal standing of such attribution (circumstantial) for the purposes of state responsibility is in doubt, however, and will be discussed further *infra*.

Forensic attribution for the purposes of this study is mainly utilized for those attacks that use malware or malicious code as a means to inflict damage, harm, or used for other malicious purposes as opposed to DDoS attacks which do not leave malware on the victim system. The Stuxnet variant attacks are arguably the most famous of these attacks to date (it must be noted that the Sauron/REMSEC malware espionage tool may be more advanced and dangerous than Stuxnet and is almost definitely state-sponsored due to the complexity

107 Id. at n. 104.

108 Id. at 86.

109 Nicholas Weaver, *What Sauron Tells Us About What NSA's Up To, and What It Should Do Next*, Lawfare (Aug. 15, 2016), https://www.lawfareblog.com/what-sauron-tells-us-about-what-nsas-and-what-it-should-do-next.

of its design.[110] As of this writing, however, this is an ongoing issue without many facts and as such, will not be discussed in depth). Stuxnet was used to attack the Iranian Natanz nuclear fuel enrichment center in 2012, becoming the first cyber weapon to cause physical harm.[111] Cyber weapons such as Stuxnet differ from previously discussed malicious cyber-attacks in that the vector of attack does not necessarily rely on the Internet. A cyber weapon may be delivered via the Internet, but it may also be delivered via a physical device such as a USB memory stick or other solid-state media. Many forms of cyber weapons are self-replicating, meaning that once they are on a system, they will attempt to infect other devices through various means of propagation, which may include the use of solid state media, the Internet or a local intranet. The computer code utilized in cyber weapons and the techniques to forensically analyze it does not differ from the forensics utilized in other types of malware.

Cyber weapons may be directed weapons in that they may be designed to attack a specific computer system or network, or they may be generalized weapons that attack a range of systems operating a specific operating system. Kaspersky Labs posited three broad categories of cyber weapons[112] "destroyers…espionage programs…, [and] cyber sabotage

110 Dan Goodin, *Researchers Crack Open Unusually Advanced Malware That Hid for 5 Years*, ArsTechnica (08 Aug., 2016), http://arstechnica.com/security/2016/08/researchers-crack-open-unusually-advanced-malware-that-hid-for-5-years/. Nicholas Weaver, *What Sauron Tells Us About What NSA's Up To, and What It Should Do Next*, Lawfare (Aug. 15 2016), https://www.lawfareblog.com/what-sauron-tells-us-about-what-nsas-and-what-it-should-do-next. (Discussing the probability that the United States NSA is responsible for the Sauron

111 Ralph Langner, *Cracking Stuxnet: A 21st-Century Cyber Weapon* (Transcript), TED.com (March 2011), https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon/transcript. (Describing the Stuxnet virus as a target cyber weapon of mass destruction.) Thomas C. Reed, *At The Abyss: An Insider's History of the Cold War* *4721-*4738 (Kindle ed., 2007). (Discussing the "Farewell countermeasure campaign" against the Soviet Union in the early 1980s and alleging that the United States Central Intelligence Agency, with the assistance of Canadian manufacturers, inserted a Trojan into a SCADA controller responsible for controlling pumps on oil pipelines that was eventually smuggled into the Soviet Union despite an ongoing trade embargo. The Trojan allegedly triggered a large explosion in the pipeline in 1982. These allegations have been denied by the Soviet Union/Russia and the account cannot be independently verified.).

112 Kaspersky Labs, *Kaspersky Security Bulletin 2012: Cyber Weapons* (18 Dec. 2012), https://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons. ("Destroyers'. These are programs designed to destroy databases and information as a whole. They can be implemented as 'logic bombs' that are introduced into victim systems either in advance and then triggered at a certain time, or during a targeted attack with immediate execution. The most notable example of such malware is Wiper. Espionage programs. This group includes Flame, Gauss, Duqu and miniFlame. The primary purpose of such malware is to collect as much information as possible, particularly very highly specialized data (e.g. from Autocad projects, SCADA systems etc.), which can then be used to create other types of threats.

tools."[113] With cyber-espionage tools posting the greatest danger as they may potentially create physical damage,[114] but all types will damage the infected systems if some preset criteria are met. Destroyers, as the name implies, attack a system and destroy data contained within; a destroyer attack may be executed immediately or have delayed execution at a preset time or when a specific condition is met.[115] Espionage programs are tools that gather and transmit data; the more specialized the data, the better these programs work.[116] While espionage, per se, is not illegal in international law, these programs may work as a reconnaissance program in that the data they gain may be used to create further exploitation to a service or harm the owner of the system. Cyber sabotage tools are cyber weapons that impact a specific system or component or a specific range of data. Sabotage programs blur the line between espionage and use of force, and as such, should be analyzed for the impact they have when activated.

Cyber weapons leave a payload of malicious computer code on each system it infects, allowing for forensic examination of the payload upon discovery. Once discovered, the payload may be forensically examined to provide evidence as to its creators, origins, and purpose. The forensic evidence derived from the examination of the cyber payload may be utilized to assist in the attribution of the cyber-attack to the state(s) responsible for their creation and utilization. However, the forensic evidence alone, without further evidence of state involvement, is not enough to attribute the attack to a state.

The examination of a cyber weapon payload may be accomplished through digital forensics and reverse engineering. Depending on the skill and technical knowledge of the creator of the cyber weapon, this may be relatively straightforward or extremely complex. The evidence gathered is generally circumstantial and consists of such information as the type

> Cyber sabotage tools. These are the ultimate form of cyber weaponry – threats resulting in physical damage to targets. Naturally, this category includes the Stuxnet worm. Threats of this kind are unique and we believe they are always going to be a rare phenomenon. However, some countries are devoting more and more effort to developing this type of threat, as well as defending themselves against it.")

113 *Id.*

114 *Id.*

115 *Id.*

116 *Id.*

of keyboard used, the language used, e.g., Lua, Python, C/C+, Assembly, etc., the time zone of the computer(s) that created the malware and so on. Truly knowledgeable and experienced programmers will leave scant details of who created such weapons unless, as has been posited regarding the Stuxnet attacks, the attackers want the systems attacked to know who attacked them.[117]

The biggest issue with technical attribution is that it does not conclusively say X or Y is the author (unless the author actually leaves their name on the code). Forensic attribution may only tell the injured state or researcher limited amounts of information which the state or researcher then draws an inference from. For example, the Sauron malware package which was discovered in August 2016 has been tentatively linked to the United States due to not only its complexity but its use of the Lua programming language (an obscure programming language seen in the Flame variant malware), and the age of the malware, reportedly built upon malware existing prior to 2001.[118] Such inference, however, does not establish attribution to the United States as any number of other states or non-state actors may be capable of creating such malware. Without greater evidence linking the Sauron malware to the United States or acknowledgment or adoption by the United States, the malware will forever be a question mark as to authorship and responsibility, thus allowing the United States or whoever is responsible for the creation and use of the malware to escape responsibility for its use.

Forensic attribution, like technical attribution, can only establish a limited number of facts for consideration regarding attribution for the purposes of state responsibility. Technical attribution may be able to link an attack to a specific geographical area or IP address, but not connect that information to a state or non-state actor. Forensic attribution may tell us

117 Ralph Langner, *To Kill a Centrifuge* (Nov. 2013), http://www.langner.com/en/wp-content/uploads/2013/11 /To-kill-a-centrifuge.pdf.

118 Nicholas Weaver, *What Sauron Tells Us About What NSA's Up to, and What It Should it Do Next*, Lawfare (Aug. 15, 2016), https://www.lawfareblog.com/what-sauron-tells-us-about-what-nsas-and-what-it-should-do-next.

what, how, and where, but not who,[119]thus forcing a state to infer who may or may not be responsible for the attack. These drawing of inference questions will be addressed next.

4.5. Indirect Attribution

Indirect or circumstantial attribution is likely the most used form of attribution by states. Indirect attribution utilizes traditional intelligence gathering, law enforcement techniques, and technical and forensic attribution to attribute an attack.[120] There are no set criteria for such attribution, and circumstantial attribution suffers from evidentiary issues concerning the quality of the evidence adduced.[121] This study will discuss Healey's model as an example of circumstantial attribution elements and then discuss the evidentiary burden that circumstantial evidence faces.

Jason Healey put forth 14 elements which he argued are central to circumstantial attribution of attacks.[122] This study will briefly discuss Healey's elements to illustrate how circumstantial attribution may operate. These elements are presented as Healey articulated them without comment, but it should be understood that the importance of each element fluctuates depending upon the evidentiary strength or weakness of the other elements, therefore while some elements may seem more important, that may not always be the fact.

Healey's elements as adopted by this study are:[123]

---

119 *See*, Jason Healey, *Concluding Assessment* 266, in, A Fierce Domain: Conflict in Cyberspace, 1986-2012 (Jason Healey, ed.,2013). ("[T]echnical tools and methodologies are unable to determine where an attack lies on the spectrum [of how States may be responsible.").

120 Jason Healey, *Concluding Assessment* 266, in, A Fierce Domain: Conflict in Cyberspace, 1986-2012 (Jason Healey, ed., 2013). (These elements have been modified for readability and contextual understanding).

121 Jack Goldsmith, *The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance* (Dec. 9, 2014). https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance. (Discussing the evidence proffered by the FBI and arguing that evidence the FBI relied upon was "conclusory in nature" and discussing that attribution such as this suffers from lack of hard evidence. Finally, Goldsmith argued that attribution deriving from traditional intelligence sources is not useful as the evidence adduced will not be presented, as states will not want to disclose the means and methods used to gather the intelligence.)

122 Healey, *id*. at n.120 at 266-274.

123 Healey, *id*. at n.120 at 275.

1. Was the attack traced back to a specific state IP address?
2. Was the attack traced back to a specific state element or organization?
3. Were the attack tools written in a national language of a state?
4. Were the attacks traced back to a state which has sole control over its cyberinfrastructure and Internet?
5. How technically sophisticated was the attack in comparison with standard attacks?
6. How sophisticated was the targeting of the attack, e.g., far-reaching or pinpoint.
7. What was the mood of the accused state and its citizens?
8. Was commercial benefit derived from the attack?
9. Does the accused state directly support hackers?
10. Is there a correlation between the attacks based upon public statements?
11. Did the accused state cooperate with the investigation into the attack?
12. Who benefits most from the attack (*cui bono*)?
13. Is there a correlation with a state's national policy regarding cyber-attacks/espionage/war?
14. Was the attack an adjunct to or associated with kinetic attacks?

Healey argued that when these elements, taken in totality, point affirmatively to a state, then the attack may be attributed to that state. While Healey may be correct that such findings may make it appear that the state is responsible, this study would argue that such circumstantial attribution fails for the purposes of attribution for state responsibility. The first problem is that each element must be demonstrated to a clear and convincing evidentiary burden.[124] These elements fail if the attacks were conducted by non-state actors, as these elements do not demonstrate the needed control by a state over a non-state actor for responsibility to lie under *Nicaragua*. This theory may be effective under alternative theories of state responsibility and will be discussed *infra*.

Only a few of these elements (1-5) discussed by Healey rely upon technical or forensic attribution. The rest rely on other forms of evidence-gathering, e.g., intelligence or traditional law enforcement techniques. In addition, the remaining elements (6-14) allow

124. Mary Ellen O'Connell, Cyber Security Without Cyber War, 17 J. Conflict & Sec. L. 187, 202 (2012). ("State practice indicates the case for attribution would have to be made with clear and convincing evidence.").

for subjective interpretation which may skew the attribution toward a perceived adversary, but not necessarily the correct adversary. All the elements suffer from the fact that none are dispositive. Each technical element is subject to spoofing, and the non-technical elements may suffer from false flag and similar traditional counter-intelligence techniques.

In addition, even if all the elements presented point affirmatively to a state, this is not, arguably, enough to attribute the attack to the state under the CIL/ARS model for attribution. While the ARS itself is silent as to the evidentiary burden needed, this study has demonstrated that the evidence to attribute the conduct to a state must be clear and convincing. The evidence presented by any form of attribution must demonstrate that the state was directly linked to the accused conduct by clear and convincing evidence. This linkage to the state or its agents is most likely not present in circumstantial attribution. As ICJ case law has demonstrated in *Nicaragua*, the evidence linking a state to a wrongful act must be such as no doubt may remain as to the state's involvement. In addition, this study would argue that at best, the circumstantial evidence adduced by the elements discussed will be a more likely than not standard as each element discussed cannot be demonstrated conclusively as each element may be spoofed or misdirected. This is not to say that circumstantial attribution cannot work; this study merely argues that the likelihood of circumstantial evidence meeting the necessary evidentiary burden is very low given the medium involved.

4.6. Technical Attribution Conclusion

A review of the current literature has demonstrated that attribution of a cyber-attack to the author of the attack is difficult, if not impossible. When technical attribution is theoretically possible, it is time-consuming and dependent upon a state having the available expertise and resources to do so. The theoretical models of attribution, however, only resolve the issue of where the cyber-attack was initiated from. There are no known means[125] to date of positively identifying an author of a cyber-attack without having physical control over the

[125] This study acknowledges the theoretical possibility that state agencies such as the United States' NSA or the United Kingdom's Government Communications Headquarters (GCHQ) may have the ability to attribute cyber-attacks other than is publicly acknowledged. However, this study may only address the known methods and leave conjecture of such things to others.

computer system in which the code for the payload was written and then only if computer forensics can recover the data.

The current iteration of the Internet was not designed to be a secure form of communication, nor does it have a mechanism for IP address verification or require users to be positively identified. As long as the Internet is an open-source means of communication which embraces the ideals of personal freedoms and anonymity, the Internet will be used for nefarious and malicious purposes. This study would theorize that even if identity controls were established, nefarious actors would find a means to circumvent positive attribution of conduct on the Internet, effectively returning the status quo to where technical attribution stands today. As of the present, no known means of technical attribution are effective or timely enough for common usage of states for the purpose of legally attributing conduct.

Technical attribution of cyber-attacks, whether through traceback techniques or forensic examination of the cyber weapons that were utilized for an attack, are not adequate, at present, to effectively link an individual or state to a malicious cyber-attack. Circumstantial attribution may demonstrate that a state's cyber territory is involved, but cannot link the state's cyber-territory to acts of the state itself.

As such, the evidence available from technical attribution, geolocation based upon IP addresses and evidence obtained from forensic examination of the cyber weapons utilized and other information from indirect sources, is utilized at present to attribute malicious cyber-attacks. This, however, leads to issues of proof, qualifying the weight of evidence, questions of evidentiary bias, and a host of associated problems.

The inability to technically attribute cyber-attacks necessitates that international law looks to other mechanisms for attributing acts to non-state actors or states themselves. Other mechanisms are necessary; to do nothing invites continued malicious acts against states via the Internet and cyberspace, thus increasing the chances that a state may react to a cyber-attack through traditional kinetic use of force against the state it perceives to be responsible for the malicious cyber-attacks.

Part One: Analysis and Conclusion

To attribute malicious cyber-attacks to a state for the purposes of state responsibility, the injured state must demonstrate the following elements:

1. The malicious cyber-attack must rise to the level of an internationally wrongful act or omission on behalf of a state.
2. The malicious cyber-attack must be technically attributed to a specific actor by evidence that demonstrates, with a minimum of clear and convincing evidence, that the actor initiated the malicious cyber-attack.
3. For the purposes of state responsibility, the actor to which the malicious cyber-attack is technically attributed to must be an agent or organ of the state to attribute the actor's actions to a state, or if the actor is not an agent or organ of the state, the injured state must prove that the state acknowledged and adopted the acts as their own after the fact, or; if the actor who initiated the malicious cyber-attack is not an agent or organ of a state, it must be demonstrated through clear and convincing evidence that the actor was operating under the direction and control of a state for state responsibility to lay. This direction and control must be enough to satisfy the effective control test as discussed *supra*, the basis of which is that the state had as much control over the non-state actor as to make it virtually indistinguishable from a state organ or actor of the accused state.

If these elements are not met, then the malicious cyber-attack may not be attributed to a state for the purposes of state responsibility.

Satisfying these elements is difficult for both technical and legal reasons. This study has demonstrated that a malicious cyber-attack may, with some difficulty, be traced to the original machine or IP address from which the attack was initiated using technical attribution techniques discussed *supra*. Acquiring direct evidence linking the machine or IP address responsible for the attack to an agent or actor of a state is virtually impossible if the accused state employs a modicum of digital hygiene. That is, jumping the air gap from machine to the human operating it, and linking the operator to the state, is virtually

impossible. Thus, linking the origins of a malicious cyber-attack by direct evidence to the state is extremely unlikely.

As gaining direct evidence linking the origins of an attack to a state is unlikely, states may engage in circumstantial attribution, utilizing multiple techniques from traditional and cyber intelligence gathering, law enforcement techniques, and other methods as put forth by Healey *supra*, to attribute attacks to a state. Whether this circumstantial attribution is enough to attribute the attacks to a state for the purposes of state responsibility is doubtful. As demonstrated *supra*, the attribution of an internationally wrongful act or omission to a state requires direct evidence of the state's involvement/control for a wrongful act or omission to be attributed to the state. As circumstantial attribution cannot demonstrate a direct connection to a state for attribution and state responsibility purposes, circumstantial attribution fails as a matter of law.

As it is virtually impossible to attribute a malicious cyber-attack by direct evidence to a state, a state may not be held responsible for the majority of malicious cyber-attacks. Thus, international law is faced with three options, (1) continue to suffer malicious cyber-attacks without a means of holding states responsible, (2) change the rules of attribution for the purposes of attributing malicious cyber-attacks, or (3) look to alternative paradigms existing in international law that may be used to hold states responsible for malicious cyber-attacks. As (1) is not an option and (2) suffers from several drawbacks (e.g., states not willing to disclose the evidence they have or the means and methods of gaining such evidence, plus the inherent subjectivity and ambiguity of such evidence), (2), in the opinion of this study, is unworkable at present. This leave (3) to be, in the opinion of this study, the most workable solution to the problem of malicious cyber-attacks.

As such, Part Two of this study will explore the idea of alternative legal paradigms as a means of holding states responsible for malicious cyber-attacks that can be directly attributed to their cyber-territory.

Part Two: Alternative Theories of State Responsibility

Chapter Five: Alternative Theories For holding States Responsible for Malicious Cyber-Attacks

5. Introduction

This study now turns to a discussion regarding alternative theories for state responsibility. This study will argue that the pre-existing legal theories of the duty to do no harm and the theory of strict liability for ultra-hazardous activities may be utilized to hold a state responsible for malicious cyber-attacks when attribution fails under the rules put forth by the ARS. This study will analyze these theories under the charter law prohibition on unlawful political intervention. This study does so to demonstrate how the duty to do no harm and the theory of strict liability may be utilized under specific theories of international law. This study will apply these theories to the malicious cyber-attacks discussed *supra* Chapter One. This study utilizes these theories to demonstrate applicable theories of state responsibility that may operate in instances where attribution fails. These theories may engage a state through indirect attribution and indirect responsibility. This study utilizes these legal theories, which operates as a matter of CIL and charter law, to demonstrate how malicious cyber-attacks may be dealt with via existing international legal frameworks.

This chapter addresses those malicious cyber-attacks that rise to the level of an internationally wrongful act, yet the wrongful act cannot be attributed to a state as the needed control or linkage to the state, or non-state actor is not present. This chapter will demonstrate that existing CIL and charter law is adaptable enough to cover malicious cyber-attacks either directly or by analogy. This chapter will also discuss how malicious cyber-attacks may be dealt with when attribution on an individual level is not possible, a situation which is prevalent in the majority of malicious cyber-attacks.

This study will begin with a discussion regarding the prohibition on unlawful political intervention. It will then discuss the duty to do no harm and the theory of strict liability for ultra-hazardous activities.

5.1. The Prohibition on Unlawful Political Intervention

This study argues that malicious cyber-attacks may violate the prohibition on unlawful political intervention This obligation prohibits states from engaging in acts that intervene with the sovereign rights of another state without permission or justification A state is prohibited from:

> [i]nterfering…in the internal or foreign affairs of another State. [The State] is only prohibited when it occurs in fields of State affairs which are solely the responsibility of inner [s]tate actors, takes place through forcible or dictatorial means, and aims to impose a certain conduct of consequence on a sovereign State…[1]

The prohibition on unlawful political intervention results in harm that falls under the prohibitions contained within the theories discussed in this chapter. The harm resulting from unlawful political intervention is unique from other harms discussed in this study. The harm inflicted upon a state through unlawful political intervention is a harm which is difficult to quantify, as it is a harm which results from interference with the freedom of a state to act independently. The harm resulting from unlawful political intervention goes to the very heart of a state, as it is directed at the very principles states enjoy as independent entities in international law: political independence and sovereignty.

In addition, the harm resulting from unlawful political intervention goes to the heart of the UN Charter. The UN Charter Art. 2(1) puts forth that the UN is "an [o]rganization [] based on the principle of the sovereign equality of all its Members."[2] Therefore, when a state unlawfully politically interferes with another state, it harms a state's sovereignty, and that harm strikes the very notion of charter law and the principles of the UN. At its core, the harm from unlawful political intervention is qualitatively different from the harm discussed previously. The harm suffered from unlawful political intervention impacts the essence of what makes a state independent in international law. The harm inflicted by unlawful

---

1 Phillip Kunig, *Prohibition of Intervention*, in, Max Planck Encyclopedia of Law (2015), http://opil.ouplaw. com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?rskey=4krYZ6&result=5&prd=EPIL. Citing, *Nicaragua*, ¶ 205.

2 U.N. Charter Art. 2 ¶ 1. ("The Organization is based on the principle of the sovereign equality of all its Members.") *See also*, Phillip Kunig, *Prohibition of Intervention*, in, Max Planck Encyclopedia of Law (2015), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?rskey=4krYZ6&result=5&prd=EPIL. Kunig posited that Art. 2(1) implies the prohibition on unlawful intervention.

political intervention theoretically impacts all the citizens of the harmed state. This wide scale impact upon a state and its citizens is different than other harms discussed in this study. While the various harms discussed herein may impact a large part of a state's citizens, the harm suffered from unlawful political intervention theoretically impacts every citizen in one manner or another. An example of this would be the 2016 Presidential elections in the United States and the alleged intervention by Russia. This alleged intervention, if proven true, would have deprived all the citizens of the United States of a freely elected President. Harming the state in toto as the democratic process was potentially thwarted by either collusion between the State of Russia and a political party and / or the alleged hacking of opposition party computers to publish information to sway voters. Either way, the free exercise of democracy was interfered with through unlawful intervention. It is this difference in harm which makes it worthy of discussion and analysis, as it offers an alternative view of how malicious cyber-attacks may be considered an internationally wrongful act.

The issue becomes how this prohibition on unlawful political intervention operates and how it applies to malicious cyber-attacks. This will be addressed briefly *infra,* followed by a brief discussion on the pragmatic application of the theory and its legality as a matter of CIL. Once this study demonstrates how the prohibition on unlawful political intervention operates, this study will discuss how the duty to do no harm and the theory of strict liability for ultra-hazardous activities may act as adjunct methods in replacing the needed attribution element to hold states responsible absent customary attribution.

5.1.1. Unlawful Intervention of Political Independence and Malicious Cyber-Attacks

The basic principle of the prohibition on unlawful political intervention was addressed by the ICJ in *Nicaragua* in which the court stated:

> the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which

> defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action or in the indirect form of support for subversive or terrorist armed activities within another State…[3]

The theory of unlawful political intervention may trace its roots to the prohibition found in Art. 10 of the Covenant of the League of Nations which states, "[t]he Members of the League undertake to respect and preserve as against external aggression the…political independence of all Members of the League…"[4] The U.N. General Assembly further elucidated this prohibition in the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, *The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter*, stating:

> [n]o State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.
>
> No State may use or encourage the use of economic [,] political [,] or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State.
> …
>
> Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State…[5]

The question, therefore, is how malicious cyber-attacks violate this prohibition. This study argues that states violate this prohibition by utilizing malicious cyber-attacks that are initiated for political purposes where the attacks are less than force, yet are intended to

---

3 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. US), 1986 I.C.J. 4 (June 27).

4 Covenant of the League of Nations Art. 10 (28 June 1919).

5 Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, *The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter*, U.N.G.A. Res 2625, U.N. Doc. A/Res/25/2625 (24 Oct. 1970) (emphasis added).

coerce a state to take action, to interfere with a political process, or to simply interfere with a state's domestic policies for the benefit of the attacking state.

An example of malicious cyber-attacks which are violative of the unlawful political intervention prohibition are the DDoS attacks initiated against Estonia in April of 2007, as discussed *supra* Chapter One. The DDoS attacks against Estonia began after a "spat with Russia over the removal of a war memorial."[6] The DDoS attacks impacted segments of Estonia's commercial cyber infrastructure[7] and were circumstantially attributed to Russia by several sources.[8] The DDoS attacks were apparently launched against Estonia to punish Estonia for a political act (the moving of the Russian statue) and to influence by coercion the domestic-Estonian political discussions regarding the removal of the statue and Estonia's apparent move toward a closer relationship with NATO. The DDoS attacks against Estonia were arguably initiated to coerce, punish, or interfere with Estonia's domestic policies regarding a purely internal political question. Thus, the DDoS attacks could be violative of the prohibition on unlawful political intervention which, this study believes, the Russian state could be responsible for based on the theories discussed *infra*.

Unlawful political intervention is an internationally wrongful act as the unlawful intervention is an act against both charter law and CIL. In this sense, unlawful political intervention results in an additional harm: i.e., the act of intervening in another state's internal affairs (not the result of that intervention). In this respect, the harm is different than that discussed *infra* regarding *Trail Smelter* or *Corfu Channel*; there, the harm was dependent upon the damage resulting from the physical act. Here, the harm is in the act itself. An act is an internationally wrongful harm once a state attempts to coerce, unlawfully, another state utilizing malicious cyber-attacks.

---

6 *The History of Cyber Attacks–A Timeline*, NATO Rev. (n.d.), http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm. (Select April 2007).

7 *See*, Andrzej Kozlowski, *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, 3 Eur. Scientific J. (Feb. 2014) (Discussing the cyber-attacks and engaging in a discussion on who probably carried out the cyber-attacks).

8 *Id. See also*, Jason Healey, *Concluding Assessment* 273-278, *in*, A Fierce Domain: Conflict in Cyberspace 1986 to 2012 (2013 Jason Healey ed.) *Cf.* Scott J. Shackelford and Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo. J. Int'l L. 971, 1007 (2011) ("Russian hackivists were widely reported to have been responsible for the cyber-attacks on Estonia in 2007 and Georgia in 2008.").

Similar DDoS attacks were carried out against Georgia in August 2008, as discussed *supra* Chapter One, as a precursor to, and adjunct to, a kinetic conflict with Russia.[9] The Georgia attacks were similar to, yet more robust than the Estonia DDoS attacks, impacting almost every element of Georgia's cyber infrastructure. The attacks against Georgia were a precursor to a kinetic event, so they may be seen as not only a means to unlawfully intervene with the political independence of a state, but also as a peremptory attack on Georgia's command and control systems and its domestic government's blending malicious cyber-attacks with militarized cyber-attacks. The initial DDoS attacks upon Georgia were directed at both civilian and state-owned computer systems. The attacks seemed to be utilized to influence the decision-making process of both Georgia and its allies. The DDoS attacks prevented Georgia from relaying information to its citizens and its allies. The attacks, which targeted Georgian state cyberinfrastructure, were meant to deny Georgian citizens from engaging with their political leadership by preventing its citizens from utilizing services of the Georgian government. In addition, the Georgian banking system and other financial services were targeted, denying Georgian citizens access to such services as a means to sway the political discourse within Georgia. In other words, it was a coercive act, and arguably violative of the prohibition on non-intervention. [10]

Both the Estonia and Georgia cyber-attacks were blamed on proxies who, in theory, acted outside of government control and also took action in support of a political cause the proxies supported. However, these attacks interfered with and harmed the political independence of the impacted state: the malicious and militarized cyber-attacks were meant as a means to intimidate, interfere, and dissuade a sovereign state from taking an action that was within its right as a sovereign to take. These attacks may either be a direct violation of the unlawful political intervention prohibition or, as will be discussed in Chapter Seven, they may illustrate a failure to prevent an unlawful political intervention by a non-state actor by the state to which the attacks were traced back; in this case, Russia.

---

9 *The History of Cyber Attacks–A Timeline*, NATO Rev. (n.d.), http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm. (Select Georgia 2008).

10 *See e.g.*, David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars Journal (Jan. 6, 2010), http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (Discussing the cyber-attacks against Georgia and the invasion of Georgia by Russia).

The question becomes what is meant by political intervention, and how did the DDoS attacks violate the prohibition? At its basest level, political intervention is any attempt by an outside actor to change the course of domestic policies through unlawful means; unlawful can be in terms of either the domestic internal laws of a state or as a matter of international law. A sovereign state enjoys dominion over its internal decision-making regarding internal and international political decisions or those decisions which impact the normal day-to-day operations. This is the political power with which an outside actor interferes.[11] *Black's Law Dictionary* defines political power as "[t]he power vested in a person or body of persons exercising any function of the State…"[12] relating to what the duty not to intervene defines as the "political, economic and cultural elements" [13] of the state. Therefore, any malicious or militarized cyber-attack that is launched against a sovereign state in order to influence a state's actions that pertain to its rights as a sovereign state would be violative of this prohibition. The DDoS attacks against Estonia and Georgia appear to have been launched to unlawfully intervene in the political, economic, and cultural decisions made by the Estonian and Georgian governments. The DDoS attacks against Estonia and Georgia were intended to influence, coerce, or punish the domestic policies of Estonia and Georgia by subjecting their domestic cyberinfrastructure to DDoS attacks: the perpetrators of the DDoS attacks were targeting specific IP addresses relating to domestic government, information and news, financial services, and emergency services. This, in turn, resulted in a violation of the prohibition on unlawful political intervention, resulting in making the attacking state responsible for an internationally wrongful act. However, such acts were never attributed to Russia or any other state; no state has been held responsible for the DDoS attacks against Estonia and Georgia.

This study argues that any malicious cyber-attack launched against a state to intervene with a state's domestic political agenda would be violative of the prohibition regarding non-

11 *Cf.* Rafael Nieto-Navia, *International Peremptory Norms (Jus Cogens) and International Humanitarian Law*, ICCNow, (n.d.), http://www.iccnow.org/documents/WritingColombiaEng.pdf. ("[T]he concept of 'national sovereignty' has undergone an evolution today, States are regulated by both their own national rules together with the continually developing laws of the international community...").

12 *Political Power*, Black's Law Dictionary 1277 (9th ed. Bryan A. Garner ed. 2011).

13 Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in accordance with the Charter of the United Nations, U.N.G.A. Res 2625, U.N Doc. A/Res/25/2625 (24 Oct. 1970).

intervention if the attack is directed at political, economic, or cultural entities with the intent to coerce a state to act in a particular manner. While it is beyond the scope of this study to delineate each possible type of malicious or militarized cyber-attack and the potential political ramifications from said attacks, it is posited that most cyber-attacks of this nature will be highly public. The attacks on both Estonia and Georgia were quite public, presumably in order to involve the populace and coerce them by putting political pressure on their leadership to act to prevent further malicious cyber-attacks.

This study argues that attribution of such attacks should be relatively straightforward, and is premised upon an action and response methodology. For example, if state A takes an action which is unpopular in state B (the action), then state A is suddenly subject to massive DDoS or other cyber-attacks which are traced to IP addresses within state B's cyberinfrastructure by clear and convincing technical evidence (the response), then state B either needs to demonstrate that it is not behind the attacks or that it did not have the technical ability to prevent the attacks. Additionally, state B has a duty to either prevent the attacks as discussed *infra* Chapter Six, demonstrate that the actions are not originating from within its cyber territory, or that it does not have the ability to prevent the acts. The state to which the attacks are attributed to may then be held responsible under the theory of the duty to do no harm or strict liability theories discussed, *infra*.

This action and response (without attribution or state responsibility) have been seen in recent malicious cyber-attacks against the NATO states which have been linked to Russia.[14] With a straining of relations between NATO and Russia over Russian involvement in the Ukraine conflict and an imposition of sanctions on Russia by NATO member states, malicious cyber-attacks have been conducted against prominent NATO countries including the United States, France, Poland, and other European countries.[15] The attacks have been traced to Russian hacking collectives and groups.[16] These attacks would appear to be violations of the prohibition on unlawful political intervention as they are in response to a

14 Michael Riley and Jordan Robertson, *Cyberspace Becomes Second Front in Russian Clash with NATO*, Bloomberg Business (Oct. 14, 2015), http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato.

15 *Id.*

16 *Id.*

political act on behalf of NATO states, and the malicious cyber-attacks are against government infrastructure, cultural outlets, and the business and financial sectors. Russia could be held responsible under the ARS for these internationally wrongful acts if it can be shown that the Russian state is using proxies to conduct the attacks, and if the effective control test is met. However, this study argues the alternative; that Russia may also be responsible under the theories discussed herein *infra*. Given the difficulties of attributing malicious cyber-attacks to a state and the difficulties of demonstrating the effective control test for non-state actors, the theories discussed herein are necessary as an alternative means of attribution for malicious cyber-attacks.

The theory of unlawful political intervention lends itself well to both theories discussed *infra*. The existing rules do not work in a majority of cases, so the international community needs to recognize and apply different forms of attribution for malicious cyber-attacks. This study demonstrates that the theory of unlawful political intervention combined with the duty to do no harm or the strict liability principle is a means of holding states responsible based upon existing CIL.

The prohibition on unlawful political intervention gives states an alternative theory to apply to malicious cyber-attacks either directly or through analogy. As states continue to utilize malicious cyber-attacks like that discussed *supra* regarding Estonia, Georgia, and the ongoing NATO-Russia cyber conflict to intervene or interfere with the political process of sovereign states, this theory on unlawful political intervention may allow states to hold a state responsible for the intervention under this theory. Colloquially, it is another tool in the toolbox for states to legally address the problem of malicious cyber-attacks.

5.2. Malicious Cyber-Attacks and the Duty to Do No Harm

It is a matter of hornbook law that a state may not allow its territory to be utilized to harm another state. This prohibition has its roots in Roman law[17] and has been an accepted practice throughout history. For the purposes of this study, the starting point for the duty to do no harm will be the prohibition as enunciated in the *Trail Smelter* arbitration,[18] where the arbitral commission held that:

> [n]o State has the right to use or permit the use of its territory in such a manner as to cause injury. . . in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence. [19]

A similar proclamation was made by the ICJ in *Corfu Channel*, where the court stated that it is "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States,"[20] which is accepted as part of the corpus of CIL. While *Corfu Channel* adds an additional element ("knowingly," which will be discussed in Section 5.3.), the basic premise of each decision has become part of the CIL relating to interstate relations. This prohibition, the "duty to do no harm," places two requirements upon the state: (1) the state may not use its territory "contrary to the rights of other States,"[21] and (2) a state has a duty to not "permit the use of its territory in such a manner as to cause injury."[22] This second duty, the duty to prevent, is addressed in Chapter Six *infra*.

---

17 Kai Sheffield, *Of Pulp Mills and Oil Spills: Strict State Liability Under Customary International Law When Energy and Resource Projects Cause Transboundary Environmental Harm*, Ecobulletin 4 (June 2011). *Quoting*, Alan E. Boyle, *State Responsibility and International Liability for Injurious Consequences of Acts Not Prohibited by International Law: A Necessary Distinction?* 39 Int'l Comp. L. Q. 1, 13-14 (1990) (Stating that the good neighbor principle and the duty to do no harm is "one of the oldest concepts available in inter-state disputes").

18 *Trail Smelter* Case (United States v. Canada), 3 Rep. Int'l Arbitral Awards 1905, 1965 (Mar. 11, 1941). *See also*, Draft Declaration on Rights and Duties of States, Art. 7, G.A. Res. 345 (IV) (6 Dec. 1949). ("Every State has the duty to ensure that conditions prevailing in its territory do not menace international peace and order.").

19 *Trail Smelter* Case (United States v. Canada), 3 Rep. Int'l Arbitral Awards 1905, 1965 (11 Mar. 1941).

20 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9).

21 Id.

22 *Id.*

The theory behind both the *Trail Smelter* and the *Corfu Channel Case* is arguably the same: a state may not allow its territory to be utilized in such a manner as to harm another state. This rule may be found in various contexts in international law, particularly in customary international environmental law: there, the prohibition on transboundary harm is put forth in the Rio Declaration Principle 2, which states:

> States have, in accordance with the Charter of the United Nations and the principles of international law . . . the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction.[23]

This idea that a state may not allow activities in its territory to harm another state is applicable beyond international environmental law. The prohibition on harm arguably extends to many different forms of harm, whether the harmful acts result from state acts or the acts of non-state actors. There is support for this proposition regarding the harm resulting from terrorist acts; for instance, the UNGA directed that:

> States . . . must refrain from organizing, instigating, assisting or participating in terrorist acts in territories of other States, or from acquiescing in or encouraging activities within their territories directed toward the commission of such acts[.][24]

Here, the UNGA recognized the duty of states to prevent harm in the form of terrorist acts and reaffirmed the states' duty to ensure that their internal domestic acts do not harm other states.[25] It is argued that the harm from malicious cyber-attacks falls within this prohibition either directly or by analogy.

It is argued from the outset that the ideas and elements posited in this study form an effective mechanism for state responsibility for malicious cyber-attacks, as a state may be responsible for cyber-attacks that emanate from its sovereign territory and harm another state and the attacks need only be attributed to the state's territory or cyberinfrastructure and not directly to the state itself. Thus, a state is responsible for cyber-attacks that originate

---

23 Rio Declaration on Environment and Development, Principle 2, Rio, 3-14 June 1992, http://www.unep.org/Documents.Multilingual/Default.asp?documentid=78&articleid=1163. *See also*, Report of the United Nations Conference on the Human Environment, Principle 21, Stockholm, 5-16 June 1972. http://www.unep.org/Documents.Multilingual /Default.asp?documentid=97&articleid =1503.

24 G.A. Res. A/49/60, Declaration on Measures to Eliminate International Terrorism (09 Dec. 1994)

25 *See also*, G.A. Res. A/51/210 (17 Dec. 1996).

from its sovereign territory under the duty to do no harm. However, as will be discussed *infra*, this is not an absolute duty: it depends in great part upon the state's ability to prevent such occurrences.

5.2.1. Cyber-Attacks and the Duty to Do No Harm: Discussion

This study will discuss the duty to do no harm through analysis of three interrelated CIL theories: (1) the *Trail Smelter* prohibition on transboundary harm; (2) the *Corfu Channel* case and the ICJ's holding concerning "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States,"[26] and (3) the theory of strict liability for ultra-hazardous activities. This discussion is intended to demonstrate through analogy and application how existing CIL may be utilized to address holding states responsible for malicious cyber-attacks.

It is important to reiterate that the duty to do no harm creates two separate duties upon the state. The duty to do no harm first binds the state regarding the state's own conduct; that is, the state itself may not engage in conduct that could harm another state. In addition, which will be discussed in Chapter Six, the duty to do no harm creates a second duty in that the state must, to the best of its abilities, prevent other actors from utilizing its territory to harm another state.

5.3. Trail Smelter and the Prohibition on Transboundary Harm

The *Trail Smelter* arbitration[27] was brought about under special agreement by the United States and Canada to determine the extent of damage that had been caused by the operation of the Trail smelter in British Columbia, Canada to the state of Washington in the United States, which was located across the international border and downwind from the smelter.[28]

---

26 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9).

27 *Trail Smelter* Case (United States v. Canada), 3 Rep. Int'l Arbitral Awards 1905 (Mar. 11, 1941).

28 *Id.* at 1908, 1911, 1913-1917.

The damage suffered by the state of Washington was due to the emission of sulfur dioxide (SO_2) from the Trail smelter; the parties to the arbitration agreed it was to the point of pollution.[29] The damage resulted from the "fumes" (airborne particulates of SO_2) which had damaged agriculture and property in the state of Washington.[30] The damage was generally economical: loss of yield from crops, loss of production in other industries, and loss of timber for logging.[31]

The *Trail Smelter* arbitration tribunal discussed harm as related to damage done by SO_2, but it had "difficulty of determining what constitutes an injurious act."[32] Accordingly, the *Trail Smelter* arbitration discusses the overall prohibition in terms of a general concept of harm, not just the harm caused by the Trail smelter. The *Trail Smelter* idea of harm looks to what the state itself would protect its citizens from and what conduct a state would punish based upon its own jurisprudence and laws.[33] To determine what constitutes a harm under *Trail Smelter*, one need only look to see what the harmed state would protect its citizens against or what actions the injured state criminalizes. This study would expand this concept of harm to include those acts which militate against international peace and security. Thus, any harm committed against a state via cyberspace and which the injured state would protect its citizens against, or which has domestic legislation prohibiting the act, or which militates against international peace and security, would be a harm under the instant theory. It must be noted that harm is not the same as an internationally wrongful act. Depending upon the harm committed, a single incident may equate to an internationally wrongful act (if the harm is such as to engage the state in itself), or it may be multitudes of smaller harms

29 *Id.* at 1913-1917.

30 *Id.* at 1920. The arbitration addressed "(a) Damages in respect of cleared land and improvements thereon; (b) Damages in respect of uncleared <sic> land and improvements thereon; (c) Damages in respect of livestock; (d) Damages in respect of property in the town of Northport [Washington]; (g) Damages in respect of business enterprises[.]"

31 *Id.* at 1913-1934.

32 Alexandre Kiss and Dinah Shelton, *Strict Liability in International Environmental Law* 1131, *in* Law of the Sea, Environmental Law and Settlement of Disputes: Liber Amicorum Judge Thomas H. Mensah (Tafsir Malick Ndiaye and Rüdiger Wolfrum, eds. 2007), http://ssrn.com/abstract=1010478.

33 *Id.*

taken in the aggregate which reaches the level of an internationally wrongful act. This idea is discussed *infra*.

It should be understood that while damage and harm are often synonymous, they can be seen as distinct ideas. Damage relates to "[p]hysical harm that impairs the value, usefulness, or normal function of something."[34] Harm relates to "[p]hysical injury, especially that which is deliberately inflicted."[35] It should be understood that harm and damage may be used interchangeably for the purposes of the *Trail Smelter* arbitration and the discussion herein. However, harm may also be understood in a broader context as it encompasses ideas of not only economic and kinetic damage, but may also refer to the long-term effects of *de minimis* issues that, over time, aggregate into something greater which causes significant harm. This idea is seen in *Trail Smelter*: a single incident of SO_2 release by the smelting facility in Canada would not have necessarily caused damage, yet the prolonged release of SO_2 created an injurious nuisance to the environment. There was no single malicious act by the Trail smelter, but a series of long-term legal acts eventually caused harm. The harm aggregated over time until it became a harm of sufficient magnitude to trigger the need for compensation to those harmed in the state of Washington. The harm, therefore, must be significant.[36] Significance may be measured by either monetary loss or actual kinetic damage, or a hybrid of both.

This idea of harm as seen in *Trail Smelter* may be extrapolated out to encompass the prohibition on malicious cyber activity that emanates from one state but harms another state. While the harm in *Trail Smelter* was physical, it was also monetary in the loss of production or value. While traditional definitions of harm involve physical properties, the domestic law of many states recognizes categories of harm or damage that go beyond physical. Harm may be psychological, as seen in the tort of intentional infliction of

34 Oxford Dictionary, *Damage* (2015), http://www.oxforddictionaries.com/definition/english/damage.

35 Oxford Dictionary, *Harm* (2015), http://www.oxforddictionaries.com/definition/english/harm. *See also, Harm*, Black's Law Dictionary 784 (9th ed. 2009). (Defining harm as "injury, loss, damage; material or tangible detriment." It is interesting to note that Black's recognizes social harm also.).

36 Christina Voigt, *Principles of IEL* 23 (n.d.), http://www.uio.no/studier/emner/jus/jus/JUS5520/h12/undervisningsmateriale/3.-principles-in-iel.pdf.

emotional distress;[37] harm may be monetary, as seen in countless breach of contract cases worldwide; or it may be seen as something between tort and contract as in a delictual breach of the duty of care. At its simplest, harm is any form of damage.[38] Harm should be divorced from the causative agent and based on the end result of the activity in question. The harm caused by SO_2 is no different than the harm caused by falling space debris or harm caused by malicious cyber-attacks; the end result is that the damage was done and is still damaging, irrespective of the source.

Harm may result from malicious cyber-attacks in numerous ways. The most obvious harm is the monetary damage done to businesses worldwide due to cybercrime, a subset of malicious cyber-attacks. The cyber security company, McAfee, estimates that businesses worldwide lost "$300 billion to $1 trillion dollars" in 2013 due to "cyber-attacks."[39] The harm from malicious cyber-attacks encompasses more than just monetary loss: it may result in the loss of intellectual property,[40] loss of data, loss of privacy, loss of security, loss of reputation, and loss of sovereignty, plus numerous other iterations of loss.[41]

Harm from malicious cyber-attacks is arguably analogous to the harm prohibited by customary international environmental law. This theory of harm is premised on the damage done to the state either physically or monetarily, or, as will be discussed *infra*, harm may be something more intrinsic like the violation of a state's sovereignty. However, harm will most often be in the form of monetary damage. In the *Trail Smelter* arbitration, the arbiters specifically addressed the SO_2 damage as a matter of economic harm as Canada had to pay the United States for the damage done by the SO_2 emissions. Even in *Corfu Channel*,

---

37 *See e.g.*, *Consolidated Rail Corp. v. Gottshall*, 512 U.S. 532 (1994). (Thomas, J., discussing the legal principles regarding the application of intentional infliction of emotional distress as applicable to the United States Federal Employees Liability Act..)

38 *See, id., Harm*, Black's Law Dictionary.

39 McAfee, *The Economic Impact of Cybercrime and Cyber Espionage* 5, Center for Strategic and International Studies (July 2013). *See also*, Oxford Economics, *Cyber-Attacks: Effects on UK Companies*, Centre for the Protection of National Infrastructure (July 2014). (Discussing the cost of cyber-attacks to UK business and detailing the costs to such things for losses such as brand reputation, the loss of IP, and the costs of cleaning up after cyber-attacks). Note that both sources use the generic term "cyber-attacks" without distinction.

40 Oxford Economics, *id*.

41 *Id.*

Albania was forced to pay monetary compensation for the harm caused by the underwater mines which damaged British ships. In the case of harm resulting from ultra-hazardous activities, the harm is premised upon the cost of rectifying the damage from the ultra-hazardous activity. The equation of harm, damage, and monetary compensation may be found in every legal system. Therefore, there is no reason not to believe that monetary damage alone is not a harm.

The question then becomes the level at which the resultant harm from cyber-attacks implicates the state and amounts to an internationally wrongful act. The general rule from *Trail Smelter*, and the rule accepted in CIL is that the harm must be "significant or substantial."[42] This is difficult to quantify, as the effects of malicious cyber-attacks are dependent upon the nature of the attack, duration of the attack, the infrastructure involved, the businesses affected, and the state's or non-state actors' ability to mitigate the damages. As it is impossible to create a test to elucidate an exact standard, it is suggested here that the test for significant or substantial effects be similar to that of an armed attack: the malicious cyber-attack should be judged by its scale and effect based upon the totality of the damage resulting from the attack. This test would be based on the injured state's ability to absorb the uncompensated monetary harm from the malicious cyber-attack. Determining what constitutes significant or substantial is based upon the scale and effect of the attack upon the state as a whole. Such determination for scale and effect, given the difficulties of quantifying the harm suffered during cyber-attacks,[43] must be quantifiable to the standards of evidence discussed, *supra*; i.e., the evidence of actual harm suffered by a state and its citizens must rise to the level of clear and convincing evidence.

This study now applies the *Trail Smelter* theory of harm to malicious cyber-attacks. The *Trail Smelter* idea of harm is two-fold: (1) conduct that the state itself would protect its

42 Christina Voigt, *Principles of IEL* 23 (n.d.), http://www.uio.no/studier/emner/jus/jus/JUS5520/h12/undervisningsmateriale/3.-principles-in-iel.pdf.

43 *See*, Oxford Economics, *Cyber Attacks: Effects on UK Companies* 4-5, Centre for the Protection of National Infrastructure (July 2014). (Discussing the difficulties of quantifying damage due to cyber-attacks by business.)

citizens from;[44] and (2) economic damage resulting from another's injurious act.[45] It is argued that the first element is easily met regarding malicious cyber-attacks. While no quantitative study has been undertaken, it is reasonable to argue that the majority of states protect their citizens from cybercrime, cyber-espionage, and other types of cyber-harms covered under the term malicious cyber-attacks as used in this study.[46] The second element is also relatively clear as it has been demonstrated that there is great economic damage to individuals and states resulting from the injurious act of malicious cyber-attacks. Therefore, it is reasonable to believe that malicious cyber-attacks may equate to prohibited harms in international law.

Based upon this concept of harm with regard to malicious cyber-attacks, it is argued that the prohibitions contained in *Trail Smelter*, which is part of the CIL, may apply through analogy to states and malicious cyber-attacks. *Trail Smelter* prohibits, in the opinion of this study, a state from utilizing its cyber infrastructure to the detriment of another state and creates a duty for the state to prevent harm from non-state actors.

This application of *Trail Smelter* also simplifies the issue of attribution for state responsibility. State responsibility will lie if it can be shown by clear and convincing evidence that malicious cyber-attacks originated from a state's cyberinfrastructure and that it resulted in significant or substantial monetary damage. Attribution, therefore, would be reduced to simply an evidentiary burden since *Trail Smelter* has no requirement for demonstrating linkage to the state or its agents. Indeed, *Trail Smelter* does not engage the state for any other reason than holding the state responsible for the internal conduct that harms another. An oft-overlooked issue in *Trail Smelter* was that the state of Canada did not own or operate the smelters responsible for the SO_2 harm, yet it was held responsible for the damage associated therefrom.[47]

---

[44] Alexandre Kiss and Dinah Shelton, *Strict Liability in International Environmental Law* 1131, *in*, Law of the Sea, Environmental Law and Settlement of Disputes: Liber Amicorum Judge Thomas H. Mensah (Tafsir Malick Ndiaye and Rüdiger Wolfrum, eds. 2007).

[45] *Trail Smelter* Case (United States v. Canada), 3 Rep. Int'l Arbitral Awards 1905 (11 Mar. 1941).

[46] This premise is supported by the fact that the *Convention on Cybercrime*, ETS No., 185 (2001), has 47 state parties to the Convention.

[47] *See*, *Trail Smelter* Case (United States v. Canada), 3 Rep. Int'l Arbitral Awards 1905, 1915 (11 Mar. 1941). (Discussing the operation and ownership of the smelter in question).

The *Trail Smelter* arbitration has many critics within the international law community.[48] However, the principles put forth in *Trail Smelter* have been recognized by the ICJ. In the *Gabčíkovo-Nagymaros Project* case, the ICJ stated:

> [t]he existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of other States or of areas beyond national control is now part of the corpus of international law relating to the environment…[49]

The ICJ's recognition, combined with other uses of the *Trail Smelter* principle in international environmental law and as part of the general CIL, firmly establishes *Trail Smelter* in the corpus of international law. Thus, *Trail Smelter* may be used outside of the environmental context.

It is this recognition of the principles elucidated in *Trail Smelter* that lends itself to the instant issue. The *Trail Smelter* principles are broad enough, as discussed, to encompass by analogy the harm resultant from malicious cyber-attacks. *Trail Smelter* demonstrates that CIL already has mechanisms in place to hold states responsible for malicious cyber-attacks that result in harm of such magnitude as to impact the state itself, even if by analogy.

5.4. The *Corfu Channel* Principles Applied to Malicious Cyber-Attacks

The *Corfu Channel*[50] case was brought by the United Kingdom against Albania for the damage and loss of life suffered when U.K. warships struck mines off the coast of Albania

---

48 *See*, Austin L. Parrish, *Sovereignty's Continuing Importance? Traces of Trail Smelter in the International Law Governing Hazardous Waste Transport*, *in*, Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration (2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_ id=765404. (Stating that some scholars "dismiss the case as a relic from a bygone era"). *See also*, John H. Knox, *The Flawed Trail Smelter Procedure: The Wrong Tribunal, the Wrong Parties, and the Wrong Law*, *in*, Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration (2006), http://papers.ssrn.com/ sol3/papers.cfm?abstract_id=665682. (Arguing that the basic premise of the tribunal was flawed, that the international community has failed to adopt the mechanisms utilized by the tribunal, that it utilized United States law, and that governments refuse to utilize the *Trail Smelter* model).

49 Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia) 1997 I.C.J. Rep. 7, 41 (Sep. 25).

50 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 (April 9).

on October 22, 1946. The contention by the United Kingdom, which was accepted by the court, was that the mines had been laid after the channel had been swept for mines, that Albania knew that the mines had been laid, that Albania failed to notify ships transiting the channel of the presence of mines in violation of international law, and that Albania was responsible for the losses suffered by the United Kingdom.

The court elucidated several theories that are germane to the issue at hand.[51] While it is accepted that stare decisis does not operate in the instant matter, the theories promulgated by the ICJ have been accepted into the corpus of CIL.[52] *Corfu Channel*, like the *Trail Smelter* arbitration, may not be directly on point with the issue of malicious cyber-attacks, but the theories promulgated by *Corfu Channel* are broad enough to be incorporated into principles concerning malicious cyber-attacks. It is important to note ab initio that the court never ascertained who actually laid the mines and relied instead on indirect attribution;[53] nevertheless, the court held Albania responsible for the explosions. The fact that the sea mines were found in Albanian waters was enough.[54]

The *Tallinn Manual* explains the holding in *Corfu Channel* by the ICJ as:

> *Corfu Channel*. . . implies that a State may not knowingly allow its territory to be used for acts contrary to the rights of other States. Accordingly, States are required under international law to take appropriate steps to protect those rights. This obligation applies not only to criminal acts harmful to States, but also, for example, to activities that inflict serious damage or have the potential to inflict serious damage[.][55]

This is an expansion of the duty to do no harm as put forth in *Trail Smelter*. However, the ICJ elucidated a mens rea element into the test for state responsibility under this theory.

---

51 *See*, Sarah Heathcote, *State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility* 295, 299, *in*, The ICJ and the Evolution of International Law (Karen Bannelier, Theodore Christakis, and Sarah Heathcote, eds. 2012).

52 *See e.g.,* Legality of the Threat or Use of Nuclear Weapons, Advisory Op., 1996 I.C.J. Rep. 22 (8 Jul.).

53 *Id.* at 17.

54 *Id.*

55 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, R.5, cmt. 3 (Michael N. Schmitt ed. 2013).

The knowledge element will be analyzed *infra* Chapter Six. In addition to the mens rea element, *Corfu Channel* sets forth several other important theories which are applicable, by analogy, to the issue of malicious cyber-attacks. These theories are general in nature and applicable to any instance of harm resulting from a state's action, including malicious cyber-attacks.

The requirements that the court in *Corfu Channel* elucidated that are important to this study are:

- A state whose territory is utilized for "an act contrary to international law. . . may be called upon to give explanation[;]"[56]
- A state may not proclaim ignorance of the harmful act without giving evidence to support the claim that it did not know of the act or those responsible for the act;[57]
- While an act originating from a state's territory does not by itself constitute prima facie proof of state responsibility, the fact that a state's territory is used "must be regarded as of special weight when it is based upon a series of facts linked together and leading logically to a single conclusion[;]"[58]
- The attitude of the state prior to and after the attack, the prior acts of a state,[59] and the feasibility of the state carrying out the attacks may be considered when ascertaining the probability of a state's responsibility for an attack; and
- That a state may not "allow *knowingly* its territory to be used for the acts *contrary to the rights* of other States."[60]

Many of the theories the court addressed in *Corfu Channel* may be seen as a continuation of the holding in *Trail Smelter*. While the cases are distinct and involve different tribunals, the theory behind *Trail Smelter* and its core holdings are seen in the ICJ's decision in *Corfu*

56 *Id.* at 18.

57 *Id.*

58 *Id.*

59 *Id.* at 19.

60 *Id.* at 22. (Emphasis added.)

Channel. These core holdings and theories posited by the court are directly applicable to this study, which will address these issues to demonstrate and discuss their applicability to cyber-attacks.

5.4.1. Corfu Channel Applied to the Issues of Cyber-Attacks: Discussion

This study will take the above issues in reverse order, first addressing what constitutes knowledge on behalf of a state, and then discussing what a state's rights are in regards to cyber-attacks. This study will then briefly address the other issues raised by *Corfu Channel.* This section will conclude with a discussion of how the *Corfu Channel* prohibitions, along with those put forward in *Trail Smelter,* apply concerning the prohibition on states not to allow their territories to be utilized to harm another state, vis-à-vis malicious cyber-attacks.

5.4.2. Corfu *Channel*: The Issues of Knowledge and Harm in Malicious Cyber-Attacks

Knowledge may be generally defined as "[a]n awareness or understanding of a fact or circumstance."[61] For the purposes of this study, knowledge may be broken down into three types: (1) actual, (2) constructive, and (3) imputed. Actual knowledge of a state would be "direct and clear knowledge"[62] of a fact derived from actual awareness gained either through direct knowledge of its agents or from information received from other states or an international organization. For malicious cyber-attacks, direct knowledge would apply when a state has a knowledge of a malicious cyber-attack originating from within its sovereign territory, or it receives notice from another state or international organization that a cyber-attack has been recursively traced to an IP address within a state's sovereign territory. Any type of knowledge on behalf of a state may be enough to implicate the state under the theories herein discussed.

---

61 Black's Law Dictionary 950 (9th ed. 2011).

62 *Id. See also, id*. ch. 2. (Discussing the idea of knowledge on behalf of the Taliban for the actions of Al-Qaeda).

Constructive knowledge is "knowledge that one using reasonable care and diligence should have, and therefore is attributed by law to a given person [or State]."[63] This is the knowledge that Albania was presumed to have had in the *Corfu Channel* case,[64] and the court used that knowledge as a basis for holding Albania responsible.[65] This knowledge is applicable to malicious cyber-attacks under the same theory, albeit with one caveat: a state has an affirmative duty to use reasonable care and due diligence in monitoring its cyber infrastructure to the extent of its technical ability while balancing the personal liberties of its people in accordance with international law. This idea of due diligence will be addressed in Chapter Six, *infra*. In the cyber context, constructive knowledge of a state is premised on the state's knowledge of the probability that malicious cyber-attacks are originating from its territory, past history of malicious cyber-attacks originating from within its territory, the likelihood of malicious cyber-attacks originating from its territory, and the state's ability to monitor for such attacks.

Constructive knowledge is a difficult standard as the technical ability to monitor for malicious cyber-attacks is dependent upon the individual State's technical ability; therefore, this standard is to be viewed within the context of the ability of the state. That is, the less advanced the cyber infrastructure of a state, and the lesser the state's ability to monitor its networks within the parameters of international law, the less likely of a finding of constructive knowledge. The inverse of this is also true; the more advanced the cyber infrastructure of a state, or the more control the state exerts over its infrastructure,[66] the higher the likelihood of imputed knowledge of cyber-attacks.

---

63 *Id.*

64 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9). (The court states "[f]rom all the facts and information mentioned above, the Court draws the conclusion that the laying of the minefield which caused the explosion of October 22nd, 1946 could not have been accomplished without the knowledge of the Albanian government." Here, where the Court uses knowledge, it is referring to either actual or implied knowledge on behalf of Albania as the court discusses the issue of due diligence prior.)

65 *Cf.* Sarah Heathcote, *State Omissions and Due Diligence* 295, in, The ICJ and the Evolution of International Law: The Enduring Impact of the *Corfu Channel* Case (Karine Bannelier, Theodore Christakis, and Sarah Heathcote eds. 2012). (Arguing that the rule of due diligence existed prior to the ICJ's decision in *Corfu Channel*).

66 *Cf.*, Jason Healey, *Concluding Remarks* 295, *in*, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (2013). (Discussing the impact of state-controlled Internet and the increasing likelihood that the state is responsible for a cyber-attack).

Imputed knowledge is important as it correlates with the knowledge discussed in *Corfu Channel*. Implied knowledge is "knowledge attributed to a given person [or State]"[67] based upon the relationship of the parties. If an agent of a state has a knowledge of a malicious cyber-attack, that knowledge may be imputed to the state itself, just as if the state had actual knowledge. This form of knowledge would be applicable in cases of states informally utilizing non-state groups (proxies) to conduct cyber operations in support of the state's objective, as has been alleged in the cyber-attacks in Estonia and Georgia. Under an imputed knowledge theory, if a state's agent has knowledge of the non-state actor's attacks, then that knowledge would, therefore, be attributed to the state for the purposes of state responsibility.

The knowledge element as elucidated by *Corfu Channel* may be met by any of these three types of knowledge. This is important in the context of malicious cyber-attacks in that by utilizing the knowledge elements put forth in *Corfu Channel* and adopting a broader understanding of them, CIL could more easily attribute malicious cyber-attacks to the responsible state. A state that has a knowledge of a malicious cyber-attack and fails to prevent the same may be responsible by omission just as if the state itself had carried out the malicious cyber-attack.

The knowledge prong is not the only issue from *Corfu Channel* that needs to be understood. The Court proclaimed that a state might not "allow *knowingly* its territory to be used for the acts *contrary to the rights* of other States."[68] This study will present what it believes constitutes an "act contrary to the rights of other States"[69] with respect to malicious cyber-attacks.[70]

"Acts contrary to the rights of other States"[71] encompasses a broad range of rights that a sovereign state enjoys. The rights of states overlap with the theory of unlawful political

---

67 Black's Law Dictionary 950 (9th ed. 2011).

68 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9) (emphasis added).

69 *Id.*

70 *See also*, Chapter Four, *supra*.

intervention. States' rights are a much farther-reaching issue; while the modern emphasis in international law has been to focus on the rights of the individual, the rights of states, particularly in regards to malicious cyber-attacks, is still an important and often overlooked issue. States' rights will be addressed only briefly; it is beyond the scope of this study to address this issue in depth and is worthy of advanced study in itself.

As a general proposition, all states enjoy a multitude of rights; these rights derive from and are included in the concept of state sovereignty.[72] By virtue of being an independent state, international law affords each state with implicit rights: to be an equal among all states,[73] to be free from threats of force and the use of force,[74] the right to manage one's own economy, the right to protection of one's economy and wealth, the right to economic freedom, the right to political stability, and the right to one's own intellectual property and

---

71 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9). *See also,* Ch. 1, *supra*. (Regarding the discussion of malicious cyber-attacks as international wrongful acts).

72 *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in accordance with the Charter of the United Nations*, G.A. Res.2625 (XXV), U.N.. Doc. A/RES/25/2625 (24 Oct. 1970). ("(1)… All States enjoy sovereign equality. They have equal rights and duties and are equal members of the international community, notwithstanding differences of an economic, social, political or other nature.
In particular, sovereign equality includes the following elements:

a. States are judicially equal;
b. Each State enjoys the rights inherent in full sovereignty;
c. Each State has the duty to respect the personality of other States;
d. The territorial integrity and political independence of the State are inviolable;
e. Each State has the right freely to choose and develop its political, social, economic and cultural systems;
f. Each State has the duty to comply fully and in good faith with its international obligations and to live in peace with other States.").

See also, Montevideo Convention on the Rights and Duties of States, *in*, U.S. Dep't of State, Pub. 1983, *Peace and War: United States Foreign Policy, 1931-1941,* 198-203 (1943). http://www.ibiblio.org/pha/paw/. (Discussing what constitutes a state in international law and the state's rights and duties) *and* Draft Declaration on Rights and Duties of States, G.A. Res. 375(IV) (6 Dec. 1949).

73 *Draft Declaration on Rights and Duties of States* Art. 4, G.A. Res. 375(IV) (6 Dec. 1949). *See also,* Phillip Marshall Brown, *The Rights of States Under International Law*, 26 Yale L. J. 85, 88-89 (1916). ("The 'right' of sovereignty, like the 'right' of independence, is theoretically a logical corollary of the 'right' to exist. If a State is to be allowed to enjoy and maintain its own separate existence; if, as a responsible international personality, it is to possess a 'reciprocating will,' it must possess freedom of will: it cannot be subject to the sovereign will of another.")

74 *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations*, G.A. Res.2625 (XXV), U.N. Doc. A/RES/25/2625 (24 Oct. 1970). Marshall Brown, *The Rights of States Under International Law*, 26 Yale L. J. 85 (1916).

that of one's citizens.[75] A state also has the right to control the ingress and egress of its borders and the right to protect itself from all forms of attack. As long as a state does not violate the protected rights of its citizens and comports itself within the customary norms of international law, a state is arguably free to do as it pleases with both its territory and its people (subject to, and balanced against, the rights of the individual under international law), and other states should respect its actions.

Any act via cyberspace that is contrary to the rights of the state may violate the principles set out in *Corfu Channel*. Malicious cyber-attacks that impact a state negatively and are without that state's consent may be considered "[a]cts contrary to the rights of [the] State[],"[76] particularly if the malicious cyber-attack is an act intended to attack the integrity of a state's sovereignty; in other words, the attack impacts the core rights that a state enjoys in international law and is conducted by a state or non-state actor as a means to gain an advantage. The advantage may be technological, monetary, political, or as punishment for an act of the effected state.

Cyber-attacks violating the *Corfu Channel* principle prohibiting acts contrary to the rights of states are constrained by the same CIL as any other violation. This means a single *de minimis* attack will not normally create an obligation on behalf of the offending state.[77] The contrary act via cyberspace must be a direct interference with the rights of a state which causes the state to suffer actual harm of such magnitude that it offends the very concept of the state and impacts the sovereign rights which rest solely with that state.

Returning to the overall theory of this section, it must be noted that the violation of the rights of a state, by itself, is a harm that falls within the theory that a state may not

---

75 *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations*, G.A. Res.2625 (XXV), U.N. Doc. A/RES/25/2625 (24 Oct. 1970). Montevideo Convention on the Rights and Duties of States, *in*, U.S. Dep't of State, Pub. 1983, *Peace and War: United States Foreign Policy, 1931-1941*, 198-203 (1943). http://www.ibiblio.org/pha/paw/. Draft Declaration on Rights and Duties of States, G.A. Res. 375(IV) (6 Dec. 1949). Marshall Brown, *The Rights of States Under International Law*, 26 Yale L. J. 85 (1916).

76 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 (April 9).

77 *See*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) 1986 I.C.J. 14, 92-94 (June 27).

knowingly inflict harm to another state. The harm is in the act itself, as the harm the state suffers is a degradation of the very ideas that make a state a state in international law. However, this act may not be enough by itself to rise to the level where the injured state may seek satisfaction.

Simply stated, an attack on those rights that a state enjoys harms the state's independence and standing. The harm is to the state's very nature and should be seen as an affront to all states under the theory of equality of states. Not only does the state suffer economically, politically or technologically, but it also suffers an attack directed at the very essence of the state itself. Such attacks threaten the core of the very international legal system, which ensures the standing of states and promotes peace and equality. In theory, such attacks may be viewed gravely, but reality treats them differently: they have become commonplace, and states have accepted them as part and parcel of the cyber age. While theoretically, every malicious cyber-attack may be a violation of the rights of a state, only those malicious cyber-attacks that meet the scale and effect test., will trigger a violation of the posited norm.

5.4.3. Corfu Channel and Cyber-Attacks: Other Considerations

Corfu Channel establishes four other ideas that are applicable and worth consideration regarding their impact upon CIL as applied to cyber-attacks. These are:

1. A state whose territory is utilized for "an act contrary to international law. . . may be called upon to give explanation[;]"[78]
2. A state may not proclaim ignorance of the harmful act without giving evidence to support the claim that it did not know of the act or those responsible for the act;[79]
3. While an act originating from a state's territory itself does not constitute prima facie proof of state responsibility, the fact that a state's territory is used "must be regarded as of special weight when it is based upon a series of facts linked together and leading logically to a single conclusion;"[80]

---

78 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 18 (April 9).

79 *Id.*

4. The attitude of the state prior to and after the attack, the prior acts of a state,[81] and the feasibility of the state carrying out the attacks may be considered when ascertaining the probability of a state's responsibility for an attack.

These ideas will be addressed briefly to demonstrate and analyze their applicability by analogy to malicious cyber-attacks and the overall theory of attributing malicious cyber-attacks to states for the purpose of state responsibility.

This study addresses those malicious cyber-attacks which amount to an internationally wrongful act based upon the scale and effect of the attack, which has been recursively traced to a state's cyberinfrastructure and for which circumstantial attribution points to the state whose territory is alleged to have spawned the cyber-attack. While this may not always be the case, these presumptions allow this study to establish and discuss a malleable baseline for such malicious cyber-attacks for future application.

The first issue is that "[a] State whose territory is utilized for "an act contrary to international law. . . may be called upon to give explanation[.]"[82] This prescription is directly applicable to the issue of malicious cyber-attacks. Due to the nature of malicious cyber-attacks, a state may not have knowledge of a malicious cyber-attack originating from its territory (or, in the case of DDoS attacks, this may implicate a number of states). As such, this idea may be said to have a precursor element: the attacked state must give the attacking state notice that the attacking state's cyber infrastructure and territory is responsible for malicious cyber-attacks. This serves not only to give the state notice but also to shift the burden onto the attacking state to take action, or "give explanation;" it may also serve as circumstantial evidence regarding attribution for state responsibility.[83] This means that once a state has notice of a malicious cyber-attack originating from its cyber

80 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 18 (April 9).

81 *Id.* at 19.

82 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 18 (April 9).

83 *See*, Jason Healey, *Concluding Assessment* 271, *in*, A Fierce Domain: Conflicts in Cyberspace, 1986 to 2012 (2013). (Discussing that the lack of state cooperation into the investigation of a cyber-attack may be an element of the analysis in circumstantial attribution of an attack to a state). *Cf.* Convention on Cybercrime Art. 23, ETS. No. 185 (23 Nov. 2001). (Codifying the principle of cooperation between parties to the cybercrime treaty).

infrastructure, it has an affirmative duty to take action to the best of its technical abilities to stop the attack and to prevent violation of the norms posited *supra.* At the very least, the state from which the malicious cyber-attacks originated from must give an explanation regarding the attack, what steps the attacking state took to curtail the attack, and explain how it failed to prevent the attack when called upon to do so.

The second issue to consider is that "[a] State may not proclaim ignorance of the harmful act without giving evidence to support the claim that it did not know of the act or those responsible for the act."[84] This second issue is closely tied to the first. It shifts the burden onto the accused state to provide evidence that its cyber infrastructure was not used, or, if it was used, that it was either a stepping-stone for the attack (a stepping-stone state may not be responsible for the attack[85] because the attack was launched from another territory and was routed through the cyberinfrastructure of the state), or that the state did not have a knowledge of the attack, and provides such evidence to assist in the investigation into the matter.[86] This issue works concurrently with the first issue to ensure state cooperation with the resolution of malicious cyber-attacks. A state that is unwilling to provide such evidence is not automatically responsible for the attacks, but the unwillingness to assist in the investigation is circumstantial evidence that may be used to attribute the attack to that state, wrongfully or otherwise.

Issues three and four reflect the ideas posited *supra*. Issue three states that "[w]hile an act originating from a State's territory itself does not constitute prima facie proof of state responsibility," the fact that a state's territory is used, "must be regarded as of special weight when it is based upon a series of facts linked together and leading logically to a

---

84 *Id.*

85 *Cf. Tallinn Manual on the International Law Applicable to Cyber Warfare* R. 8 (Michael N. Schmitt ed. 2013) ("The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the cyber operation to that State.").

86 *Cf., Tallinn Manual on the International Law Applicable to Cyber Warfare* R. 8, cmt. 2 (Michael N. Schmitt ed. 2013). (Discussing cyber-attacks that meet the requirements of illegal force: "[P]ursuant to rule 5, a State must not knowingly allow its cyber infrastructure to be used to the rights of other States. However, the International Group of Experts was unable to achieve consensus as to whether that rule applies to States through which cyber operations are routed. To the extent that it does, the State of transit will bear responsibility for failing to take reasonable measures to prevent that transit.")

single conclusion."[87] Issue four posits that "[t]he attitude of the State prior to and post-attack, [combined with] the prior acts of a State,"[88] and the probability of the state's cyberinfrastructure being implicated in the attack may be considered when ascertaining the probability of a state's responsibility for an attack.

These four *Corfu Channel* elements may be used by an injured state when attempting to hold a state responsible for the violation of the duty to do no harm. The injured state may seek proof from the accused state, to which the accused state must give a substantive reply. The injured state may also take into consideration that the attack, subject to the proof offered by the accused state, originated from the territory of the accused state, and the injured state may consider past acts of the accused state along with the accused state's attitude concerning the accused violation. None of these elements alone is dispositive for purposes of attribution, but when taken together, they form a paradigm accepted in international law which may aid in attribution based upon the accused state's conduct. The *Trail Smelter* and *Corfu Channel* cases demonstrate specific ideas in CIL that are directly applicable to the problem of malicious cyber-attacks.

These issues are particularly appropriate given that, as is true with the majority of malicious cyber-attacks, the harm caused in the *Trail Smelter* case was transboundary and caused by a non-state actor, and the attacks in *Corfu Channel* were only indirectly attributed to the state. Since these facts are analogous to the majority of malicious cyber-attacks, the CIL established in these cases is applicable through analogy to malicious cyber-attacks. This idea is put forth in the *Tallinn Manual* as the comments to Rule 5 state:

> [t]he International Group of Experts deliberately chose not to limit the prohibition [contained in rule 5] to narrower concepts. . . in order to emphasize that the prohibition extends to all cyber activities from one State's territory that affect the rights of other States and have a detrimental effect on another State's territory.[89]

87 *Id.*

88 *Id.* at 19.

89 *Tallinn Manual on the International Law Applicable to Cyber Warfare* R. 5, cmt. 5 (Michael N. Schmitt ed. 2013). Rule 5 establishes that "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive control to be used for acts that adversely and unlawfully affect other States."

This prohibition on the use of one state's territory to harm another state is recognized in CIL, and it provides a mechanism to hold a state responsible for malicious cyber-attacks originating from within their sovereign territory without direct attribution. Under CIL, the accused state must either demonstrate that it was not responsible for the attacks or that the state whose territory was utilized to harm another state took appropriate action to prevent malicious cyber-attacks to the best of its technical abilities. Otherwise, responsibility may attach.

5.5. Strict Liability, Ultra-Hazardous Activities, and Customary International Environmental Law as Applied to Malicious Cyber-Attacks

Customary international environmental law recognizes, in limited circumstances, that the existing international legal framework is inadequate regarding certain specific activities.[90] These activities include: "nuclear power plant operation, space launches, orbital spacecraft and satellite operation, shipment of petrochemicals, and *other activities*."[91] These activities are referred to as "ultra-hazardous"[92] in recognition of the potential harm associated with them. These ultra-hazardous activities are regulated through the emerging legal paradigm of strict liability: any state whose territory is utilized for these activities may be held strictly liable for any harm resulting from those activities. Strict liability means that irrespective of the cause of the harm, as long as the harm is related to the identified activities, then the state is responsible without any other considerations.[93] Charme believed that such an emerging legal paradigm should be regarded as an emergence of CIL regarding the application of strict liability for states.[94]

---

90 Joni S. Charme, *Transnational Injury and Ultra-Hazardous Activity: An Emerging Norm of International Strict Liability*, 4 J. L. & Tech. 75(1989).

91 *Id.* (Emphasis added.)

92 *Id.*

93 *See also*, *Strict Liability*, Black's Law Dictionary (9th ed. 2009). ("Liability that does not depend on actual negligence or intent to harm, but is based on the breach of an absolute duty to make something safe…").

94 Joni S. Charme, *Transnational Injury and Ultra-Hazardous Activity: An Emerging Norm of International Strict Liability*, 4 J. L. & Tech. 75(1989). *But cf.* Kai Sheffield, *Of Pulp Mills and Oil Spills: Strict State Liability Under Customary International Law When Energy and Resource Projects Cause Transboundary Environmental Harm*, Ecobulletin 4 (June 2011).

The premise for holding states liable for such activities is based upon the activities themselves and the potential for widespread environmental harm resulting from otherwise lawful activities. States know or should know that these activities have the potential for great harm due to their very nature. Ultra-hazardous activities have a much greater chance of causing significant harm and the resulting damage from the ultra-hazardous activity is much greater than the harm from other lawful acts.

The harm resulting from ultra-hazardous activities may also result in more diverse and widespread damage, and the resultant damage is difficult to minimize or contain. In theory, states balance the costs and benefits of such activities, and the states find that it is in their interests to utilize the ultra-hazardous activity despite the risks. If an incident happens that causes harm related to the ultra-hazardous activity, the state is held liable without a showing of fault or negligence[95] because the state has accepted the risks associated with the activity.

The question, therefore, is whether this imposition of strict liability for ultra-hazardous activities extends to acts in cyberspace by analogy, and, if so, whether a state may be held strictly liable for malicious cyber-attacks that originate from its sovereign territory based upon the potential for harm that is associated with Internet availability and malicious cyber-attacks.

At first glance, the idea of holding states strictly liable for the use of their cyber territories may seem to be an overreach. However, if this idea of strict liability is looked at as a purely economic function—if one compares the monetary loss or harm due to traditional ultra-hazardous activities to that of monetary losses or harm resulting from malicious cyber-attacks—the theory becomes less abstract, this idea of economic harm and monetary loss will be explored in-depth, infra.

(Discussing whether strict liability for transboundary harm is recognized as CIL. Sheffield discusses that while *Trail Smelter* stands for such a proposition, states have not seemingly embraced the idea as a matter of state practice though there are circumstances where the issue is raised in *opinio juris*.)

95 *See generally*, Kai Sheffield, *Of Pulp Mills and Oil Spills: Strict State Liability Under Customary International Law When Energy and Resource Projects Cause Transboundary Environmental Harm*, Ecobulletin (June 2011).

Prior to discussing the theory of strict liability, malicious cyber-attacks and the ultra-hazardous paradigm, a brief analysis of the environment for malicious cyber-attacks, the economic factors of cyber-attacks, and the commonalities will be discussed to allow for better comparison to traditional forms of ultra-hazardous activities.

5.5.1. Operating Environments: Comparing Cyber Space to the Natural Environment

The idea of applying the CIL theory of ultra-hazardous strict liability to cyberspace is in part dependent upon analogous environments: the harm done to the natural realm should be and is analogous to harm done in the cyber realm. One may be puzzled by the analogy of the natural environment to that of cyberspace. At first blush, the two systems seem to be as different as imaginable. However, in reality, the systems are similar in many respects. First, both systems lack a true definition of what they encompass. For instance, "the [natural] environment is a term that everyone understands, but no one is able to satisfactorily define."[96] This statement is applicable to cyberspace as cyberspace does not have a true definition;[97] however, that does not stop commentators from discussing cyberspace (or the natural environment) in depth. Second, both systems are interconnected and discrete, and they significantly impact human lives. Third, both systems are highly complex and dependent upon keystone features. Fourth, both systems encompass the globe, are composed of distinct yet interrelated parts and are impacted greatly by human interaction.

As a universally accepted definition for cyberspace has yet to be formulated, for the purposes of this study, the *Tallinn Manual*'s definition of cyberspace is adopted. The *Tallinn Manual* defines cyberspace as "[t]he environment formed by physical and non-physical components, characterized by the use of computers and the electromagnetic

96 Thilo Marauhn, *Customary Rules of International Environmental Law–Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace? 465, 466* in *Peacetime Regime for State Activities in Cyberspace* (Katharina Ziolkowski ed. NATO 2013).

97 *See, e.g., id.*

spectrum, to store, modify, and exchange data using computer networks."[98] The global Internet is only one part of the concept of cyberspace, albeit a significant part. Cyberspace "has political, economic, social and cultural aspects going far beyond the notion of pure means of information transfer."[99] Like the natural environment, cyberspace has no delineated boundaries; cyberspace is ever-growing and theoretically infinite.

While it would be an exaggeration to claim that cyberspace is as important as the natural environment, the digital environment is the lifeblood of communication and commerce for the modern individual, business, and state, and multiple other operations are dependent upon it. It is not too great a stretch to proclaim that modern life is dependent upon the digital environment that is cyberspace. The majority of the planet is touched directly or indirectly and facilitated through cyberspace, and with each passing day, the world arguably becomes more dependent on it.

Like the acts of states and individuals that cause harm to the natural environment across state boundaries, malicious cyber-attacks are manmade and create harm across multiple state boundaries; they may also cause similar effects and have a similar economic impact as those incidents in the natural world. The major difference is that natural transboundary harm may be localized due to environmental conditions, i.e., natural environmental harm may be localized to a particular area dependent upon environmental factors such as weather, water courses, time of year, etc. Malicious cyber-attacks are not limited by means of traditional geography or environmental conditions; it is possible that they impact even more individuals and create even greater economic harm. An attack that impacts London may also impact New York, Los Angeles, Bangkok, and many other disparate locations.[100] Malicious cyber-attacks may impact cyberspace and the digital environment irrespective of the geography of the targets, creating a greater global impact than the majority of environmental tragedies.

---

98 *The Tallinn Manual on the International Law Applicable to Cyber Warfare* 258 (Michael N. Schmitt, ed. 2013).

99 Thilo Marauhn, *Customary Rules of International Environmental Law–Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace? 465, 466* in *Peacetime Regime for State Activities in Cyberspace* (Katharina Ziolkowski ed. NATO 2013).

100 A good example of this is the Stuxnet worm discussed in Chapter One *supra*. Stuxnet was mainly directed toward the Iranian nuclear program, but after the worm escaped to the wild, it was found in multiple computer systems worldwide.

The comparison of transboundary harm to the natural environment and transboundary harm caused by malicious cyber-attacks may be strengthened by a comparison of damages or cost of harm from incidents. While it is impossible to quantify the true cost of either environmental disasters or the losses to cyber-attacks, rough parallels may be drawn. For instance, the British Petroleum/Deepwater Horizon oil spill in the Gulf of Mexico in 2010 cost an estimated $64 billion (£40 billion) for cleanup, compensation, court costs, fines, and settlement costs.[101] The 1986 Chernobyl nuclear disaster in Ukraine as cost an estimated $235 billion over the past 25 years and is expected to grow by another $1-2 billion.[102] In comparison, according to McAfee, "cybercrime, cyber espionage, and malicious cyber activities"[103] cost an estimated $300 billion to $1 trillion per year globally.[104] While one-off environmental tragedies are not necessarily representative of the ongoing cost of environmental degradation, they do provide some information for comparison. Both types of incidents include a human element, meaning that both types of incidents may directly impact the individual. In natural disasters, the human element may be exposed to toxins or radiation, as in cases of transboundary environmental harm. The human element regarding malicious cyber-attacks may be harm through financial loss, damage to digital equipment that the individual relies upon, or through triggering events such as loss of power, destruction of nuclear plants, or disabling air traffic control, all of which results in direct harm to the individual.

The individual is impacted by incidents in both the natural and cyber environments. While no individual life has been directly claimed due to malicious cyber-attacks as of this writing, malicious cyber-attacks have been utilized as adjuncts to kinetic attacks that have

101 Graeme Wearden, *BP Oil Spill Costs to Hit £40-billion*, The Guardian (2 Nov. 2010), http://www.theguardian.com/business/2010/nov/02/bp-oil-spill-costs-40-billion-dollars.

102 Mikka Pineda, *Fukushima Vs. Three Mile Island Vs. Chernobyl*, Forbes (17 Mar 2011), http://www.forbes.com/2011/03/16/japan-disaster-nuclear-opinions-roubini-economics.html.

103 McAfee, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies 3 (July 2013).

104 It is impossible to quantify either the true cost of environmental disasters or the losses suffered by cyber-attacks.

resulted in reported deaths.[105] Individuals are impacted by both direct and indirect costs of malicious cyber-attacks, such as loss of productivity, loss of confidence, and psychological trauma. It must be remembered that while malicious cyber-attacks occur in the abstract against states, corporations, and other entities, it is the end consumer and user that ends up paying, directly and indirectly, for the damages done by cyber-attacks.

Crawford [106] posited that environmental damage is "incremental and may involve complex and diffuse causal mechanisms[.]" This idea is analogous to that of malicious cyber-attacks, which may be described in the same terms. Environmental damage and malicious cyber-attacks are either highly complex, man-made problems, or they may be relatively simple and straightforward. Just as a dam bursting due to excessive rainfall may cause environmental damage, a dam that fails to open its floodgates due to a simple Trojan locking out a control panel may cause identical environmental damage. In this manner, a direct analogy to environmental law as applied to malicious cyber-attacks is fully warranted and appropriate as the resultant damage is constant in both.

Commentators have likened cyberspace to a global commons, or Common Pool Resource (CPR).[107] Like other natural commons shared by humanity, cyberspace too is a shared resource. The other recognized commons are the "the High Seas; the Atmosphere; Antarctica; and, Outer Space[,]"[108] which, like cyberspace, are beyond the control of any

105 *See,* Erich Follath and Holger Stark, *The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor*, Spiegel, (Nov. 2, 2009), http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html. (Discussing how cyber-attachs against Syrian anti-aircraft installations may have resulted in deaths from a kinetic attack.) David Makovsky, *The Silent Strike How Israel Bombed a Syrian Nuclear Installation and Kept it Secret*, The New Yorker (Sept. 17, 2012), http://www.new yorker.com/ magazine/2012/09/17/the-silent-strike. Ward Carroll, *Israel's Cyber Shot at Syria*, DefenseTech (Nov. 26, 2007), http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/.

106 James Crawford, *Brownlie's Principles of Public International Law* 354 (8th ed. 2012).

107 *See,* Charlotte Hess, *The Virtual CPR: The Internet as a Local and Global Common Pool Resource* (May 1995), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/234/iascp-95-II.pdf?sequence=1. (Positing that the Internet has four common overlapping commons: social, informational, budgetal, and technical).

108 United Nations Environmental Program, Division of Environmental Law and Conventions, *Background* (1 Oct. 2014), http://www.unep.org/delc/GlobalCommons/tabid/54404/Default.

single state, yet utilized by most. Like the traditional commons, cyberspace is used by the international community to the benefit and detriment of mankind.

Thus applying customary international environmental law and treaties by analogy to the issues regarding the Internet and cyberspace, particularly the misuse of the shared resource, allows for parallel guidance by analogy. Applying the theory of strict liability for transboundary harm to malicious cyber-attacks is an efficient means of creating an international legal regime for malicious cyber-attacks.

One factor that bears discussing is the role of non-state actors in both environmental harm and cyber-attacks. Dupuy and Hoss[109] posited that the majority of environmental harm results from the acts of non-state actors.[110] This same statement may be made regarding malicious cyber-attacks: a majority of malicious cyber-attacks are believed to be the work of non-state actors. It is argued that the significant distinction between the non-state actors who do environmental harm and the non-state actors responsible for cyber harm is that those who are responsible for environmental harm do not do so intentionally, but the harm results from an otherwise legal act; in contrast, those responsible for malicious cyber-attacks normally do so with intent to create harm, whether a non-state actor or state is responsible for the harm.

The harm done by malicious cyber-attacks, like that of environmental harm, may range from *de minimis* to catastrophic. The harm may be limited to the cyber domain or may extend into the physical world. The role of the non-state actor in both areas, however, necessarily imputes the state, as was demonstrated *supra*. Under existing CIL, it may be argued that a state has a duty to monitor and prevent non-state actors from utilizing its territory to cause harm in another sovereign's territory. This duty engages the state and makes it incumbent upon the state to do all within its technical abilities to prevent malicious cyber-attacks from being carried out within its sovereign territory, and the duty potentially

109 Pierre-Marie Dupuy & Cristina Hoss, *Trail Smelter and Terrorism: International Mechanisms to Combat Transboundary Harm, in* Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration 225 (Rebecca M. Bratspies & Russell A. Miller eds. 2006). (Linking transboundary environmental harm and terrorism to that of non-state actors).

110 *Id.*

makes the state strictly liable for malicious cyber-attacks that it is capable of preventing but fails to prevent.

5.5.2. Applying the Theory of Strict Liability to Cyber-Attacks

The idea of strict liability for conduct originating from one sovereign territory that is harmful to another state is not new by any means. Lassa Oppenheim posited his theory of strict (vicarious) liability for states over 100 years ago. He argued that:

> States are, according to the Law of Nations, in a sense responsible for certain acts other than their own—namely, certain unauthorized injurious acts of their agents, of their subjects, and even of such aliens as are for the time living within their territory. This responsibility of States for acts other than their own I name "vicarious" responsibility… [111] Since the Law of Nations is a law between States only, and since States are the sole exclusive subjects of International Law, individuals are mere objects of International Law, and the latter is unable to confer directly rights and duties upon individuals. And for this reason the Law of Nations must make every State in a sense responsible for certain internationally injurious acts committed by its officials, [and] subjects[.][112]

This theory of strict or vicarious liability is discussed in the comments of the ARS, where the ILC states:

> [i]n theory, the conduct of all human beings, corporations or collectivities linked to the State by nationality, habitual residence or incorporation might be attributed to the State, whether or not they have any connection to the Government. In international law, such an approach is avoided, both with a view to limiting responsibility to conduct which engages the State as an organization, and also so as to recognize the autonomy of persons acting on their own account and not at the instigation of a public authority. Thus, the general rule is that the only conduct attributed to the State at the international level is that of its organs of government, or of others who have acted under the direction, instigation or control of those organs, i.e., as agents of the State.[113]

111 Lassa Oppenheim, *International Law. A Treatise. Vol. 1 (Peace)* 246-248, (2nd ed., Kindle ed. 2012).

112 *Id.* at 248-249 (emphasis added).

113 *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, ch. 2, gen. cmt. 2, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

The ILC chose to limit the application of strict liability in part due to the decision in the *Tellini* case,[114] where the committee appointed by the Conference of Ambassadors to ascertain which state was responsible for the assassination of Enrico Tellini stated:

> [t]his responsibility of a State is only involved by the commission in its territory of a political crime against the persons or foreigners if the State has neglected to take all reasonable measures for the prevention of the crime and the pursuit, arrest and bringing to justice of the criminal.[115]

This finding seemed to be a deviation from the accepted rule at that time that a state was liable without exception for acts against other states originating from within a state's sovereign territory.[116] It may be argued that the ILC limited the applicability of strict liability as a matter of policy, not legality. It is argued that cases such as *Trail Smelter* and *Corfu Channel* and works of distinguished scholars such as Oppenheim, established a baseline for strict liability for states. That baseline has been recognized in customary international environmental law, but it has been limited within the ARS as a matter of policy. It is posited herein that strict liability as a matter of CIL is a practical method for holding states responsible for cyber-attacks originating from within their territories.

---

114. League of Nations, 4 O.J.L.N. 1349 (No.11, November 1923). Robert B. Kane, *The Corfu Incident, 1923*, 78-79, in, War in the Balkans: An Encyclopedic History from the Fall of the Ottoman Empire to the Breakup of Yugoslavia (Richard C. Hall ed., 2014). ***See also***, Draft Articles on Responsibility of States for Internationally Wrongful Acts, ch. 2, cmt. 4, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001). ***See also***, Franciszek Przetacznik, *Protection of Officials of Foreign States According to International Law* 104 (1983). (Discussing the *Tellini* case background and state responsibility for political crimes or offenses).

115 League of Nations, 4 O.J.L.N. 1349 (No.11, Nov. 1923). It is important to note that this rule exists in the ILC's ARS where states may be held responsible for their omissions. *See*, Chapter Seven, *infra*.

116 *See generally*, League of Nations, 4 O.J.L.N. 1246 et seq. (Nov. 1923). (Both parties to the dispute discuss the responsibility of the state in which the crime was committed. *See, e.g., id*. at 1288 (comments of M. Poltis) i.e. Greece accepts that it owes Italy reparation for the assassination as it occurred within Greece's territory, and that although Greece itself was not morally responsible, Greece seems to accept legal responsibility.)

5.5.3. Analysis of Strict Liability for Ultra-Hazardous Activities and Cyber-Attacks

Strict liability for ultra-hazardous activities is premised on similar theories as strict liability for states that knowingly allow their territory to be utilized for activities that have potentially deadly consequences and accept the responsibility for those acts. In simpler terms, the state benefits from allowing the ultra-hazardous activity and bears responsibility if the activity causes harm.[117]

Liability for ultra-hazardous activities is based upon knowledge of the potential harm that is allowing the activity entails, and deriving an economic benefit from the activity yet accepting the risk of the potential harm arising. Unlike the theory of strict liability posited *supra*, which is arguably a creature of CIL, strict liability for ultra-hazardous activities exists as a matter of treaty law and CIL. For instance, the *Convention on International Liability for Damage Caused by Space Objects* Art. 2[118] requires that "[a] launching state shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the Earth or to aircraft in flight." The preamble to the convention sets forth the rationale for strict liability stating that "[t]aking into consideration that, notwithstanding the precautionary measures to be taken by states and international intergovernmental organizations involved in the launching of space objects, damage may on occasion be caused by such objects[.]"[119] The treaty recognizes the potential danger of the act, so it ensures that if any accident may happen, the injured party will be promptly compensated. The convention also binds the state to be responsible for any party utilizing its territory for a space launch irrespective of whether or not it is acting privately or as an actor of the state. Thus, the convention only allows claims to arise from a state against another state.

---

117 Kai Sheffield, *Of Pulp Mills and Oil Spills: Strict State Liability Under Customary International Law When Energy and Resource Projects Cause Transboundary Environmental Harm*, Ecobulletin (June 2011).

118 U.N.G.A. Res. 2777 (29 Nov. 1971), *in*, United Nations Treaties and Principles on Outer Space, Related General Assembly Resolutions and Other Documents, U.N. Doc. ST/SPACE/61/Rev.1 (n.d.).

119 U.N.G.A. Res. 2777 (29 Nov. 1971), preamble.

As a matter of CIL, the strict liability for ultra-hazardous activities theory encompasses a broad range of activities as elucidated *supra*; the CIL theory is in line with that of the treaty version: a state is absolutely liable for damage arising from the activity. This theory may be extended to cover malicious cyber-attacks based upon the potential harm arising from malicious cyber-attacks, and the economic benefit states derive from the Internet and access to the World Wide Web. As has been demonstrated by historical and ongoing malicious cyber-attacks, the possibility of extreme economic damage from a malicious cyber-attack is real and present.

Just as a state knows the possibility of damage resulting from the operation of a nuclear reactor or damage from space launches, a state also knows the possibility of damage resulting from malicious cyber-attacks. This possibility of damage from an otherwise lawful activity, just like the aforementioned activities, place the state in a position where it must accept liability for the potential damages for the acts resulting from the misuse of the Internet, just as they would be responsible for damages resulting from the misuse of a nuclear reactor or a space launch, irrespective of the actors behind the misuse. In both instances, the state is held accountable for the activities within its sovereign territory.

This theory is supported by the sheer economic magnitude and the potential damage from malicious cyber-attacks. The economic damage resulting from malicious cyber-attacks, as discussed *supra*, is of such magnitude that states cannot claim that they are not aware of the danger arising from the use of the Internet. It is argued that the economic damage resulting from malicious cyber-attacks is on par with any other of the previously recognized ultra-hazardous activities, and as such, states should be held liable for the damages resulting from the otherwise lawful activity. This is particularly true when it is compared to the economic benefit that states derive from the use of the Internet for itself and its citizens.

5.5.4. Strict Liability Theories and Cyber-attacks: Conclusion

It is accepted that the theory of strict liability as applied to malicious cyber-attacks may seem, for lack of a better term, extreme. This study, however, uses the theory of strict liability to demonstrate an accepted norm in CIL that may apply to malicious cyber-attacks by analogy. States which utilize malicious cyber-attacks for their own purposes (e.g.,

espionage) and which result in a harm could be held responsible under the theory of strict liability for ultra-hazardous activities based on the states' knowledge of the potential for harm based upon the activity undertaken. In addition, applying the theory of strict liability for ultra-hazardous activities to malicious cyber-attacks would allow an injured state to seek compensation from the originating state. This theory also may create a situation in which states, knowing the potential for responsibility, will take steps to better monitor and secure their cyberinfrastructures to prevent malicious cyber-attacks to the best of their abilities.

Holding states responsible for the misuse of their cyber territories and giving injured states a mechanism for compensation for injuries suffered helps mitigate against scenarios where states utilize self-help to deal with the issue of cyber-attacks either through "hackback"[120] or other mechanisms, including the use of force.[121] While it is accepted that states may still seek self-help for injuries suffered, an alternative mechanism may diminish the desire to seek self-help in the first place.

This form of responsibility, however, would only apply to the originating state unless it may be shown that the state in which the malicious cyber-attacks originated "knowingly allow[ed] its cyber infrastructure located in its territory or under its exclusive governmental control to be used for"[122] such malicious cyber-attacks. Such a demonstration, however, must be balanced against the state's technical ability to do so. This study would subscribe to the theory that a state, to the extent of its cyber capabilities, has a duty to "take reasonable measures"[123] to prevent malicious cyber-attacks.

The above-posited theories ensure that states are cognizant of their cyber territories since they are responsible for the acts emanating from those cyber territories. This responsibility for a state's own cyber territory must be balanced against the inherent rights of each state's

120 Jay P. Kasen and Ruperto Mujeca, *Optimal Hackback*, 84 Chicago – Kent L. J. 831, 832 (June 2010).

121 *Id.*

122 *Tallinn Manual on the International Law Applicable to Cyber Warfare* R. 3 (Michael N. Schmitt ed. 2013).

123 *Id.*, R. 3, cmt. 7.

citizens' freedom of speech and expression.[124] A state cannot limit the individual's freedom due to the potential responsibility emanating from the state's own cyber territory; the state must balance the freedom of expression against the potential harm resulting from potential cyber-attacks being launched from its territory. This, in turn, may inspire states to further criminalize malicious cyber-attacks and strengthen their domestic law enforcement response to malicious cyber-attacks or balance such risks against possible international responses to cyber-attacks.

5.6. Conclusion: Alternative Theories for Holding States Responsible for Cyber-Attacks

This study has demonstrated that due to the nature of malicious cyber-attacks and the Internet, legal attribution of malicious cyber-attacks to the responsible author is difficult, if not impossible. Given the nature of the harm, the potential for creation of larger issues for harmed state's, and the possibility of kinetic spillover (not to mention the economic harm) and other harms suffered by states, this study argues that the alternative forms of state responsibility discussed herein offer a viable alternative for holding state's accountable outside the current CIL paradigm. Without finding alternative methods for assigning responsibility for conduct in cyberspace, it may be argued that malicious cyber-attacks will continue to grow with a strong probability of kinetic overflow as a result.

The theories posited in this chapter, both singularly and when taken together, demonstrate a pragmatic legal alternative to the problem of attribution and state responsibility. Under the duty to do no harm theory, a state could be held accountable for the violations of international law when the harm originates from within its territory if the state knew or should have known of the malicious cyber-attacks. The duty to do no harm has long been recognized in international law and is malleable enough to cover the harms inflicted upon states via malicious cyber-attacks by analogy.

---

124 *See e.g., The Universal Declaration on Human Rights* Art. 12, U.N.G.A. Res. 217A (1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence…").

The theory of strict liability for ultra-hazardous activities demonstrates that a state may be held accountable for allowing ultra-hazardous activities within their territory based on the knowledge of the risks associated with such acts. This theory may govern states' use of cyberspace through analogy: just as allowing certain kinetic acts in physical space implicate the state, allowing certain acts in cyberspace implicate the state for ultimate responsibility for those acts.

The prohibition on unlawful political intervention lies at the core of charter law and is applicable to malicious cyber-attacks that target political, economic, or cultural targets within a state in order to coerce a sovereign state to take a desired political action. The prohibition on unlawful political intervention recognizes particular prohibited acts on behalf of states that are unlawful; cyberspace has been shown to be an excellent vector for those prohibited acts. Nothing contained within the theory of the prohibition on unlawful intervention stipulates the vectors used in the prohibition; thus, the prohibition on unlawful political intervention applies directly to those acts in cyberspace.

All the above-discussed theories are strengthened regarding malicious cyber-attacks as they greatly reduce the complexity and necessity of attribution. Instead of determining if an internationally wrongful act has occurred and then attempting to attribute the wrongful act to a state actor for the purposes of state responsibility (which is difficult, if not impossible, in malicious cyber-attacks), the posited theories here only require an injured state to demonstrate through clear and convincing evidence that the cyber territory of a state was implicated in the attacks for responsibility to lie, a much easier task given the technical abilities of attack attribution.

Working together, these theories create a pragmatic framework for holding states responsible for malicious cyber-attacks which originate from within a state's sovereign territory. These theories are well recognized in international law and govern malicious cyber-attacks either through analogy or directly. This allows proven theories in international law to be applied to this relatively new problem, saving international law from having to reinvent the proverbial wheel to deal with this growing problem.

Chapter Six: Indirect Responsibility, Due Diligence, and the Duty to Prevent Malicious Cyber-Attacks

6. Introduction

This study now turns to the state's duty to prevent malicious cyber-attacks, the due diligence principle, and indirect responsibility of states in CIL. It will be argued in this chapter that based upon the obligations on states discussed in Chapter Five *supra*, a corresponding duty to prevent violations of these norms exists in CIL. In addition, it is argued that these obligations on behalf of states create a legal condition where a state may be indirectly responsible for the acts of non-state actors when the state has a duty to prevent an act but fails to do so.[1] The duty to prevent, however, is not solely associated with the theories discussed in Chapter Five *supra*; as will be discussed in the next section, a duty to prevent harms existing international law stands alone.

The duty to prevent harm exists in multiple norms of international law, including but not limited to, customary international environmental law, IHL, and international investment law.[2] As a matter of general CIL, the duty to prevent has arguably existed since Grotius noted that:

> a sovereign could become complicit in crimes of individuals through principles of *patientia* (where a community or its ruler know of a crime committed by a subject but fail to prevent if they can and should) and *receptus* (where a ruler fails to punish or extradite fugitives).[3]

---

1 *See e.g.*, Jan Arno Hessbruegge, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. Int'l. L. & Pol. 265, 268 (2004). ("Acts or omissions of non-state actors are themselves generally not attributable; however, the state may incur responsibility if it fails to exercise due diligence in preventing or reacting to such acts or omissions.")

2 *See generally*, International Law Association, *ILA Study Group on Due Diligence in International Law First Report* (07 Mar 2014). (Discussing various forms of the duty to prevent found in international law.)

3 *Id*. at 2, n. 2 (07 Mar 2014). *See also*, Aaron X. Fellmeth and Maurice Horwitz, Guide to Latin in International Law (2011). ("Patientia" translates from Latin to English as "forbearance."). *See also*, Hugo Grotius, *On The Law of War and Peace*, Bk. 2, Ch. 21, ¶ 2 (A.C. Campbell trans. 1814). ("In the case of a sovereign's responsibility for the acts of his subjects, there are two things to be considered, which require minute inquiry, and mature deliberation, and those are the forbearance, and the encouragement or protection, which he has shewn[sic] to their transgressions. As to forbearance, it is an acknowledged point, that when he knows of a

The duty to prevent has evolved into both general and specific norms. As discussed in Chapter Five, *supra*, a general duty to do no harm may be found in both *Trail Smelter* and in *Corfu Channel*. In addition to the duty to do no harm, a state has the corresponding duty to prevent those same harms from originating from within its territory. It is argued that a state, which has an obligation not to allow their territory to be used to the detriment of another state, has a corresponding duty to prevent their territory from being used to the detriment of another state. It is argued that a state may not allow conduct from non-state actors that the state itself is prohibited from engaging in. The duty to prevent therefore holds a state responsible for failing to prevent prohibited conduct. A state that fails to prevent a prohibited act, either through an act of the state or by omission by the state, has committed an internationally wrongful act by failing to prevent prohibited conduct and thus allowing an injury to another state which originated from within its sovereign territory. This general duty to prevent would encompass any act that a state may not lawfully engage in, not just the examples discussed herein. This duty to prevent is not absolute, as will be discussed *infra*; this study will argue that a state must have the ability to prevent the harmful acts in question for responsibility to lie.

6.1. The Duty to Prevent: Discussion

In addition to the general duty to prevent harm, states have a duty to prevent specific acts in CIL and treaty law. For instance, a duty to prevent terrorism was elucidated when the League of Nations stated that it is:

> the duty of every state neither to encourage nor tolerate on its own territory any terrorist activity with a political purpose… [and that] every State must do all in its power to prevent and repress acts of this nature and must for this purpose lend its assistance to governments which request it…[4]

---

delinquency, which he neither forbids nor punishes, when he is both able and bound to do so, he becomes an accessory to the guilt thereof…besides the knowledge of a deed, to constitute a participation in the guilt, the person so knowing it, must possess the power to prevent it. And this is what is meant by the legal phrase, that the knowledge of a crime, when it is ordered to be punished, is taken in the sense of forbearance or connivance, and it is supposed that the person, who ought to have prevented it, did not do so. In this place knowledge implies a concurrence of will, and connivance a concurrence of design.") *See also*, Grotius, *id*., ¶ 3

4 12 League of Nations Off. J. 1759 (1934). *As quoted by*, Justin S.C. Mellor, *Missing the Boat: The Legal and Practical Problems of the Prevention of Maritime Terrorism*, 18 Am. Univ. Int'l L. Rev. 341 (2002).

This duty to prevent terrorism has been codified by multiple conventions, including the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation;[5] Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents;[6] and the Convention to Prevent and Punish the Acts of Terrorism Taking Form of Crimes Against Persons and Related Extortion That Are of International Significance;[7] just to name a few.[8] This international focus on the duty to prevent terrorism impacts not only the generic duty to prevent but also has special implications for the duty to prevent malicious cyber-attacks. This study argues that this generic duty to prevent international terrorism may control, by analogy, malicious cyber-attacks in general, or specifically engage states to prevent analogous attacks in cyberspace.

In addition to the treaties discussed, the UN Security Council has addressed the issue of the duty to prevent in regards to terrorism. The Security Council in Resolution 1373[9] held that "2… States shall… (b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information."[10] The Security Council recognized in the wake of the 9/11 attacks that states had a duty to prevent terrorist acts and the duty to exchange information[11] with other states in order to prevent terrorist acts. This duty to prevent terrorist attacks reiterates the duty to prevent harm to

5 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 974 U.N.T.S. 14118 (23 Sept. 1971).

6 Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, U.N.G.A. Res. 3166, 1035 U.N.T.S. 15410 (14 Dec. 1973).

7 Convention to Prevent and Punish the Acts of Terrorism Taking Form of Crimes Against Persons and Related Extortion That Are of International Significance, OAS Treaty Series, no. 37, 27 U.S.T.S. 3949 (2 Feb. 1971)

8 *See e.g.*, Daniel O'Donnell, *International Treaties Against Terrorism and The Use of Terrorism During Armed Conflict and by Armed Forces*, 88 Int'l Rev. Red Cross 853 (Dec. 2006). (Discussing the multiple treaties invoked against terrorism "and the obligations of [S]tates with regard to them.")

9 S.C. Res. 1373, S/RES/1373 (2001).

10 *Id.* at (2)(b).

11 S.C. Res. 1373 at (3)(b). (States shall "(e)xchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts…")

another state originating from a state's territory. Res. 1373 bases this duty to prevent terrorism in part upon the ideas posited in the UN General Assembly's Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations,[12] finding that terrorism is violative of the principles put forth in both UNGA Res. 2625 and the UN Charter. That is, terrorism "constitutes a threat to international peace and security…"[13] and "the need to combat by all means, in accordance with the charter of the United Nations, threats to international peace and security caused by terrorist acts…"[14] The Security Council in Res. 1373 noted "the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials…"[15] Given the fact that malicious cyber-attacks have emerged as a means to fund terrorism[16] and engage in the very activities that Res. 1373 is concerned about, Res. 1373 and the duty

12 Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, U.N.G.A. Res. 2624, A/RES/25/2625 (24 Jan. 1970).

13 S.C. Res. 1373, preamble, S/RES/1373 (2001).

14 *Id.*

15 S.C. Res. 1373 (3)(g)(4).

16 *See, e.g.*, Hendi Yogi Prabowo, *Terrorist Financing, Cybercrime and the Underground Economy*, Jakarta Post (July 9, 2012), http://www.thejakartapost.com/news/2012/07/09/terrorist-financing-cybercrime-and-underground-econ omy.html#sthash.fcIafqos.dpuf. (Discussing church bombings in Indonesia in 2011. "The National Police's Densus 88 counterterrorism unit arrested five suspects in the case of the Surakarta church bombing. Among them was an information technology (IT) expert, Rizki Gunawan, who used his skills to illegally gather funds from the Internet. According to the police, Rizki was able to hack into, among others, a multi-level marketing (MLM) company website and reaped around Rp. 5.9 billion (US$625,400). The police believed that part of the funds were used to support the church bombing attack in 2011.") United Nations Office on Drugs and Crime & United Nations Counter-Terrorism Implementation Task Force, *The Use of the Internet for Terrorist Purposes* 7, ¶ 15 (2012). ("Online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud. An example of the use of illicit gains to finance acts of terrorism can be seen in the United Kingdom case against Younis Tsouli...Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment accounts, which were used to route the funds through several countries before they reached their intended destination. The laundered money was used both to fund the registration by Tsouli of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity.")(Internal citations omitted). OECD Financial Action Task Force, *Financing Terrorism* (29 Feb. 2008). (Discussing wire fraud and cheque fraud as methods of traditional terrorist financing. Activities that are now more commonly conducted via criminal cyber-attacks.)

to prevent would attach to such activities as malicious cyber-attacks, specifically regarding those attacks associated with transnational terrorism, and by analogy, to malicious cyber-attacks in general. This application, however, is only a small part of what is argued to be a larger norm.

Terrorism is not the only codified duty to prevent. The duty to prevent exists in relation to genocide. There is a specific duty to prevent genocide contained within the Genocide Convention, Art. 1 in which "[t]he Contracting Parties confirm that genocide, whether committed in peace or in a time of war, is a crime under international law which they undertake to prevent and punish."[17] In addition, a specific duty to prevent obligation may be found in such instruments as the Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children and multiple others.[18] As a result of these and other codified duties to prevent, the argument can be made that a general duty to prevent harm (duty to prevent) exists in international law. This disparate duty to prevent obligation has created a general duty to prevent harm in CIL. This specific duty to prevent arguably creates a more general duty to prevent which controls malicious cyber-attacks and the state's duty to prevent.

As for CIL, one of the earliest modern cases recognized by the ILC regarding the specific duty to prevent harm is the *Tellini* case,[19] where international jurists in response to specific questions[20] posed to them by the League of Nations, stated:

> [t]he responsibility of a State is only involved by the commission in its territory of a political crime against the persons of foreigners if the State has neglected to take *all reasonable measures* for the prevention of the crime and the pursuit, arrest and bringing to justice of the criminal.[21]

---

17 Convention on the Prevention and Punishment of the Crime of Genocide, 78 U.N.T.S. 277 (12 Jan. 1951).

18 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, U.N.G.A. Res. A/RES/55/25 (2001).

19 5 League of Nations Off. J. 525 (1924). (The matter arouse due to the assassination of Enrico Tellini and others conducting a survey in Greece concerning matters between Greece and Albania.) *See also*, International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* ch. 2. cmt. 3, U.N.G.A. A/56/10 (2001).

20 *Id.* (The League of Nations posed a series of questions to international jurists of which, question V. asked "[i]n what circumstances and to what extent is the responsibility of a State involved by the commission of a political crime in its territory?")

This enunciates that states may have a duty to prevent certain acts. While the *Tellini* case enunciates a narrow rule (protecting foreigners from political crimes such as assassination) specific to the questions asked, the duty to prevent exists as a general proposition as to prevent harm. Support of such a proposition may be found in other international cases. As discussed *supra*, for instance, *Trail Smelter* held that states have a specific duty to prevent transboundary harm.[22] In *Corfu Channel*, the ICJ refers to such a duty obliquely, discussing that Albania did nothing to prevent mines in the channel from harming British warships; the ICJ referred to such actions as "a grave omission"[23] of Albania's international responsibility.[24] The ICJ implied in *Corfu Channel* that Albania had a duty to prevent harm to the transitioning warships. The duty to prevent harm is addressed in *Iran Hostage*[25] and *Bosnia Genocide*[26], but with respect to specific treaty applications.

In addition to the specific and general duty to prevent discussed *supra*, the ILA Study Group on Due Diligence gives the example of the specific duty for states to prevent their territory from being utilized in crimes that injure other states. The ILA Study Group on Due Diligence references the *S.S. Lotus Case*, where Justice Moore discussed the principle put forth in *United States v. Arjona*,[27] in which the United States Supreme Court held that "[i]t is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people,"[28]thus demonstrating

---

21 *Id. (*Emphasis added).

22 Rebecca M. Bratspies and Russell A. Miller, *Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration* (2006).

23 Corfu Channel Case, Judgment, 1949 I.C.J. Rep. 4, 23 (9 Apr.). ("In fact, nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania.")

24 *Id.*

25 United States Diplomatic and Consular Staff in Tehran, Judgment, 1980 I.C.J. Rep. 3 (24 May).

26 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 2007 I.C.J. Rep. 43 (26 Feb.).

27 *United States v. Arjona*, 120 U.S. 479, 484 (1887). (The Court explained the rationale for this, holding that "[t]his rule was established for the protection of nations in their intercourse with each other…" *id*. at 485.)

that a specific duty to prevent crime against another state existed in the 19th century and which is still, arguably, applicable to issues present today. The specific duty to prevent criminal acts in addition to the general duty to prevent is applicable to the issue of malicious cyber-attacks.

If this statement by the United States Supreme Court, adopted by reference by the Permanent Court of International Justice (PCIJ) and the ILA, is applied to malicious cyber-attacks, it may be argued that a duty to prevent criminal acts, including those that occur in cyberspace, exists within CIL. The *Arjona* prohibition, while specifically addressing counterfeiting, is applicable to all transnational crimes. As cyberspace is arguably the largest vector for transnational crime today, the *Arjona* prohibition should and arguably does, apply as a matter of CIL. There is no logical reason for customary prohibitions to only apply to kinetic crimes and not digital ones. A criminal act is a criminal act irrespective of the medium used to conduct the act. Too often commentators treat digital space as a separate domain where customary rules do not apply. This study militates against this idea as CIL should apply either directly or through analogy to all mediums. If a state initiates a criminal act in cyberspace, then the state would bear responsibility if the act constitutes an internationally wrongful act. Therefore, under the instant theory, a state would be responsible for failing to prevent a criminal act in cyberspace if the act constituted an internationally wrongful act and the state had or should have had a knowledge of the act and failed to prevent the act.

The duty to prevent discussed *supra* is supported by the *Tallinn Manual* in Rule 5, where the *Manual* puts forth that "[a] state shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive control to be used for acts that adversely and unlawfully affect other states."[29] The *Tallinn Manual* applies this rule to states "irrespective of the attributability of the act,"[30] potentially implicating a state for the conduct of a non-state actor via indirect responsibility. The *Tallinn Manual* does not limit the scope of this

28 International Law Association, *ILA Study Group on Due Diligence in International Law First Report* 2 (07 Mar 2014). *Quoting*, *S.S. Lotus Case*, 1927 P.C.I.J., (ser. A.) No. 10, (7 Sep.)

29 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, R. 5 (Michael N. Schmitt ed. 2013).

30 *Id*. R.5, cmt. 1.

rule to either use of force or armed attack, despite the focus of the *Manual*;[31] instead, the *Tallinn Manual* holds that:

> this Rule covers *all acts* that are unlawful and that have detrimental effects on another State…The term 'unlawful' is used in this Rule to denote an activity that is contrary to the legal rights of the affected State. The international Group of Experts deliberately chose not to limit the prohibition [contained in Rule 5] to narrower concepts…in order to emphasize that the prohibition extends to all cyber activities from one State's territory that affect the rights of other States and have detrimental effects on another State's territory…[32]

The International Group of Experts in the *Tallinn Manual*, however, could not agree as to whether this prohibition engages a duty to prevent on behalf of the state.[33] The international experts, based upon comment 7 to Rule 5, believed that it would be too difficult to mount "comprehensive and effective defenses against all possible threats."[34] It is unknown to the author of this current study, why the international group of experts didn't simply make the duty to prevent conditioned upon the state's ability to prevent. This study would argue that the duty to prevent should be premised upon the technical ability of the state combined with the state's demonstrated willingness to prevent. Simply put, the greater the state's technical ability and/or the greater control a state has over its cyber infrastructure, the greater likelihood a state would be held accountable via the duty to prevent; less the state's actions to prevent, for malicious cyber-attacks originating from within its sovereign territory. This study would argue that taking the prohibition contained in Rule 5 in consideration of existing CIL militates against the idea that that Rule 5 does not engage the state regarding the duty to prevent malicious cyber-attacks.

This study, therefore, would add the additional element of the duty to prevent, as discussed *supra*, regarding the technical ability of the state to detect and prevent a malicious cyber-attack. In addition, the ability to prevent encompasses non-digital acts by the state, e.g., passing laws that prohibit malicious cyber-attacks. This study will briefly discuss the ability

---

31 *Id*. R.5, cmt 5.

32 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, R. 5, cmt. 5 (Michael N. Schmitt ed. 2013). (Emphasis ours).

33 *Id*. R. 5, cmt. 7.

34 *Id.*

of states to prevent malicious cyber-attacks in the next section. This study will then explore alternative legal sources that support the theory on the duty to prevent. After which, this study will address the theories of due diligence, omissions on behalf of a state, and indirect responsibility before concluding this chapter.

6.1.1. The Ability to Prevent Malicious Cyber-Attacks

This study argues that given the theory of due diligence and the duty to prevent, a state has the duty to prevent malicious cyber-attacks. However, this study also argues that the duty on behalf of states to prevent malicious cyber-attacks is not an absolute duty.[35] The prevention of malicious cyber-attacks, at the very least, requires a state to have the ability to monitor outbound transnational cyber traffic and the resources, both human and monetary, to support such activities. In addition, to their technical ability, states need to comply with emerging norms regarding the duty to prevent, by enabling laws that criminalize malicious cyber-attacks; enabling domestic legislation to support the sharing of attack information and cooperating with the international community to prosecute those who violate this prohibition.[36]

The technical ability of a state is impacted by considerations of the state's wealth and technical knowledge. A great disparity exists in the international community in both wealth and technical ability; each state must be held accountable under the duty to prevent based on the individual state's ability to prevent. This idea would hold wealthier, more technically able states to a higher level of responsibility regarding the duty to prevent, and less capable states to a lower standard. But, to prevent a state from becoming a cyber sanctuary,[37] all

35 *See*, Micheal N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 Yale L. J. F. 68, 74 (2015). ("[I]f taking measures to counteract harmful cyber activities directed abroad is technically impractical, the [S]tate that fails to do so is not in breach of its due diligence obligation; the diligence that is due under the legal standard cannot exceed a State's capabilities.")

36 *See e.g.*, Convention on Cybercrime, E.T.S. 185 Ch. 2 *et seq*. (23 Nov. 2001). (Detailing the steps required by signatories to the convention regarding establishing criminal prohibitions for computer crimes.)

37 *See*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. Nat. Sec. L. & Pol. 87, 94-98 (2010). (Arguing that to identify a sanctuary State "a victim state must at a minimum examine a sanctuary state's criminal law dealing with cyber-attacks, its enforcement of the law, and its

states must be held to a minimum standard regarding the duty to prevent. States' resource availability and technical knowledge regarding the prevention of malicious cyber-attacks is only one element in the overall paradigm.

There are multiple factors that may impact a state's ability to prevent malicious cyber-attacks, including the state's domestic cyberinfrastructure, domestic law enforcement capabilities, and technical ability to identify outgoing malicious cyber-attacks. The ability to prevent malicious cyber-attacks must also be balanced against the individual's protected freedoms.[38]

A state may demonstrate, at a minimum, its willingness to prevent malicious cyber-attacks by taking those steps necessary to secure its digital infrastructure to the best of the state's abilities. In addition, a state demonstrates a willingness to prevent malicious cyber-attacks, when, as Graham[39] elucidated, a state:

1. "[E]nact[s] stringent criminal laws against the commission of international cyber-attacks from within national boundaries."[40]
2. "[C]onduct[s] meaningful, detailed investigations into cyber-attacks."[41]
3. "[P]rosecute[s] those who have engaged in […malicious cyber] attacks."[42]
4. "[C]ooperate[s] with victim [S]tates' own investigations and prosecutions of those responsible for [malicious cyber] attacks."[43]

---

demonstrated record of cooperating with victim states' own investigations and prosecutions of cyber offenders who have acted across borders.")

38 *See e.g.*, Universal Declaration of Human Rights arts. 12, 19-21, 27. G.A. Res. 217A (10 Dec. 1948). *See also*, Combating the Criminal Misuse of Information Technologies, G.A. Res. 55/63 ¶ 1 (A-J) (22 Jan. 2001). (Calling for the cooperation of law enforcement entities in the sharing of information on illegal use of information technology and noting that individual liberties be respected.)

39 *See e.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. Nat. Sec. L. & Pol. 87, 93-94 (2010). (Discussing these requirements in regards to cyber-attacks that equate to the illegal use of force.)

40 *Id.*

41 *Id.*

42 *Id.*

These ideas presented by Graham are supported by the text of the *Convention on Cybercrime*, which codifies these general themes for signatory states. It is a state's willingness to do these things which signify its desire and ability to prevent, in addition to its technical abilities.

A state's technical ability to prevent malicious cyber-attacks is a separate element to those discussed previously. Relatively inexpensive technology exists for states to monitor outbound Internet traffic for the malware responsible for malicious cyber-attacks[44] originating within a state's domestic cyber infrastructure. It is argued that states who do not utilize such technology (either software or hardware), or states who do not have their domestic Internet providers utilize such technology, may violate the duty to prevent by omission. That is, if a state fails to take the adequate steps to protect its domestic cyber infrastructure from being utilized to harm another state, that state has violated the norm of the duty to prevent. This idea is premised on the fact that if a state knows that its territory is being utilized to harm another state and takes no action to prevent said act, then the state

---

43 *Id*.

44 *See*, Brian Wippich, *Detecting and Preventing Unauthorized Outbound Traffic* 9-11, SANS Inst. (2007). (Discussing the ability to inexpensively monitor outbound traffic by using packet filtering devices and firewalls. Wippich discussed these techniques in reference to corporations and not states.) *See also*, Huijun Xiong, Prateek Malhotra, Deian Stefan, Chehai Wu, and Danfeng Yao, *User-Assisted Host-Based Detection of Outbound Malware Traffic*, Information and Communications Security 293-307 (2009). (Discussing "host-based security tool that identifies suspicious outbound network connections through analyzing the user's surfing activities…" in order to determine whether a machine is part of a bot (DDoS) network.) Michael K. Reiter and Ting-Feng Yen, *Traffic Aggregation for Malware Detection*, Detection of Intrusions and Malware, and Vulnerability Assessment 207-227 (2008). (Discussing the use of software to analyze computer systems' communications to determine whether the system is infected with malware and communicating with a botnet.)

is responsible for that action due to its own failure to act.[45] A state must take all reasonable efforts to prevent a malicious cyber-attack or bear responsibility for the same.[46]

As the proper utilization of such software and hardware requires expertise on behalf of the state and the ability to employ experts, the technical ability to prevent is dependent upon the state's ability to fund such activity. A state must act to the best of its abilities to comply with this idea.

Additionally, states that detect malware within their domestic cyberinfrastructure have the duty to trace the data packets of the outbound cyber-attack and attempt to prevent further attacks. States that have traced malicious cyber-attacks to specific IP addresses should make every attempt to discern who is responsible for initiating the attacks and do all within the domestic power of the state to prosecute any individual responsible for initiating malicious cyber-attacks. Additionally, states should share this data with other states to make them aware of the attack and the threat originating from the attack and offer mutual cooperation in order to prevent further spreading via the Internet of the malicious software.[47] This duty has already been placed upon those signatories of the *Convention on Cybercrime*,[48] and as such, this duty may potentially be seen as an emerging norm, particularly in light of actions in regards to multiple resolutions regarding information technology and cyber-attacks by the UNGA.[49]

---

45 *See*, International Law Commission, *Draft Articles of Responsibility of States for International Wrongful Acts*, Art. 2, cmt. 4, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001). ("For example, in the *Corfu Channel* case, ICJ held that it was a sufficient basis for Albanian responsibility that it knew, or must have known, of the presence of the mines in its territorial waters and did nothing to warn third States of their presence. In the United States Diplomatic and Consular Staff in Tehran case, the Court concluded that the responsibility of the Islamic Republic of Iran was entailed by the 'inaction' of its authorities which 'failed to take appropriate steps', in circumstances where such steps were evidently called for. In other cases, it may be the combination of an action and an omission which is the basis for responsibility.")

46 *See e.g.*, The Tellini Case, 5 League of Nations Off. J. 525 (1924).

47 *See generally, Convention on Cybercrime* arts. 1-11, ETS No. 185 (23 Nov. 2001). *Cf.* S.C. Res. 1373, S/RES/1373 (2001).

48 *Id.* arts. 20-21.

49 Combating the Criminal Misuse of Information Technologies, U.N.G.A. Res. 55/63 (22 Jan. 2001). U.N.G.A. Res. 56/121(19 Dec. 2001). U.N.G.A. Res. 7/239 (20 Dec. 2002). U.N.G.A. Res. 58/199 (23 Dec. 2003). U.N.G.A. Res. 64/211 (21 Dec. 2009).

States need not act alone in this endeavor; one of the simplest means of combating malicious cyber-attacks is the sharing of information. As discussed *supra* in Chapter Three, the computer code that drives malicious cyber-attacks is often recycled and improved code from a previous cyber-attack that is already known to computer science.[50] Numerous commercial and private organizations exist that document and track malware and its progeny, and this data is open and available, e.g., open source threat intelligence information.[51] As states detect new forms of attack, such data should be openly shared, as this data is needed for states to effectively combat new and emerging malicious cyber-attack.

To summarize, as a matter of policy, the more cyber-capable the state, the greater the duty to prevent cyber-attacks. Developing states that do not have either the financial or technical ability to monitor their cyber infrastructure are bound only to the extent that they are capable of preventing. While this idea introduces a level of subjective interpretation as to the ability of individual states, it may simply act as a matter of rebuttable presumption for a state. That is, a state that is accused of allowing its cyber infrastructure to be utilized for cyber-attacks need simply show that it did not have the ability to stop the attacks due to technical, financial, or awareness issues. This may not absolve the state of all its duty to prevent, but it may minimize the state's indirect responsibility for the malicious cyber-attack. States may demonstrate a willingness to prevent its domestic cyber infrastructure from being utilized for malicious cyber-attacks by promulgating legal means to criminalize such acts, cooperating with other states in the prosecution of such attacks, and complying with emerging norms regarding the handling of malicious cyber-attacks.

---

50 Abby Dinham, *Hackers 'Recycling Code' to Spread Worms*, ZDNet (June 1, 2004), http://www.zdnet.com/article/hackers-recycling-code-to-spread-worms/. *See also*, G.A. Res. 55/63, *id*.

51 Javier Inclan, *Advanced Malware Detection Through Threat Intelligence*, HP (2014).

6.2. Due Diligence and Malicious Cyber-Attacks

This study now turns to the issue of due diligence and the duty it places upon states regarding malicious cyber-attacks. While the theories previously discussed *supra* arguably impose a due diligence obligation upon states standing alone; the arguments noted *supra*, however, may be criticized due to their roots in less populated realms of international law, e.g., the specificity of customary international environmental law. However, as "a general principle, the presumption is that the principle applies unless [S]tate practice or *opinio juris* excludes it."[52] As no CIL has been identified by this study that would preclude such application of the discussed theories, the presumption is that the theories previously discussed apply, arguably creating a due diligence standard standing alone. However, as the due diligence principle in international law, in general, is unsettled, this study will discuss the issue of due diligence in more detail to flesh out its impact upon the duty to prevent malicious cyber-attacks.

As the exact basis for due diligence has not been delineated, an argument may be made that the due diligence obligation exists, per se, concurrent to, and in addition to, that of the duty to prevent. Yet, as Schmitt argued, it may also be based upon the theory of sovereignty. Schmitt put forth that "[d]ue diligence derives from the principle of sovereignty. To the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding legal obligations…"[53]

An argument may also be made that due diligence as a legal operation may stand as an independent norm in that the same legal principles that created the duty to prevent, e.g., *Trail Smelter* and *Corfu Channel*, arguably stand for duty on states to be diligent regarding the use of their territory. There is no clear theory regarding the application of due diligence in international law.[54] The ILA, when discussing the development of the due diligence theory post-*Corfu Channel* stated: "[n]ormative and institutional fragmentation has

[52] Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 Yale L. J. F. 68, 73 (2015).

[53] Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 Yale L. J. F. 68 (2015).

[54] International Law Association, *ILA Study Group on Due Diligence in International Law First Report* 4 (07 Mar 2014).

revealed significant divergence in the application of due diligence, both in terms of the scope of its application, and seemingly, its content."[55] This issue of the scope and content of the due diligence requirement for states regarding malicious cyber-attacks will be discussed briefly *infra*, in order to discern how the principles apply to the instant question.

This study will briefly analyze the content of the principle before addressing the scope, as it is necessary to understand and define the content of a principle prior to applying it. One issue in defining what due diligence is the idea that the due diligence principle changes in concert to the obligation discussed.[56] As a baseline, Koivurova stated that:

> [h]istorically, due diligence had its main impact on the responsibility of States for private actors, which pertained to the preventive measures expected of a State in its sphere of exclusive control when international law was breached by private persons, not by the State as a legal entity.[57]

The ILA offers several examples of what due diligence may be, but does not, per se, define due diligence, instead stating that such considerations, along with others, will be addressed in the Second Report.[58] However, the ILA acknowledges the theory that a common standard for due diligence may exist and by extension a common definition; the ILA just does not elucidate what it is.[59] The ILA does indicate "that the content of due diligence is made by reference to international, rather than domestic standards."[60] The ILA also cites G.A. Res. 2625, the Declaration of Principles of International Law Concerning Friendly Relations, where the G.A. stated that states have an obligation to refrain from allowing conduct within their domestic territory that may harm another state,[61] thus arguably signaling agreement that as a unified theory, the due diligence principle may be founded upon the theory of the duty to do no harm.

---

[55] *Id.*

[56] Timo Koivurova, *Due Diligence*, Max Planck Encyclopedia of Law ¶¶ 1-2 (Feb. 2010).

[57] Timo Koivurova, *Due Diligence*, Max Planck Encyclopedia of Law (Feb. 2010).

[58] International Law Association, *ILA Study Group on Due Diligence in International Law First Report* 4 (07 Mar 2014).

[59] *Id.*

[60] *Id.*

[61] *Id.*

At a base level, the ILA holds that the due diligence principle is one of conduct. That states have an obligation to prevent certain conduct.[62] While the source and scope of these obligations are subject to much debate, at its base, the prohibited conduct evolves around the idea that states are obligated to prevent harm from impacting other states. Each section discussed by the ILA in one manner or another describes the state's obligation to prevent a form of harm or prevent a violation of international law which may result in harm, thus confirming the obligation as "a State must take measures to ensure their territories are not used to the detriment of other States."[63]

This obligation on behalf of states is not only for the state's own conduct but for all conduct originating from within its sovereign territory, thus potentially implicating the state for the acts of non-state actors. As Hessbruegge posited, "the state may incur responsibility if it fails to exercise *due diligence* in preventing or reacting to such acts or omissions [of non-state actors.]"[64] However, as Schmitt articulated, the state does not have an absolute duty in regards to malicious cyber-attacks (what Schmitt calls "harmful cyber activity").[65] Schmitt argued that:

> First, if taking measures to counteract harmful cyber activities directed abroad is technically impractical, the state that fails to do so is not in breach of its due diligence obligation; the diligence that is due under the legal standard cannot exceed the state's capabilities.[66]
>
> Second, if the burden on the territorial state in taking remedial actions is so onerous as to be unreasonable under the circumstances, inaction will not constitute a breach. In gauging reasonableness, "[t]he nature, scale, and scope of the (potential) harm to both States must be assessed."[67]

---

62 International Law Association, *ILA Study Group on Due Diligence in International Law First Report* 17 (07 Mar 2014).

63 Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 Yale L. J. F. 68, 69 (2015).

64 Jan Arno Hessbruegge, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. Int'l. L. & Pol. 265, 268 (2004).

65 *Id*. n.63 at 74.

66 *Id*.

67 *Id.*

> Third, the due diligence obligation only indisputably applies to ongoing cyber activities that are generating serious adverse effects in another country, although they need not be physically destructive or injurious.[68]

Thus, the due diligence obligation is not an absolute obligation on behalf of the state.

However, it may be argued that as long as malicious cyber-attacks inflict harm upon another state and the harm-inducing state meets the elements posited by Schmitt, that is, they have the capabilities to prevent a malicious cyber-attack; the burden of prevention is not onerous; and the malicious cyber-attack is ongoing, a state has a due diligence obligation. The obligation of due diligence in regards to malicious cyber-attacks is simply premised upon the resultant harm from the malicious cyber-attacks.

As to the scope of the obligation, there is debate whether the due diligence obligation exists standing alone within the CIL or whether the due diligence theory is only implicated through the primary norm in question. The ARS struggled in identifying the role of due diligence between the first reading and the second reading, with the ARS finally placing due diligence in "consideration of a primary rule,"[69] removing it from the purview of the ARS. The ARS only discusses the issue of due diligence in the commentary to the rules posited by it. The ARS states:

> [t]he articles lay down no general rule in that regard. The same is true of other standards, whether they involve some degree of fault, culpability, negligence or want of due diligence. Such standards vary from one context to another for reasons which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation.[70]

Economides posited, "[a] state commits itself to act in a reasonably cautious and diligent manner, by taking all the measures of precaution necessary to avoid a particular harmful event, these are, given the expression used, the obligations of due diligence."[71] A due

---

68 *Id.* (Internal citations omitted.)

69 *Id.* ¶ 5.

70 International Law Commission, *Draft Articles of Responsibility of States for International Wrongful Acts*, Art. 2, cmt. 3, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

diligence failure to take the necessary precautions to avoid allowing harm to another state is an omission of an international responsibility on behalf of the state. Hence, a state will be responsible for the resulting harm to the injured state. This is demonstrated by the ICJ's holding in the *Iran Hostage* case[72] where Iran failed to "take appropriate steps…to protect"[73] the United States consulate; this failure to take action by Iran was an omission of its due diligence owed to the United States under the treaty provisions of the Vienna Convention on Consular Relations, as it was part of Iran's ordinary duty owed to the United States to ensure the safety and security of the United States consulate. The due diligence obligation as argued herein and as demonstrated by *Corfu Channel* and the *Iran Hostage* case does not stand for the proposition that States must prevent all harm, but they must take reasonable care to prevent foreseeable harm.

Applying this discussion to the matter of malicious cyber-attacks, it is apparent that the due diligence obligation impacts the state's duty to prevent malicious cyber-attacks. The due diligence obligation would hold that a state must take care to the best of its abilities to prevent malicious cyber-attacks, particularly those attacks that it has knowledge of originating within its sovereign territory. This obligation is subject to the issues discussed *supra*, as put forth by Schmitt. While it is not possible to conclusively say where the due diligence obligation originates from, or what its true basis is in international law, it is arguable that such a theory exists and impacts malicious cyber-attacks either directly or through analogy. As with the duty to prevent, the due diligence obligation may implicate the state for the acts of non-state actors.

---

71 Constantin P. Economides, *Content of the Obligation: Obligations of Means and Obligations of Results, in,* The Law of International Responsibility 378 (James Crawford, Alain Pellet, and Simon Olledon eds. 2010).

72 United States Diplomatic and Consular Staff in Tehran, 1980 I.C.J. Rep. 3 (24 May).

73 *Id.* at 31. *See also*, Anna-Karin Lindblom, *The Responsibility of Other Entities: Non-Governmental Organizations, in,* The Law of International Responsibility 358 (James Crawford, Alain Pellet, and Simon Olledon eds. 2010).

6.3. Indirect Responsibility by States

The theories discussed in this chapter implicate the state not necessarily for the state's own actions, but for the actions of others. Both the duty to prevent and the due diligence obligations engage the state to ensure that the state's sovereign territory is not utilized to the detriment of other states. As these norms implicate not only actions on behalf of the state but also non-state actors, a state may, therefore, be held responsible in international law for the acts of others. This responsibility on behalf of the state for the acts of non-state actors implicates the state for the purposes of state responsibility indirectly. That is, a state which violates the discussed norms herein will be responsible for those violations just as any other internationally wrongful act on behalf of the state. However, the violations, per se, were not the act of the state, but the failure to meet the duty to prevent or the due diligence obligation.

This application of indirect responsibility may seem at odds with the ARS as states are held responsible for the actions of non-state actors irrespective of attribution of conduct. However, while the state is being held indirectly responsible for the conduct of a non-state actor, the state is also being held responsible for the violation, on behalf of the state, for failing to either prevent the harm or for the failure to adhere to the due diligence obligation. Thus, a state may be responsible for its own failures and for the conduct of non-state actors in limited circumstances as discussed herein.

The duty to prevent and the due diligence obligation may hold states responsible for the acts of non-state actors if the state fails to fulfill its international obligations by either failing to prevent a malicious cyber-attack that rises to the level of an internationally wrongful act or for the state's failure to adhere to the state's due diligence obligation.

The duty to prevent and due diligence obligation are closely intertwined. This chapter sets them apart as two distinct theories within international law. However, as there is significant overlap between the two theories in practice, it may be impossible to discern where one norm ends, and the other begins. This is particularly relevant in regards to due diligence obligation as the source; the boundaries and application of the due diligence obligation are difficult to define. The due diligence obligation is recognized in international law

irrespective of the scholarly debate surrounding it and holds states accountable for their inaction regarding malicious cyber-attacks.

The duty to prevent, like the due diligence obligation, may be premised upon multiple norms in international law. These norms dictate that a state has a duty to prevent their domestic territory from being used to the detriment of other states. While the norms discussed do not, per se, encompass malicious cyber-attacks, they do control through analogy and as such, a duty to prevent malicious cyber-attacks arguably exists in international law.

Chapter Seven: The Impact of the 9/11 Attacks on the Customary International Law of State Responsibility

7. Introduction

This study now turns to the question of whether the actions of the United States and its allies after the 9/11 terror attacks established a new rule of attribution for the acts of non-state actors to a host state. This study will argue that the invasion of Afghanistan by the United States and its allies in response to the 9/11 attacks, which were never attributed under international law to the Taliban, the de facto government of Afghanistan, may have created a new rule of attribution for the acts of non-state actors to its host state. This new rule of attribution would be a means for states to attribute malicious cyber-attacks initiated by non-state actors or are otherwise unattributable to the host state.

This discussion concerning a potential emerging rule is important as the final reading of the ARS was sent to the UNGA less than three months after the terror attacks on the United States on September 11, 2001, and the subsequent invasion of Afghanistan by the United States and its allies. Thus, the impact of the 9/11 attacks and the response by the United States et al., was never analyzed by the ILC with respect to the ARS and as a result, such a theory as proposed by this study was never contemplated by the ARS.

7.1. The 9/11 Attacks and Their Impact on the Customary International Law of State Responsibility

To analyze whether CIL was formed in response to the 9/11 terror attacks, this study will engage in an in-depth analysis of the immediate response to the 9/11 attacks by the United States, NATO, and the P5 Security Council members.

This study addresses the 9/11 attack and subsequent invasion as a sui generis event for the purposes of determining if new CIL for the attribution of internationally wrongful conduct occurred.

7.1.1. The 9/11 Attacks and the Invasion of Afghanistan as a Sui Generis Event

It is an unfortunate reality that terror attacks occur. Terror attacks have occurred since at least the first century CE[1] and have continued into modern times. There is no single cause for terrorism, and terror groups have long been diverse in their cause and want. Terror groups may be stand-alone groups or state-sponsored or affiliated. In modern times, terror groups were, at least from an American perspective, a criminal matter dealt with by law enforcement and the judiciary.[2] That is not to say that military force had not been used to deter or punish states for assisting or training terror groups, but such actions were extremely rare prior to 2001.[3]

The holding of Afghanistan responsible for the acts of Al-Qaeda and the subsequent invasion and toppling of the Taliban government was and is still unique in modern international law. In modern history, no such action had transpired before. While military intervention into conflict zones and peacekeeping operations have been conducted in other instances, no military intervention in modern times had been premised on removing a government by assigning responsibility to that government for the acts of a non-state actor. Fortunately, terror attacks on the scale of the 9/11 attacks had not happened prior to 9/11 nor had attacks of such magnitude happened since. It is the magnitude of the attacks and the international response thereto and the subsequent altering of the existing state responsibility paradigm, if ever so slightly, that makes these attacks and international response sui generis, thus standing alone in international law. This sui generis event is such

---

1 Gerard Chaliand & Arnaud Blind, *Zealots and Assassins* 55-57, *in*, The History of Terrorism: From Antiquity to Al Qaeda (Gerard Chaliand ed., 2007).

2 *See e.g.*, 18 U.S.C. § 2332b (LII, 2016). *Cf.*, Andrew Majoran, *The Illusion of War: Is Terrorism a Criminal Act or an Act of War*, Mackenzie Inst. (July 31, 2014), http://mackenzieinstitute.com/illusion-war-terrorism-criminal-act-act-war/.

3 For example, United States President Ronald Reagan ordered the bombing of "terrorist facilities and military installations" located in Libya in 1986. Barbara Salazar Torreon, *Instances of Use of United States Armed Forces Abroad, 1789-2015*, 12, Cong. Res. Serv. (Oct. 15, 2015).

that new CIL arguably sprung from the post-9/11 international response and gave rise to the instant discussion.

7.1.2. The 9/11 Attacks and the International Response

On September 11, 2001, four commercial airliners were hijacked and utilized as weapons of mass destruction by the hijackers. At 0845 hours, the first airliner, American Airlines (AA) Flight 11, a Boeing 767 airliner, was flown into the north tower of the World Trade Center in New York City.[4] Eighteen minutes later, at 0903 hours, a second 767 airliner, AA Flight 77, was flown into the south tower of the World Trade Center.[5] At 0943 hours, a third airliner, a Boeing 757, United Airlines (UA) Flight 175 was flown into the Pentagon in Washington D.C.[6] Finally, at 1010 hours, a Boeing 757, UA Flight 93. was intentionally crashed into a field in Somerset, Pennsylvania.[7]

The attacks on 9/11 resulted in the loss of over 3,000 lives and resulted in billions of dollars of economic loss around the world. It was later shown that the nineteen hijackers[8] believed responsible for the attacks were linked to the terrorist organization, Al-Qaeda.[9] At the time of the attack, Al-Qaeda was believed to be operating and training in Afghanistan either with the explicit permission of the Taliban government or at a minimum acquiescence thereto. But Al-Qaeda was not an agent of, nor did the Taliban exhibit any control over Al-Qaeda to meet the effective control test to establish state responsibility for non-state actors.

---

4 *September 11: Chronology of Terror*, CNN.COM, http://archives.cnn.com/2001/US/09/11/chronology.attack/. See also, National Commission on Terrorist Attacks, *The 9/11 Commission Report* 1-14 (2004).

5 *Id.*

6 *Id*.

7 *Id*.

8 National Commission on Terrorist Attacks, *The 9/11 Commission Report* 2-5 (2004).

9 George W. Bush, *Address to the Joint Session of the 107th Congress*, Sept. 20, 2001, *in* Collected Speeches of George W. Bush 2001-2008 66 (2010). ("The evidence we have gathered all points to a collection of loosely affiliated terrorist organizations known as Al-Qaeda.") *See also*, National Commission on Terrorist Attacks Upon the United States (9/11 Commission), *The 9/11 Commission Report* 145-169, 215-278, (July 22, 2004).

7.1.3. The International Response

The international response to the 9/11 attacks was immediate, with an almost universal declaration of condemnation for the acts and support for the United States.[10] Various international bodies took positions in support of the United States immediately after the attacks and supported, directly, indirectly, or through acquiescence, the military response to the 9/11 attacks by the United States. By supporting the military response, which resulted in the invasion of Afghanistan and the removal of the Taliban government, the course of CIL on state responsibility was, in the opinion of this study, directly impacted. This study will analyze the actions of the major actors within the invasion of Afghanistan to support this argument.

7.1.3.1. The United Nations

On September 12, 2001, the United Nations Security Council issued Resolution 1368, in which Art. 3 "[c]all[ed] on all states to work together urgently to bring to justice the perpetrators, organizers, and sponsors of these terrorist attacks and stresses that those responsible for aiding, supporting or harboring the perpetrators, organizers, and sponsors of these acts will be held accountable…"[11] Shortly thereafter, on September 28, 2001, the Security Council issued Resolution 1373[12] in which the Security Council adopted the following:

- That "any act of international terrorism constitutes[s] a threat to international peace and security."[13]

---

10 *See*, Greg Trevalio and John Altenburg, *Terrorism, State Responsibility, and the Use of Military Force*, 4 Chi. J. Int'l L. 97, 108-109 (2003). (Discussing the support for the United States actions in Afghanistan post-9/11.)

11 S.C. Res.1368 ¶3, U.N. Doc. A/RES/1368 (Sept. 12, 2001). (Emphasis in original). *See also*, Ben Smith and Arabella Thorp, *The Legal Basis For The Invasion of Afghanistan* 2, House of Commons (UK), SN/IA/5340 (2010). ("[T]he Resolution [1368] clearly gives a general authorisation for action to bring the perpetrators to justice.")

12 S.C. Res. 1373, U.N. Doc. S/RES/1373 (28 Sept. 2001). *See also*, Smith and Thorp, *id.*

13 *Id.* S.C. Res. 1373

- "Reaffirm[ed] the inherent right of individual and collective self-defense as recognized by the Charter of the United Nations as reiterated in Resolution 1368."[14]
- "Call[ed] on States to work together urgently to prevent and suppress terrorist acts…"[15]
- "Reaffirm[ed] the principle…that every State has a duty to refrain from organizing, instigating, assisting or participating in terrorist acts in another State or acquiescing in organized activities within its territory directed toward the commission of such acts."[16]
- "Declar[ed] that acts, methods, and practices of terrorism are contrary to the purposes and principles of the United Nations."[17]

On November 12, 2001, the Security Council adopted Resolution 1377[18] in which the Security Council formally "adopt[ed] the…declaration on the global effort to combat terrorism."[19] The declaration adopted in Resolution 1377 closely echoed the ideas proposed in Resolutions 1368 and 1373. Resolution 1377 is more important for what it does not say, that is, it was the first Security Council resolution issued after the United States and its allies began an air assault and bombing campaign against Taliban forces.[20] Indeed, Resolution 1378[21] was issued two days after Resolution 1377, over a month after the initial air campaign against Taliban forces, and weeks after the United States and its allies had inserted ground troops into Afghanistan. It stated that the Security Council "[s]upport[s] international efforts to root out terrorism, in keeping with the Charter of the United Nations…"[22] and that the Security Council:

---

14 *Id*

15 *Id.*

16 *Id.*

17 *Id*. at ¶5

18 S.C. Res. 1377, U.N. Doc. S/RES/1377 (12 Nov. 2001).

19 *Id.*

20 The Guardian, *US Response: Attack on Afghanistan*, (n.d.), http://www.theguardian.com/flash/0,5860,567567,00.html.

21 S.C. Res. 1378, U.N. Doc. S/RES/1378 (Nov. 14, 2001).

> [c]ondemn[s] the Taliban for allowing Afghanistan to be used as a base for the export of terrorism by the Al-Qaida network and other terrorist groups and for providing safe haven to Usama Bin Laden, Al-Qaida and others associated with them, and in this context support[s] the efforts of the Afghan people to replace the Taliban regime…[23]

This last statement, in which the Security Council condemns the Taliban and seemingly attributes, albeit vicariously, partial responsibility for the 9/11 attacks on the Taliban in Afghanistan, is important. At no time were the 9/11 attacks attributable to the Taliban (the de facto government of Afghanistan) under existing CIL as expressed by the ARS. Indeed, under the ARS, the Taliban, as the de facto government of Afghanistan, could be responsible only for those acts that have been "attributed to the State at the international level [and those acts] of its organs of government, or of others who have acted under the direction, instigation, or control of those organs, i.e., as agents of the State…"[24]

This was not the first time the Security Council had brought the Taliban to task concerning Al-Qaeda. The Security Council had given the Taliban notice prior to the 9/11 attacks concerning the conduct of Al-Qaeda and for the support of terrorists within Afghanistan. In 1998, the Security Council twice voiced its concern over the harboring of terrorists in Afghanistan,[25] and "[d]emand[ed]…that the Taliban stop providing sanctuary and training for international terrorists and their organizations…"[26] In 1999, the Security Council, in Resolution 1267, reiterated the demand upon Afghanistan and the Taliban to stop allowing its territory as a safe harbor for terrorists and to stop allowing terrorists to train in Afghanistan. The Security Council went even further: for the first time, it specifically mentioned Usama bin Laden and Al-Qaeda when the Security Council "[d]eplor[ed] the fact that the Taliban continue[d] to provide safe haven to Usama bin Laden and to allow him and others associated with him to operate a network of terrorist training camps from

---

22 *Id.*

23 *Id*.

24 *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Ch. 2, cmt. 2, 38, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

25 S.C. Res. 1193, U.N. Doc. S/RES/1193 (28 Aug. 1998). S.C. Res. 1214, U.N. Doc. S/RES/1214 (8 Dec. 1998).

26 S.C. Res. 1214 ¶13.

Taliban-controlled territory and to use Afghanistan as a base from which to sponsor international terrorist operations…"[27] Indeed, in Resolution 1267, the Security Council went so far as to state that "the failure of the Taliban authorities to respond to the demands in paragraph 13 of Resolution 1214 (1998) constitutes a threat to international peace and security…"[28] The Security Council then:

> insist[ed] that the Afghan faction known as the Taliban, which also calls itself the Islamic Emirate of Afghanistan, comply promptly with its previous resolutions and in particular, cease the provision of sanctuary and training for international terrorists and their organizations, take appropriate effective measures to ensure that the territory under its control is not used for terrorist installations and camps, or for the preparation or organization of terrorist acts against other States or their citizens, and cooperate with efforts to bring indicted terrorists to justice; [and]
>
> demand[ed] that the Taliban turn over Usama bin Laden without further delay to appropriate authorities in a country where he has been indicted, or to appropriate authorities in a country where he will be returned to such a country, or to appropriate authorities in a country where he will be arrested and effectively brought to justice…[29]

The Security Council again addressed the actions of the Taliban in 2000 in Resolution 1333, demanding again that the Taliban stop allowing its territory from being used by terrorists and comply with Security Council Resolution 1267,[30] turn over Usama bin Laden to a country where he had previously been indicted for terrorist acts, and demanded that all terrorist training camps be closed.[31] In addition, the Security Council recognized "that the failure of the Taliban authorities to respond to the demands in paragraph 13 of resolution 1214 (1998) and in paragraph 2 of resolution 1267 (1999) constitutes a threat to international peace and security…"[32]

---

27 S.C. Res. 1267, U.N. Doc. S/RES/1267 (15 Oct. 1999).

28 *Id.*

29 *Id.* ¶1-2.

30 S.C. Res. 1333, U.N. Doc. S/RES/1333 ¶1 (19 Dec. 2000).

31 *Id.* ¶1-3.

32 S.C. Res. 1333.

The impact of this prior notice on behalf of the Security Council of the actions of the Taliban in harboring Al-Qaeda and Usama bin Laden adds an interesting idea of a notice requirement to the idea of state responsibility as posited herein. This idea will be addressed *infra* in the analysis section.

7.1.3.2. North Atlantic Treaty Organization (NATO)

The NATO response was immediate. Within hours of the attacks, NATO released a statement in which all eighteen NATO members offered support and assistance.[33] On September 12, 2001, the North Atlantic Council met to discuss 9/11. The council stated:

> that if it is determined that this attack was directed from abroad against the United States, it shall be regarded as an action covered by Article 5 of the Washington Treaty, [34] which states that an armed attack against one or more of the Allies in Europe or North America shall be considered an attack against them all.[35]

For the first time, NATO viewed a presumptive terror attack as an armed attack triggering the right to self-defense and collective self-defense.

On the same day, the Euro-Atlantic Partnership Council (EAPC)[36] pledged its assistance

---

33 North Atlantic Treaty Organization, Statement by the North Atlantic Council, PR/CP (2001) 122 (11 Sep. 2001), http://www.nato.int/docu/pr/2001/p01-122e.htm.

34 The North Atlantic Treaty Art. 5 (4 Apr. 1949)

> "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.")

35 North Atlantic Treaty Organization, Statement by the North Atlantic Council, PR/CP (2001) 124 (12 Sep. 2001), http://www.nato.int/docu/pr/2001/p01-124e.htm.

36 The Euro-Atlantic Council is composed of: Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kazakhstan, Kyrghyz Republic, Latvia, Lithuania, Luxembourg, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Tadjikistan, Turkey, Turkmenistan, Ukraine, United Kingdom, United States, Uzbekistan. *See*, Statement of the Euro-Atlantic Partnership Council, PR-123 (12 Sep. 2001). http://www.nato.int/docu/pr/2001/p01-123e.htm.

"to undertake all efforts to combat the scourge of terrorism."[37] This statement by the EAPC is interesting in that it represents the views of not only NATO members but also the member states, which traditionally were either non-aligned states or former members of the Soviet Union. These non-aligned states and those from the former Soviet Union represent a diverse collection of states that had traditionally opposed actions by the United States in various forms during the Cold War. While the statement does not specifically endorse any approach taken by the United States, it recognizes that the attacks upon the United States were such to trigger a collective response.

The first public indication that the intended state target would be Afghanistan and the Taliban/Al-Qaeda was on September 20, 2001, when the United States Deputy-Secretary of State, Richard Armitage, met with the NATO secretary general and briefed the secretary-general "on information acquired up to now by the United States authorities on the terrorist attacks of 11 September."[38] After this briefing, NATO reiterated the invocation of Art. 5 of the Washington Treaty and formally indicated that the individuals responsible for the terror attacks were affiliated with Al-Qaeda. The NATO secretary general stated:

> [t]he briefing addressed the events of 11 September themselves, the results of the investigation so far, what is known about Osama bin Laden and the Al-Qaida organization and their involvement in the attacks and in previous terrorist activity, and the links between Al-Qaida and the Taleban regime in Afghanistan… We know that the individuals who carried out these attacks were part of the world-wide terrorist network of Al-Qaida, headed by Osama bin Laden and his key lieutenants and protected by the Taleban.
>
> On the basis of this briefing, it has now been determined that the attack against the United States on 11 September was directed from abroad and shall, therefore, be regarded as an action covered by Article 5 of the Washington Treaty, which states that an armed attack on one or more of the Allies in Europe or North America shall be considered an attack against them all.[39]

The secretary-general then stated that the decision to invoke the Art. 5 provisions was a

---

37 *Id.*

38 NATO Update, *High-Level US Official at NATO HQ*, 26 Sept. 2001, http://www.nato.int/docu/update/2001/0917/e0920a.htm.

39 North Atlantic Treaty Organization, Statement by NATO Secretary-General, Lord Robertson, 2 Oct. 2001, http://www.nato.int/docu/speech/2001/s011002a.htm.

unanimous decision on behalf of all eighteen member states.[40] NATO followed the announcement on October 2, 2001, with an announcement on October 4, 2001, in which it operationalized its plans to support the United States by establishing eight "measures,"[41] including such military-specific acts as blanket overflight permission in all NATO members territories "for military flights related to operations against terrorism…"[42] NATO specifically addressed these measures as a fight against terrorism while impliedly acknowledging that the state harboring terrorists would be targeted.

NATO's support produced results on October 7, 2001, when the United States and British aircraft attacked Taliban positions within Afghanistan[43] with aircraft from both countries utilizing NATO states' airspace either as launching points or transiting through on the way to the attacks. The day after the initial attacks, the NATO secretary-general stated, "[t]his operation is not directed against the people of Afghanistan. It is designed to strike against al-Qaida terrorist training camps and military installations of the Taliban regime in Afghanistan."

Finally, on December 6, 2001, NATO released a statement from the Ministerial Meeting of the North Atlantic Council in which the Council laid out its ideology toward its combined response to terrorist attacks. In paragraph four of the document, NATO states:

> [o]ur fight is not against Islam or the innocent people of Afghanistan. Our countries are helping to provide humanitarian assistance to the Afghan people, who have suffered under the cruelty of the Taliban regime. Our fight, the fight of the international community, is against the terrorists, their networks and those who harbor them, as stated in Resolution 1368 of the UN Security Council.[44]

---

40 *Id.*

41 North Atlantic Treaty Organization, *Statement to the Press by NATO Secretary-General, Lord Robertson on the North Atlantic Council Decision on Implementation Of Article 5 of the Washington Treaty Following the 11 September Attacks Against the United States*, 4 Oct. 2001, http://www.nato.int/docu/speech/2001/s011004b.htm.

42 *Id.*

43 Patrick E. Tyler, *A Nation Challenged: The Attack; U.S. and Britain Strike Afghanistan, Aiming at Bases and Terrorist Camps; Bush Warns 'Taliban Will Pay A Price'* NY Times (Oct. 7, 2001), http://www.nytimes.com/2001/10/08/world/nation-challenged-attack-us-britain-strike-afghanistan-aiming-bases-terrorist.html.

This idea of targeting "those who harbor [terrorists]"[45] was not, per se, a new idea in international law. But the specific linking of the Taliban to the acts of Al-Qaeda and attributing the 9/11 attacks to the Taliban is an expansion of the existing state responsibility paradigm which will be discussed in depth *infra*.

7.1.3.3. State Specific Response: Permanent Members of the Security Council

7.1.3.3.1. United States

The response by the United States was initially focused on the traditional law enforcement approach to counter-terrorism that had been the prevalent paradigm to terror attacks prior to 9/11. The initial response as directed by the then-President of the United States, George W. Bush, was to direct intelligence and law enforcement assets to "find those responsible and bring them to justice."[46] At the same time, the president made it clear that the United States would "make no distinction between the terrorists who committed these acts and those who harbor them."[47]

On September 12, 2001 "[t]he President tasked principals to…develop a strategy to eliminate terrorists and punish those who support them."[48] This idea of punishing those who support or harbor terrorists was further refined to apply to anyone that "supported Al-Qaeda."[49]

---

44 North Atlantic Treaty Organization, Statement issued at the Ministerial Meeting of the North Atlantic Council held at NATO Headquarters, Brussels, 6 December 2001, M-NAC-2 (2001) 159, http://www.nato.int/docu/pr/2001/p01-159e.htm.

45 *Id.*

46 George W. Bush, *Address to the Nation on the September 11 Attacks*, in, The Collected Speeches of George W. Bush 58 (2013).

47 *Id.*

48 *Id.*

49 *Id.* at 331.

The focus on holding the Taliban responsible for the actions of Al-Qaeda began on September 13, 2001, when President Bush ordered military plans to be drawn up to attack the Taliban.[50]

The President wanted the United States to strike the Taliban, step back, wait to see if they got the message, and hit them harder if they did not. The president made it clear that the military should focus on targets that would influence the Taliban's behavior.[51]

The initial focus of these attacks was not, per se, regime change within Afghanistan, rather the goal to gain compliance by the Taliban in handing over the leadership of Al-Qaeda to the United States. [52] On September 17, 2001, President Bush authorized covert action plans within Afghanistan utilizing joint CIA/military special forces. Additionally, the president directed further plans for military action be formulated if the Taliban rejected the ultimatum.[53] The United States would also target the funding and support networks for Al-Qaeda in an attempt to eliminate any and all outside support.

The United States Congress acted on September 14, 2001, by introducing and passing the "Authorization to Use Military Force"[54] (AUMF), which President Bush signed into law on September 18, 2001. §2(a) of AUMF, states:

> [t]hat the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons, he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.[55]

---

50 *Id.*

51 The 9/11 Commission Report 330-333 (2004).

52 *Cf. id*. at 331-332. (Discussing the establishment of demands to the Taliban to turn over Osama bin Laden, close terrorist training camps, and comply with all Security Council resolutions.)

53 *Id.* at 333.

54 Authorization to Use Military Force, Pub. L. No. 107-40, 115 Stat. 24 (2001).

55 *Id.* at §2.

The AUMF specifically granted President Bush statutory authority under the War Powers Act, giving the president full control of military forces to act, as needed, within the guidelines of the Act.

On September 20, 2001, in remarks to a joint session of the United States Congress, President Bush formally stated what had been discussed in private: that the United States believed Al-Qaeda was responsible for the terror attacks. President Bush stated, "[t]he evidence we have gathered all points to a collection of loosely affiliated terrorist organizations known as Al-Qaeda. They are the same murderers indicted for bombing American embassies in Tanzania and Kenya, and responsible for bombing the USS Cole."[56] The president then linked Al-Qaeda with the Taliban and indirectly linked 9/11 to the Taliban, stating that "we condemn the Taliban…[b]y aiding and abetting murder, the Taliban is committing murder…"[57]

The culmination of United States action occurred on October 7, 2001, when the United States and its allies launched a naval and air bombardment upon Afghanistan. In his address to the United States public, President Bush stated:

> [o]n my orders, the United States military has begun strikes against al-Qaeda terrorist training camps and military installations of the Taliban regime in Afghanistan. These carefully targeted actions are designed to disrupt the use of Afghanistan as a terrorist base of operations and to attack the military capability of the Taliban regime.[58]

President Bush continued equating the acts of Al-Qaeda with those of the Taliban. This connection was further elucidated when the United States formally notified the Security Council of the attacks pursuant to Art. 51 of the United Nations Charter. The United States stated, "the attacks on 11 September 2001 and the ongoing threat to the United States and its nationals posed by the Al-Qaeda organization have been made possible by the decision

---

56 George W. Bush, *Address to Joint Session of the 107th Congress, in*, The Collected Speeches of George W. Bush 66 (2013).

57 *Id.* at 67. (The president was speaking in a broader context concerning the acts of oppression and murder within Afghanistan under the Taliban, but the connotation was clear that the United States viewed the Taliban as complicit in the 9/11 attacks.)

58 George W. Bush, *Address to the Nation on Operations in Afghanistan, in*, The Collected Speeches of George W. Bush 75 (2013).

of the Taliban regime to allow the parts of Afghanistan that it controls to be used by this organization as a base of operation."[59]

Finally, President Bush stated that:

> [w]e are joined in this operation by our staunch friend, Great Britain. Other close friends, including Canada, Australia, Germany, and France, have pledged forces as the operation unfolds. More than 40 countries in the Middle East, Africa, Europe and across Asia have granted air transit or landing rights. Many more have shared intelligence. We are supported by the collective will of the world…[60]

This show of support by the collective states demonstrates either a complete disregard for the existing customary law of state responsibility, ignorance thereto, or the establishment of a new custom. This too will be discussed *infra.*

7.1.3.3.2. United Kingdom

The United Kingdom, arguably the United States' closest ally and the state with the largest loss of life outside of the United States from the attacks,[61] was the closest international partner with the United States in regards to the military response. When the then-Prime Minister Tony Blair learned of the attacks, his initial public response was that the United Kingdom "would stand shoulder-to-shoulder with the United States."[62]

The U.K. Home Secretary Jack Straw "promised that Britain would provide any military and intelligence help to assist the US in bringing the perpetrators to justice."[63] Indeed, the

---

59 Letter Dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations Security Council Addressed to the President of the Security Council, S/2001/946.

60 *Id.*

61 *British Victims of September 11*, The Guardian (10 Sept. 2002), http://www.theguardian.com/world/2002/sep/10/september11.uk. (Reporting that 67 U.K. citizens were lost in the attacks on 9/11).

62 Michael White and Patrick Wintour, *Blair Calls For World Fight Against Terror*, Special Report: Terror in the United States, The Guardian (12 Sept. 2001), http://www.theguardian.com/politics/ 2001/sep/12/uk.september11. *See also*, Lindsay Clutterbuck, *The Transatlantic Impact of 9/11* (Sept. 13, 2011), The Rand Corp., http://www.rand.org/blog/2011/09/the-transatlantic-impact-of-911.html.

UK government honored these words, and on October 7, 2001, they launched naval and air bombardments upon Afghanistan territory in conjunction with the United States and other allied forces.[64] The basis for these attacks upon Afghanistan was that the UK government believed that Al-Qaeda, as supported by the Taliban in Afghanistan, posed a continued threat to the United States and other countries.[65] Thus the United Kingdom invoked its Art. 51 right to individual and collective self-defense with the United States against Al-Qaeda and the Taliban.

The United Kingdom viewed the Taliban as an accomplice to 9/11, believing that by:

> not complying with these demands [of the Security Council to turn over Osama bin Laden and other al Qaeda leaders] and their obligations under international law to combat terrorism, the Taliban themselves became involved in international terrorism and clearly violated international law. In doing so, it has been argued, the Taliban became an accomplice of al-Qaeda, which made them too internationally responsible for the terrorist attacks of 11 September 2001…[66]

This idea of being an accomplice before and after the fact is an interesting idea though the idea did not comport with CIL as it existed on September 11, 2001, as posited by the ARS. However, one may argue that the act of being an accomplice state may fall within the rubric of Art. 11.[67] An act assisted in after-the-fact may be considered an adoption by a state, but it is argued that this idea of an accomplice state is different in toto than that of the adoption of an act after the fact.

---

63 *Id.*

64 Patrick E. Tyler, *A Nation Challenged: The Attack; U.S. and Britain Strike Afghanistan, Aiming at Bases and Terrorist Camps; Bush Warns 'Taliban Will Pay A Price'* NY Times (Oct. 7, 2001), http://www.nytimes.com/2001/10/08/world/nation-challenged-attack-us-britain-strike-afghanistan-aiming-bases-terrorist.html.

65 Letter Dated 7 October 2001 From the Chargé d'affaires of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations Addressed to the President of the Security Council, U.N. Doc. S/2001/947.

66 Ben Smith and Arabella Thorp, *The Legal Basis For The Invasion of Afghanistan* 5, House of Commons (UK), SN/IA/5340 (2010).

67 *Draft Articles on Responsibility of States for Internationally Wrongful Acts,* Art. 11, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

7.1.3.3.3. France

France's position was one of solidarity and support with the United States. In a television interview on September 13, 2001, the President of France, Jacques Chirac, stated that France would stand with the United States and that France was in full support of the invocation of Art. 5 of NATO treaty.[68]

In addition to holding Al-Qaeda responsible, France also saw the role that the Taliban played in sheltering and harboring terrorists, and associated 9/11 to not only Al-Qaeda but also to the Taliban who "sheltered and supported…al Qaeda."[69] France, like the United States and the United Kingdom, held the Taliban responsible for the acts of Al-Qaeda.

France also actively supported military operations in Afghanistan against the Taliban and Al-Qaeda, acting in support of NATO operations and as a member of the International Security Assistance Force.[70]

7.1.3.3.4. Russia

The Russian response to the 9/11 attacks and the subsequent invasion of Afghanistan caught many commentators by surprise.[71] President Putin, the Russian president at the time of the attacks, was particularly vocal in his support of the United States, stating "[t]here is no doubt that such inhuman actions cannot be left unpunished. The whole international community must rally in the fight against terrorism."[72]

---

68 Christine Amanpour, *America Under Attack: Talk with French President Jacques Chirac (Transcript)*, (Sept. 13, 2001), http://archives.cnn.com/TRANSCRIPTS/0109/13/se.31.html.

70 *See*, S.C. Res. 1386, U.N. Doc. S/Res/1386 (20 Dec. 2001). (Authorizing the International Security Assistance Force).

71 *See e.g.*, John O'Loughlin *et al*., *A 'Risky Turn'? Putin's 9-11 Script and Ordinary Russians*, 56 Europe-Asia Studies 3 (2004). (Discussing the surprising acceptance to the opening of the "Eurasian" heartland to American bases as such acceptance was traditionally against traditional Russian geopolitical thinking.)

It should be noted that there was a split within Russia on how to view the attacks. Originally, the Russian Foreign Ministry discussed the attacks and those who perpetrated them under the "restrictive analysis"[73] rubric: they saw the attacks as a criminal matter referring to the attacks as "crimes of terrorists in the USA."[74] Other facets of the Russian government described the attacks and the response to them from a military viewpoint: these attacks were not criminal so much as an act of illegal aggression.[75] The view of the Russian government begins to solidify toward supporting military action beginning with a meeting of President Bush and Russian Foreign Minister Igor Ivanov on Sept. 19, 2001, when the foreign minister stated to the press, "Russia has always favored expanded international cooperation in the struggle against extremism and terrorism, because no state, however, strong it may be, cannot tackle the problem single-handedly."[76]

The Russian Duma broached the idea of a military response by stating, "[t]he organizers of the acts of terrorism and their patrons must be identified and brought to justice. Any,

---

72 On Russian President Vladimir Putin's Telegram of Condolence to US President George Bush (Sept. 11, 2001), http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/196ef713841ec63b432 56ac60 02f8ea7!OpenDocument.

73 *See*. Christian Tams, *The Use of Force Against Terrorists*, 20 European J. Int'l L. 359, 363-364 (2009). (Describing the normative approach to terrorism pre-9/11 as "restrictive analysis–an approach seeking to limit the military force to the largest extent possible," and discussing the "approach [to] terrorism as a problem of criminal law to be addressed by means short of international military force.")

74 Ministry of Foreign Affairs of the Russian Federation, *Press Release: UN Security Council Statement Regarding Terrorist Acts in USA* (Sept. 12, 2001), http://www.mid.ru/bdomp /brp_ 4.nsf/e78a48070f128a7b43256999005bcbb3/65016b35f6a5140e43256ac6002f8eb1!OpenDoc ument. (Unofficial translation from Russian). *See also*, Ministry of Foreign Affairs of the Russian Federation, *Press Release: Decision No. 438 by the Permanent Council of the Organization for Security and Cooperation in Europe on the Acts of Terrorism in New York City and Washington, D.C.* (Sept. 14, 2001), http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/f85a74e6866e14e 443256aca003ae7cf!OpenDocument.

75 *See*, Russia–NATO Statement (Sept. 13, 2001), http://www.mid.ru/bdomp/brp_4.nsf /e78a48070f128a7b43256999005bcbb3/66b3a03f8a8b608843256ac7003efef0!OpenDocumen t. ("Russia and NATO are calling on the international community to join in the fight against terrorism. Russia and NATO will intensify cooperation under the Founding Act in order to defeat this greatest evil.")

76 Transcript of statement by Russian Foreign Minister Igor Ivanov on the Results of His Meeting with US President George Bush, September 19, 2001, http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/78985760deef75c 643256acd00616db0!OpenDocument.

including military, actions by states or international organizations against international terrorists should be based on the generally recognized principles and rules of international law, proportionate and strictly considered."[77] The issue of the Taliban as a threat emerged in a statement by the U.S.–Russian Working Group on Afghanistan, when the group stated "[i]n accordance with the UN Security Council Resolution 1333 (2000), agreement was reached to enhance further joint and parallel efforts to counter threats coming from the Taliban in Afghanistan. It was emphasized that such a fight should not be a one-time effort nor spontaneous in its nature, but rather be based on a comprehensive and long-term basis, in the interest of stamping out this universal evil as a phenomenon."

On September 24, 2001, President Putin stated that Russia supported the proposed "anti-terror"[78] operations in Afghanistan. As part of the Russian support, Russia would supply: (1) intelligence concerning the "infrastructure and locations of international terrorists and about the bases training militants";[79] (2) make Russian airspace available to flights "carrying humanitarian cargo to the area of that anti-terrorist operation";[80] (3) coordinate with Russia's "Central Asian allies"[81] to allow the use of their airspace and potentially airfields in support of anti-terror operations; (4) offer "to take part in international search and rescue operations";[82] and (5) agree to "provide additional support to armed forces in the form of arms and military hardware supplies"[83] to the internationally recognized government of Afghanistan. In addition, President Putin made the option available for further support to those involved in the anti-terror operation in Afghanistan.[84]

---

77 Federal Assembly of the Russian Federation Resolution by the State Duma, On the Struggle Against International Terrorism (Sept. 19, 2001), http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43 256999005bcbb3/ 489a88b 06710998d43256 ad10056f420!OpenDocument.

78 Statement by President Vladimir Putin of Russia, Moscow, September 24, 2001, http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/5e2870b37fe461 dc43256ad20031b7f8!OpenDocument. (Unofficial translation from Russian).

79 *Id.*

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

The Russian response to the United States and NATO's operations in Afghanistan against the Taliban and Al-Qaeda are important for several reasons. Russia, when it was the Union of Soviet Socialist Republics (USSR), was the antagonist to the United States and NATO during the Cold War. Indeed, NATO was formed, partially, in response to the perceived threat of the Soviet Union. As the modern embodiment of the Soviet Union, Russia has not always been seen to have the best interest of Western powers at heart. One may posit that for Russia to support the military campaign against the Taliban and Al-Qaeda, the acts of the United States and NATO were understood by the Russian government as legitimate in international law. Additionally, Russia's acceptance to the apportioning of blame to the Taliban in addition to Al-Qaeda for 9/11 is of enormous importance for the creation of a new customary norm for state responsibility. Given that even at the beginning of the twenty-first century it may be contended that Russia, along with the United States are still the two most prominent, albeit usually opposed, international powers. Accordingly, the weight of both the principal actors in supporting the attribution of responsibility to the Taliban for the acts of Al-Qaeda is significant.

7.1.3.3.5. China

Of the five permanent members of the United Nations Security Council, China's initial reaction to the attacks, while sympathetic, was the most cautious regarding the United States' response. While this caution by China may have been a result of existing tensions between China and the United States,[85] it quickly dissipated as China grew to support the United States' position on the invasion of Afghanistan.[86] China's initial support was qualified as China "insist[ed] on several conditions for any US action. [Actions taken by the United States] should be authorized by the United Nations Security Council, be based on concrete evidence, observe international law, and not target innocent civilians."[87] China,

85 Mark Mackinnon, *China's Chance: How 9/11 played into Beijing's Plans in Asia*, The Globe and Mail (Sept. 6, 2012), http://www.theglobeandmail.com/news/world/chinas-chance-how-911-played-into-beijings-plans-in-asia/article593666/.

86 Michael Szonyi, *Commentary No. 81: The Effects of September 11 and Its Aftermath on China, and The Chinese Response*, Canadian Security Intelligence Service (Spring 2002), http://www.csis-scrs.gc.ca/pblctns/cmmntr/cm81-eng.asp.

however, did not push for a Security Council resolution authorizing the use of force by the United States and acquiesced to the military actions in Afghanistan by the United States and its allies.[88] Along with the other permanent members of the Security Council, China accepted that the Taliban was in part responsible for the attacks and as a permanent member of the Security Council, supported (or acquiesced to) all resolutions concerning the Taliban and the anti-terror resolutions put forth by the Security Council.

7.1.3.3.6. Other International Response

While only the United States and Great Britain actively used military forces in the initial invasion of Afghanistan on October 7, 2001, they were actively supported by NATO countries[89] and had pledges of support from over forty countries.[90] Many others supported the actions of the United States and its allies in various ways. Numerous regional bodies supported the acts of the United States after 9/11 and supported the military intervention in Afghanistan. Many regional bodies such as the Organization of American States took the additional step of recognizing that states that harbor or aid terrorist organizations would be deemed to be complicit in any act taken by the terrorist group in contravention of international law. It is clear that a majority of states either directly supported or acquiesced to the United States and NATO's actions in Afghanistan.

---

87 *Id.*

88 Jacques deLisle, *9/11 and U.S.–China Relations*, Foreign Policy Research Inst. (Sept. 2001), http://www.fpri.org/enotes/2011/201109.delisle.911.html#note2. Mark Mackinnon, *China's Chance: How 9/11 played into Beijing's Plans in Asia*, The Globe and Mail (Sept. 6, 2012), http://www.theglobeandmail.com/news/world/chinas-chance-how-911-played-into-beijings-plans-in-asia/article593666/. Michael Szonyi, *Commentary No. 81: The Effects of September 11 and Its Aftermath on China, and The Chinese Response*, Canadian Security Intelligence Service (Spring 2002), http://www.csis-scrs.gc.ca/pblctns/cmmntr/cm81-eng.asp. (Archived content).

89 *See*, Council of Foreign Relations, *US Led Attack on Afghanistan Begins* (n.d.), http://www.history.com/this-day-in-history/us-led-attack-on-afghanistan-begins. ("On [October 7,] 2001, a U.S.-led coalition beg[an] attacks on Taliban-controlled Afghanistan with an intense bombing campaign by American and British forces. Logistical support was provided by other nations including France, Germany, Australia and Canada and, later, troops were provided by the anti-Taliban Northern Alliance rebels.")

90 George W. Bush, *Address to the Nation on Operations in Afghanistan*, *in*, The Collected Speeches of George W. Bush 75 (2013).

7.2. Analysis

Given the information *supra* concerning the response by the United States, NATO, and other states after 9/11, and given the basic understanding of the existing CIL on state responsibility, a discussion and analysis of these facts and law are in order. This study will utilize the information presented in Chapter Two for the purposes of determining the formation of custom.

7.2.1. State Practice

In the matter of state practice, it is important to note that all permanent members of the UN Security Council and forty-four states participated in some form either directly or indirectly in the attacks on the Taliban and Al-Qaeda.[91] This conduct, while publicly debated and justified, did not provoke significant protest from relevant number of states. Only two states have openly questioned the legality of the military operation.[92] In addition, the invasion of Afghanistan and the removal of the Taliban government had the seeming support of the UNGA.[93] The first issue is whether this single response is enough to establish state practice for the purpose of establishing new CIL, and were the actions of the Security Council, NATO, and other states supporting the invasion of Afghanistan extensive enough to demonstrate "a requisite grounding in general state practice."[94]

State practice is established by "practice, which is uniform, extensive and representative in character…(ii) Although normally some time will elapse before there is sufficient practice to satisfy these criteria, no precise amount is required."[95] This initial question of whether uniformity of practice was established is debatable as to uniformity of practice as aside

---

91 The UNGA also seemingly supported military operations against Afghanistan, *see*, *Condemnation of Terrorist Attacks in the United States of America*, G.A. Res. 56/1 (VIII), U.N. GAOR 55th Sess., U.N. Doc. A/Res/56/1 ¶¶ 3-4 (18 September 2001).

92 Ruys, *id*, at 281.

93 *Id.*

94 John Tasioulas, *Opinio Juris and the Genesis of Custom*, 26 Aust. Y.B. Int'l L. 199 (2007).

95 International Law Associations Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary Law* (as amended by the London Conference) Art. 12 (2000).

from the initial claim by the U.S. and NATO there has been little subsequent state practice in holding a state responsible for the actions of a non-state actor, with only the U.S. and Israel claiming this idea to date thus, it is debatable whether this limited amount of state practice is enough.

Given the view of the states participating and the Security Council, the holding of the Taliban at least partially responsible for 9/11 is uniform as defined by the ILA Reports Art. 13 in that the collective uniformity of state actions did not vary substantially. "Collective" uniformity means that different states must not have engaged in substantially different conduct, some doing one thing and some another.[96] That is, all the states acted with external conformity in assigning responsibility to the Taliban. [97] This study would argue that this is seemingly met in the instant matter as all the participating states acted in conformity with the acts of the United States and its allies.

The idea of extensiveness, as put forth in the ILA Reports, is a qualitative rather than quantitative idea.[98] The standing of the states who participate is more important than the total quantity of states participating. This factor is also met in that all the major world powers in the form of the permanent members of the Security Council, endorsed the act of holding the Taliban responsible for the acts of Al-Qaeda.

The question whether state practice is representative in nature is defined as both a:

> negative and positive. The *positive* aspect is that, if all major interests ('specially affected States') are represented, it is not essential for a majority of States to have participated *(still less a great majority, or all of them*). The *negative* aspect is that if important actors do *not* accept the practice, it cannot mature into a rule of general customary law.[99]

Here, the specially affected states, as discussed infra, involved were mainly the United States and, the Security Council, NATO, and 44 other involved states, but 9/11 touched

96 *Id.* Art. 13.

97 *Id.*

98 *Id.* Art. 14, cmt. e.

99 ILA, *id.*, n. 102. (Emphasis added).

many other states. While it is doubtful that if the United States had acted unilaterally, a new custom might have been formed, this argument is unnecessary given the other states that were involved and the high-level international support for the acts of the United States and its allies. This support is demonstrated by the support of the Security Council which held the Taliban partially responsible for the acts of Al-Qaeda. Defining what important actors need act is not clear, however, in the instant matter, this study would argue that the important actors are the specially affected states, the United States, the Security Council, NATO and the 44 states involved in the invasion of Afghanistan. In this respect, all the important actors worked together against the Taliban. Thus, this study would argue that the practice prong is met, particularly as per the ILA Art.14 which emphasizes that "it is not simply a question of how many states participate in the practice, but *which* states."[100] In this respect the "which states" are those argued above, the specially affected states, the Security Council, NATO and other actors involved in the invasion of Afghanistan.

This study argues that based upon the impact of the 9/11 attacks on the United States in terms of economy, damage to the national psyche, the long-term effects on the United States, and the United States subsequent actions in international law to pursue al Qaeda and the Taliban that the actions of the United States, for demonstrating state practice, should be viewed as a specially affected state. There is no set qualification to determine that a state is a "specially affected state." The ICJ in the *North Sea Continental Shelf* case stated that specially affected states "include those whose interests are specially affected."[101] Who is considered a specially affected state will depend upon the circumstances presented in the formation of the custom.[102] The International Committee of the Red Cross has argued that for the development of international humanitarian law that those parties who participate in an armed conflict may be regarded as specially affected.[103] This study argues, that it is those states who supported the military intervention and who were parties thereto are specially affected states as was discussed supra and in chapter two supra. Thus, the United States,

100 *See also*, Tasioulas, *supra*. ("[A] customary norm does not require the consent of all States in order to come into existence…")

101 North Sea Continental Shelf Cases, 1969 I.C.J. Rep. 3,43 (20 Feb.)

102 *See*, Int'l Comm. Red Cross, *Customary IHL* (n.d.), https://ihl-databases.icrc.org/customary-ihl/eng/docs/.

103 *Id.*

the Security Council, NATO, and the 44 states that participated in one form or another in the invasion of Afghanistan all should be considered specially affected states as all these members (with the exception of China but China acquiesced to the other Security Council members and approved of the acts of the Security Council) participated in one form or another in the armed conflict. In addition, many of the states involved in the invasion of Afghanistan also lost citizens in the 9/11 attacks thus making them specially affected due to the loss of their citizens in the terror attack.

The second part of state practice, duration, is a difficult question. If one looks at the time states were engaged in Afghanistan, the duration to date has been over fifteen years. However, this arguably is not enough time as the engagement in Afghanistan still stems from the original acts in 2001. Since the invasion of Afghanistan only one instance of state practice can be found at this level, i.e., the invasion a state due to the acts of a non-state actor; that being the invasion of Lebanon by Israel in 2006, hence there is the duration of practice albeit on a small scale. As such, the second prong of sufficient practice seems to fail.[104] Thus, if a new custom was formed, it would be under an alternative theory and more controversial as to its formation.

It should be noted, however, that other forms of state responsibility such as the holding of states responsible for malicious cyber-attacks without direct attribution to the state seem to be on the rise. While this is qualitatively different from the state practice seen with the invasion of Afghanistan and the overthrow of the Taliban government, such acts may signal either a lessening of the importance of rules of attribution or a shift toward indirect responsibility. Whether this is due to the acts of the United States and its allies of holding the Taliban responsible for the acts of Al-Qaeda is impossible to demonstrate, and as such, this study takes no position other than to note its occurrence.

This study will now turn to the question regarding an alternative reading regarding the actions of states against the Taliban. This study will briefly discuss alternative interpretations of state acts against the Taliban. That is, did states act against the Taliban for the Taliban's own acts and not the acts of al Qaeda.

104 *But cf.,* Jack L. Goldsmith & Eric A. Posner, *The Limits of International Law* 23 (2005). ("[C]ustomary international law is usually based on a highly selective survey of [S]tate practice that includes only major powers and interested [S]tates.")

7.2.1.1. Alternative Reading of State Practice

One may argue, indeed many have, that states acted in Afghanistan against the Taliban for the Taliban's own failures in respect to al Qaeda and the Taliban's crimes against the people of Afghanistan. The Taliban has been accused of various illegal acts and had failed since at least 1999 to comply with Security Council resolutions to turn over Usama bin Laden and other al Qaeda leadership.[105] The failure to turn over Usama bin Laden as requested in 1999 is particularly important as his extradition was sought by the United States in response to bin Laden's alleged involvement with the terrorist bombings of United States Embassies in Tanzania and Kenya in 1998.[106] Yet the Taliban ignored the requests of the Security Council and was, for lack of a better term, an international pariah because of its own acts in Afghanistan and its lack of respect for international law. It is the Taliban's actions, or lack thereof, combined with the events of 9/11 that many commentators feel were the impetus to invade Afghanistan and overthrow of the Taliban and rid the world of two entities the Taliban and al Qaeda.

This study does not discount the possibility that states used the events of 9/11 to justify the invasion of Afghanistan and the overthrow of the Taliban. However, based upon this studies interpretation of the official statements of the Security Council and its members the states, which linked the acts of the Taliban to that of al Qaeda and held (in the eyes of this study) the Taliban responsible for the actions of al Qaeda, as such this study adopts an alternative interpretation. The alternative interpretation is that the Taliban was held vicariously responsible, based upon its failure to act in accordance with international law and its own lack of due diligence, for the actions of al Qaeda. This study believes this alternative interpretation is bolstered by subsequent state practice by specially affected states when

105 Mark A. Drumbl, *The Taliban's 'Other' Crimes*, 23 Third World Qrtl'y 1121 (2003). *See e.g.,* S.C. Res.1267 (1999), S/Res/1267 (15 Oct. 1999).

106 Christopher Greenwood*, International Law and the 'War on Terrorism*.' 78 Int'l Aff. 301 (2002). S.C. Res. 1267 (1999).

those state attempted negotiations with the Taliban by the United States and its allies.[107] If the specially affected states believed that the invasion of Afghanistan was solely to remove the Taliban, then it is doubtful that those same states would now be engaging with the very entity it sought to remove. However, if those states saw the Taliban as only vicariously responsible for the acts of al Qaeda, then when al Qaeda has (figuratively) been removed from Afghanistan it would make sense to re-engage with the Taliban to seek peace in Afghanistan. This study argues that it was the Taliban's vicarious responsibility for the acts of al Qaeda and the Taliban's failures to adhere to Security Council demands that lead to the invasion of Afghanistan and the Taliban's overthrow.[108]

In addition, if states had wished to act against the Taliban for its own crimes, states had seven years to do so as the Security Council had singled out the Taliban as early as 1999 and had determined as late as 30 July 2001 "that the situation in Afghanistan constitute[d] a threat to international peace and security in the region…"[109] arguably justifying the use of force against the Taliban. However, the Security Council, nor any state took action against the Taliban. No action was taken against Afghanistan until after the events on 9/11.[110] The events of 9/11 inexorably tied the Taliban to the acts of al Qaeda, particularly, as discussed supra, as the Taliban had prior notice of the potential threat that al Qaeda posed to international peace and security.

Lastly, a detailed analysis of Security Council resolutions, and statements by member states, as demonstrated supra; In which the states justified the invasion of Afghanistan and the overthrow of the Taliban, supports the theory that those states linked the acts of al Qaeda to the failure to act by the Taliban and held the Taliban responsible for those failures and

---

107 Mushtaq Yusufzai, Abigail Williams. and F. Brinley Bruton, *Taliban Begins Secret Peace Talks with U.S., Afghan Officials: Sources*, NBC News (Oct.18, 2016), http://www.nbcnews.com/news/ world/ taliban-begins -secret-peace- talks-u-s-afghan-officials-sources-n668131.

108 *Cf.* Andre Nollkaemper. *The Security Council and the Use of Force (Legal Aspects of International Organization)* 163 (Niels Blokker and Nico Schrijver eds., 2015). ("[I]t has been noted that, since the Taliban regime provided AL Qaeda with shelter and training facilities and allowed the organization to use Afghanistan as its base from which to sponsor international terrorist operations the proximate result of that conduct would be an armed attack on the United States.")

109 S.C. Res. 1363 (1999), S/Res/1267 (30 July 2001).

110 *Cf.* S.C. Res. 1368 (2001), S/Res/1363 (12 Sep. 2001). (Recognizing the right to use self-defense).

ascribed the acts of al Qaeda vicariously to the Taliban. For example, in S.C. Res. 1378, the Security Council

> [condemned] the Taliban for allowing Afghanistan to be used as a base for the export of terrorism by the Al-Qaida network and other terrorist groups and for providing safe haven to Usama Bin Laden, Al-Qaida and others associated with them, and in this context supporting the efforts of the Afghan people to replace the Taliban regime…[111]

In the eyes of the Security Council, the Taliban was vicariously responsible for the terror attacks that al Qaeda launched by allowing al Qaeda to utilize its territory. By utilizing the verb "allowing" the Security Council is demonstrating its belief that the Taliban had some control over the acts of al Qaeda and by failing to control the acts of al Qaeda the Taliban was subsequently vicariously responsible for the acts of al Qaeda. The term "allow" as used by the Security Council signifies that there was a relationship between the Taliban and al Qaeda and that the Taliban could have prevented al Qaeda from conducting the terror attacks on the United States.[112] While some may argue that the term is inconsequential to the current argument, this study believes that the official acts of the Security Council must be interpreted in the strictest sense and believes that the Security Council chooses its words with care. Therefore, the use of the word "allowing" is significant.

Such association between the Taliban and al Qaeda and the holding of the Taliban responsible for the acts of al Qaeda may be found in other official communications by states and NATO. For instance, the NATO Secretary General linked the actions of al Qaeda to the Taliban when he stated

> the results of the investigation so far, what is known about Osama bin Laden and the Al-Qaida organization and their involvement in the attacks and in previous terrorist activity, and the links between Al-Qaida and the Taleban regime in Afghanistan… [offer clear and convincing evidence that al Qaeda is responsible for the attacks on 9/11]. [113]

---

111 S.C. Res. 1378 (2001), S/Res/1378 (14 Nov. 2001).

112 *Cf.,* Eric Posner and Alan O. Sykes, *An Economic Analysis of State and Individual Responsibility Under International Law*, 9 Am. L. and Econ. Rev.72 (2007). (Arguing that "that the basic rationale for state responsibility under international law is akin to the rationale for vicarious liability under domestic law…" Vicarious responsibility in this respect would apply in the instant matter as the Taliban had, in tort terms, the duty to control al Qaeda and when it failed to do so it became vicariously liable for al Qaeda's acts.)

113 North Atlantic Treaty Organization, Statement by NATO Secretary-General, Lord Robertson, 2 Oct. 2001, http://www.nato.int/docu/speech/2001/s011002a.htm.

Thus, linking the Taliban to the acts of al Qaeda and holding the Taliban vicariously liable. Such linkage may be found in comments by the leaders of the United States, Great Britain, France, and Russia as demonstrated supra. Based upon these comments, which as discussed infra constitute opinio juris, this study argues that the Taliban was held vicariously responsible for the acts of al Qaeda and not because of the acts of the Taliban standing alone. This study therefore rejects the theory that Afghanistan was invaded due to the actions of the Taliban standing alone.

This study will now turn to the question of *opinio juris* to ascertain whether there is *opinio juris* to establish a legal belief for the purposes of forming a new custom.

7.2.2. Opinio Juris

Opinio juris as the subjective element is difficult to ascertain. On the one hand, one could look at the actions of the Security Council and its approval for the invasion of Afghanistan and argue that the element has been met due to the apparent legal backing of the act by the Security Council. However, this alone may not be enough as the situation has not been repeated to allow states to repeat their actions out of a sense of legal obligation.

As discussed in Chapter Two, determining the existence of *opinio juris* may be difficult as there is no test, per se, to determine whether states were acting out of a sense or belief that the state may be under a legal obligation to act, or the acts were accepted as legal.[114] Ascertaining why a state act is difficult to determine and may involve some modicum of the reading of tea leaves.[115]

The simplest method for ascertaining whether opinio juris is present would be to apply the standard that the ILC elucidates:

> 1. Evidence of acceptance as law (opinio juris) may take a wide range of forms.

---

114 Jo Lyn Slama, *Opinio Juris in Customary International Law*, 15 Okla. City Y. L. Rev. 603 (1990).

115 *Cf.*, Jack Goldsmith and Eric Posner, *The Limits of International Law* 24 (2005). ("Opinio juris is really a conclusion about a practice's status as international law; it does not explain how a widespread and uniform practice becomes law.")

> 2. Forms of evidence of acceptance as law (opinio juris) include, but are not limited to: public statements made on behalf of States; official publications; government legal opinions; diplomatic correspondence; decisions of national courts; treaty provisions; and conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference.[116]

Under the ILC one can find great support in the public statements, diplomatic correspondence, and conduct made by the security council members and other states as to the legality of the invasion of Afghanistan and the idea that the Taliban was responsible for the conduct of Al-Qaeda; as discussed *supra*. One may, under the ILC articulation, make a strong argument that opinio juris exist for the instant matter, however, as the presence of opinio juris is open to much debate further analysis is needed.

The ILA Reports, while discussing *opinio juris* in Rules 16-19, offers little as to how to determine its existence. Indeed, the ILA holds that demonstrating whether *opinio juris* exists is not necessary to the formation of custom.[117] As discussed in Chapter Two, other commentators have argued several mechanisms for determining *opinio juris* without universal acceptance of any theory. A review of pertinent ICJ case law reveals no test, per se, to determine the existence of opinio juris. The ICJ in the *North Sea Continental Shelf cases*[118], in discussing opinio juris stated:

> in order to achieve this result [of constituting *opinio juris*], two conditions must be fulfilled. Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, i.e., the existence of a subjective element, is implicit in the very notion of the *opinio juris sive necessitatis*. The States concerned must, therefore, feel that they are conforming to what amounts to a legal obligation. The frequency or even habitual character of the acts is not in itself enough. There are many international acts, e.g., in the field of ceremonial and protocol, which are performed almost invariably, but which are motivated only by considerations of courtesy, convenience or tradition, and not by any sense of legal duty.[119]

---

116 International Law Commission, *Identification of Customary International Law*, Draft Conclusion 10, U.N. Doc. A/CN.4/L.872 (30 May 2016). *Report of the International Law Commission*, 68th Sess., U.N. Doc. A/71/10 (2 May-10 June and 4 July-12 August 2016).

117 *Id*. R. 16.

118 North Sea Continental Shelf, Judgment, 1969 I.C.J. 3 (28 Feb.).

119 North Sea Continental Shelf, *supra* at 44 ¶77.

The ICJ in *Nicaragua* adopted its finding in the *North Sea Continental Shelf cases* holding that to analyze the opinio juris of an act; the court "has to appraise the relevant practice."[120] The court then explains:

> [i]t is not to be expected that in the practice of States the application of the rules in question should have been perfect...The Court does not consider that, for a rule to be established as customary, the corresponding practice must be in absolutely rigorous conformity with the rule. In order to deduce the existence of customary rules, the Court deems it sufficient that the conduct of States should, in general, be consistent with such rules, and that instances of State conduct inconsistent with a given rule should generally have been treated as breaches of that rule, not as indications of the recognition of a new rule. If a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule.[121]

Specifically addressing the opinio juris element, the court held that:

> to be satisfied that there exists in customary international law an *opinio juris* as to the binding character of [an act by a State]. This *opinio juris* may, though with al1 due caution, be deduced from *inter alia*, the attitude of the parties and the attitude of States toward [the act.] …It would therefore seem apparent that the attitude referred to expresses an *opinio juris* respecting such rule (or set of rules)…[122]

Taking the ICJ discussion on opinio juris together, it is apparent that to discern *opinio juris*, the party arguing for the existence of opinio juris must demonstrate that the parties subjectively believed that their actions were legal and that the acts were not prohibited as a matter of CIL.

Under ICJ case law, the subjective belief in the instant matter would, therefore, be demonstrated by the state's outward manifestation of the legality of the acts of attributing the conduct of Al-Qaeda to the Taliban as demonstrated by their verbal and physical acts in support thereof. In the instant matter, the approval of the attribution to the Taliban for the actions of Al-Qaeda, outside of the existing CIL of state responsibility as put forth by

---

120 Military and Paramilitary Activities in and Against Nicaragua (Nicar v. U.S.), 1986 I.C.J. 14 (June 27).

121 *Id.* at ¶186.

122 *Id.* at ¶188.

the ILC in the ARS, was demonstrated by the actions of those states in supporting the actions of the United States and its allies. Simply put, the Security Council and its members, NATO and its members, and all other states who took part in approved of or acquiesced to the military operations in Afghanistan in any manner demonstrated a subjective belief that these acts were legal.

It can be argued therefore that the opinio juris element is met. However, the argument of whether there was enough density or duration of practice again argues against the formation of custom. Based upon this doubt concerning density and duration state practice, it is doubtful that custom emerged as a result of the actions of the parties to the instant matter regarding their collective acts against the Taliban. As such, this study will turn to an analysis of alternative theories of formation for the purposes of discussion analysis. It is important to note, however, that as discussed *supra,* these theories are controversial and are not settled as a matter of international law.

7.2.3. Analysis Under Alternative Theories

In the alternative to the traditional formation of CIL, one may argue that the post-9/11 attacks created a new form of custom based solely upon the actions of states immediately after the 9/11 attacks. With the showing of *opinio juris* discussed *supra*, Cheng's theory, as discussed *supra* Chapter Two, on instant custom might be applicable here. It may be argued that the international response to 9/11, as evidenced by the acts of the Security Council and other states, created instant custom based solely on the demonstrated *opinio juris* by the actions of the Security Council, NATO, specially affected states, and a UN General Assembly resolution seemingly in favor of military intervention in Afghanistan,[123] along with the support of other states for the United States and its allies in Afghanistan, thus recognizing that the Taliban was responsible for the actions of Al-Qaeda as it was the Taliban and the state of Afghanistan which the international community was holding responsible.

This study believes that, while controversial, Cheng's instant custom theory is workable

123 *Condemnation of Terrorist Attacks in the United States of America*, G.A. Res. 56/1 (VIII), U.N. GAOR 55th Sess., U.N. Doc. A/Res/56/1 ¶¶ 3-4 (18 September 2001).

given the demonstrated *opinio juris*, and it also has a modicum of state practice. This study believes that in the face of a new type of terror attack, one arguably involving a weapon of mass destruction (in the form of commercial airliners), states reacted to create a new rule on attributing the conduct of a non-state actor or agent to the host state.

In many respects, it appears that the conduct of the United States and its allies was so far outside the customary rules of state responsibility as to ignore them entirely. The collective response to 9/11 was such as to set aside any legal reasoning and act out of necessity; the CIL existing at the time was insufficient to apply to the situation at that time. To that end, the collective states acted as the situation dictated, not as the customary law called for. In doing so, the states arguably created a new custom for holding states accountable for the acts of non-state actors.

Some argue that the initial use of force in self-defense was based upon Security Council authorization and this created a new custom for the use of force against non-state actors; such reasoning is inapplicable here. The Security Council ab initio linked the Taliban to the acts of Al-Qaeda due in part to the acquiescence of the Taliban to previous acts within the Taliban-controlled territory. The Security Council, as discussed *supra*, on three occasions prior to 9/11 called the Taliban to task concerning Al-Qaeda, imposing notice on the Taliban that the acts of Al-Qaeda were in violation of international law. This created a situation where the legality of acting post -9/11 was not, per se, considered: instead, the complicity of the Taliban was recognized based on the previous knowledge.

However, this study recognizes that the above-discussed theory lies at the fringe of international law, and traditional and formalist scholars would likely not be persuaded as to the formation of CIL. As such, this study will discuss Kirgis's sliding scale theory for the formation of CIL and the interpretation of the post-9/11 events by other scholars.

Kirgis's theory, as discussed *supra* Chapter Two, is based upon a sliding scale[124] consisting of varying ratio of state practice and *opinio juris*. Simply put, Kirgis theorized that the more of one constitutive element, the less of the other constitutive element that is needed. However, as there is no basis for quantifying the ratio of elements, or what the demarcation

124 *See id*., *supra* Chapter Two n. 111-118.

point is where custom blooms, Kirgis's theory is difficult to quantify. Kirgis's theory, like Cheng's, is not widely accepted by scholars, but Kirgis's theory is arguably more accepted, but that is the opinion of this study based on selected readings, and it is impossible to quantify to any exactitude.

As a theoretical construct, Kirgis's theory is attractive, particularly when discussing situations as presented in the instant discussion. That is where a situation is present where you have state practice and *opinio juris*, but with less than overwhelming proof of either element. Under Kirgis's theory, it may be enough to argue that you have both constitutive elements present, involving a large portion, albeit less than overwhelming, of states, engaging in the practice, but a seemingly larger number of states expressing *opinio juris* by the acts of the Security Council, NATO, specially affected states, or by supporting the UN General Assembly special resolution, in toto. One could argue that by utilizing Kirgis's theory, the act of attributing the conduct of Al-Qaeda to the Taliban established a new custom for the attribution of purely non-state conduct to a state. However, the question of the extensiveness of state practice would again cloud this assertion as it is difficult to say with any certainty whether state practice, in the single limited instance, was enough for custom to spring.

Under both Cheng's and Kirgis's theories, it is arguable that a new custom for attributing the conduct of a non-state actor to the host country was created by the actions of the United States and NATO post-9/11. However, the acts of the United States and NATO did not dispel the existing customary rules of state responsibility; they did, however, create an exception to the existing CIL of state responsibility. That is, a state will only be responsible for its own acts or those acts of its agents as elucidated by the ILC in the ARS. However, this rule now has a specific, rather narrow, exception.

7.2.4. A New Rule of Attribution?

The acts of the United States and its allies did not establish a new custom for overall state responsibility; that is, they did not displace the existing customary rule that a state, under normal conditions, will only be responsible for its own acts and that of its agents as put forth in the ARS. What the United States and its allies did, in the opinion of this study, was

establish a new exception to the existing customary rules of state responsibility. Just as a state may be responsible for those acts it adopts after the fact,[125] now it is arguable that a state will be held liable for the acts of a non-state actor if the state has prior notice of the non-state actor committing an internationally wrongful act and does not take actions to curtail the non-state actor or take steps to bring the non-state actor into compliance with international norms. This custom or duty is analogous to the holding of the *Corfu Channel* case where the court held that a state has a general duty not to allow its territory to be used to harm another state.[126] Here, though, the new custom is more specific and encompasses a specific notice requirement to the offending state.

The Taliban was held responsible for the acts of Al-Qaeda. Prior to holding the Taliban responsible, the Security Council attempted to engage the Taliban to gain the Taliban's compliance and assistance in bringing Al-Qaeda and its leadership to justice and stopping Al-Qaeda from committing acts of terrorism. This is demonstrated by the fact that: (1) The Taliban, as the de facto government of Afghanistan, had notice from the Security Council that it was harboring a terrorist organization in Al-Qaeda;[127] (2) the Security Council demanded that the Taliban turn over the leaders of Al-Qaeda to a state where the leaders had been lawfully indicted;[128] (3) the Taliban refused the Security Council's requests;[129] (4) the Security Council found that the presence of Al-Qaeda was a threat to international peace and security;[130] (5) Al-Qaeda attacked the United States, triggering the United States and the United Kingdom to invoke their Art. 51 right to self-defense with the acquiescence

---

125 See, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Art. 11, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

126 Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (April 9).

127 S.C. Res. 1193, U.N. Doc. S/RES/1193 (28 Aug. 1998). ("Deeply concerned also at the continuing presence of terrorists in the territory of Afghanistan…"). *See also*, S.C. Res. 1267, U.N. Doc. S/RES/1267 at ¶ 1(15 Oct. 1999). *See also*, S.C. Res. 1333, U.N. Doc. S/RES/1333 ¶1 (19 Dec. 2000).

128 S.C. Res. 1267 at ¶ 2, id. (The Security Council "[d]emands that the Taliban turn over Usama bin Laden without further delay to appropriate authorities…")

129 S.C. Res. 1333, U.N. Doc. S/RES/1333 ¶1 (19 Dec. 2000).

130 S.C. Res. 1214, U.N. Doc. S/RES/1214 (8 Dec. 1998). ("Deeply disturbed by the continuing use of Afghan territory, especially areas controlled by the Taliban, for the sheltering and training of terrorists and the planning of terrorist acts, and reiterating that the suppression of international terrorism is essential for the maintenance of international peace and security…")

of, if not approval of, the Security Council; (6) the United States offered an ultimatum for surrender, in compliance with the Security Council resolutions, of the Al-Qaeda leadership which the Taliban refused. Thus, the United States and its allies were prompted to invade Afghanistan in self-defense, thereby arguably creating a specific exception to the CIL of state responsibility.

This new exception to the CIL of state responsibility is premised upon a state failing to comply with international law and having lawful notice of the threat posed by its harboring a potential threat to international peace and security. Thereby, the harboring state, once it is placed on notice of the potential threat, is now responsible for the action taken by the threat group because it did not take steps to stop the threat.

It is the opinion of this study that custom may have sprung from the acts of the United States and its allies regarding holding a state responsible for the acts of non-state actors. It is recognized, however, that such a theory, as posited *supra*, lay at the edge of modern international law. Additionally, with little state practice to confirm this exception to the existing CIL, any definitive formation of a new custom is impossible to affirmatively state. This study will briefly analyze subsequent state practice to determine if CIL continues to bloom or if the issue remains static.

7.2.4.1. Subsequent State Practice in Support

There has been only one incident of state practice in support of holding states responsible for the acts of non-state actors since the 2001 invasion of Afghanistan. However, the single incident, the 2006 Israel intervention in Lebanon illustrates subsequent state practice.

This study will briefly discuss the Israel invasion of Lebanon in 2006 and its actions against the terrorist organization Hezbollah. This study will not delve into the past conflicts involving both these states as they are not germane to the instant issue other than to note Lebanon had not had true territorial integrity since 1978 and different terror groups such as Hamas, the PLO, and Hezbollah have used Lebanese territory in attacking Israel. This study focuses on the Hezbollah war of 2006 and will argue that actions of Israel towards Hezbollah support the theory posited supra that state responsibility had been altered, and that custom is blooming but not fully settled.

7.2.4.1.1. The Hezbollah War of 2006

The 2006 Lebanon War is similar to the invasion of Afghanistan in that a state acted against a non-state actor in the sovereign territory of another state; in the instant matter Israel, acting in claimed self-defense attacked Hezbollah terrorists in Lebanon. In addition, Israel claimed that both Lebanon and Iran were responsible for the actions of Hezbollah. Israel argued that since Hezbollah was a minority member of the Lebanese government and that Iran is the primary state sponsor of Hezbollah both states were responsible for the actions of Hezbollah. Israel had previously argued that

> were it not for the terrorism and its support infrastructure that operates with impunity from, and with the blessing and direct support of, these regimes [Lebanon and Iran], in violation of the most basic legal norms and explicit Security Council resolutions, Israeli measures of defense would be unnecessary…[131]

Israel seemingly has adopted the theory posited by this study that states are responsible for the actions of non-state actors within the territory of the state. This mindset by Israel lends credence to the theory that the CIL of attribution may have been altered post-9/11. It appears from the actions and claims of Israel that some states are seeking to hold states responsible for the actions of non-state actors within a states sovereign territory.

In respect to the Lebanon War of 2006, the claims of responsibility by Israel are a bit more complicated than those of the United States and its allies in respect to Afghanistan. This complication is due in part to the fact that members of Hezbollah were actually members of the Lebanese government, Lebanon did not have full control over its territory, and Israel did not seek to overthrow the government of Lebanon (the entire invasion was premised on the recovery of Israeli soldiers which had been kidnapped by Hezbollah), nor did Israel militarily pursue Iran; Israel sought only to establish a temporary buffer and rescue its kidnapped military members, the Hezbollah war is factually different. This study will briefly analyze the Lebanon war to demonstrate the instant issues.

On the night of July 12, 2006, during a combined arms attack by Hezbollah forces against

---

131 Letter Dated 17 November 2004 from the Permanent Representative of Israel to the United Nations, UN Doc. A/59/571 (2004).

Israeli territory, an Israeli military patrol was ambushed on the Israeli side of the border fence with Lebanon by Hezbollah fighters.[132] As a result of the Hezbollah ambush, three Israeli soldiers were killed, and two other soldiers were kidnapped by Hezbollah. Israel pursued the Hezbollah fighters in an attempt to recover the kidnapped soldiers but suffered further combat losses. Hezbollah subsequently attempted to ransom the kidnapped soldiers back to Israel in return for jailed Hezbollah fighters. Israel refused and launched military attacks against Hezbollah in Lebanon and initiated an air and naval blockade against parts of Lebanon. Israel subsequently invaded southern Lebanon and occupied limited territory until its withdrawal due to U.N. brokered cease-fire on 14 Aug. 2006.

Israel claimed that its actions in Lebanon were based on self-defense and invoked U.N. Charter art. 51 to justify its actions.[133] In addition, Israel sought to hold Lebanon responsible on the basis that Hezbollah was a part of the government of Lebanon. This position, re state responsibility on the basis of being part of the government, by Israel, in the opinion of this study is tenuous as Hezbollah controlled 14 out of 128 parliamentary seats. Having a minor part in a state's government and no direct control does not meet the requisite needed showing of control on behalf of Lebanon. However, the act of self-defense against non-state actors has been recognized by the Security Council in Res. 1368 and 1373 and arguably was a valid act on behalf of Israel. In addition, the actions of Israel in holding Lebanon responsible for the actions of Hezbollah support the theories posited herein that a state may be held responsible for the actions of non-state actors if the state has prior notice that the non-state actor has or is violating international law. Here Lebanon had prior notice of the threat Hezbollah posed to Lebanon itself and its neighbors. The Security Council in Res. 1559 (2004) had noted that armed militias in Lebanon such as Hezbollah was a threat to Lebanon and a threat to Lebanese territorial integrity. In S.C. Res.1680, the Security Council expressed its concern that arms were moving into Lebanese territory in an effort to arm militias such as Hezbollah (and many others it must be noted) that threatened both Lebanon and its neighbors.

---

132 *Identical Letters Dated 12 July 2006 from the Permanent Representative of Israel to the United Nations Addressed to the Secretary-General and the President of the Security Council*, G.A. A/60/937, S.C. A/2006/515 (12 Jul. 2006).

133 Letter Dated 12 July, *id.*

Lebanon had ample prior notice that Hezbollah posed an internal and external threat to Lebanon and its neighbors. When Lebanon failed to disarm Hezbollah, and allowed Hezbollah to act as an autonomous militia within its territory, Lebanon, in the opinion of this study, became complicit and responsible in part for the military actions taken by Hezbollah against Israel. Just as the Taliban were held responsible for the actions of al Qaeda. This idea was supported in part (aside from the claim that Lebanon's government was responsible as some of its parliament was Hezbollah members) by the claims of Israel and a majority of Security Council members.[134] However, as noted supra, Lebanon had not had true territorial integrity since at least 1978 and had been weakened by the intervention of Syria into Lebanese domestic affairs and was still dealing with the fallout of the Lebanese Civil War thus mitigating its complicity as Hezbollah and other non-state actors were acting independent of the government of Lebanon. That is, Lebanon was arguably in a worst position to deal with those non-state actors within its midst than the Taliban regarding al Qaeda.

As Israel invoked art. 51 against Lebanon on the basis that Lebanese territory was being utilized by non-state actors and sought to hold Lebanon responsible in-part, it supports the argument made herein that a state is responsible for the use of its sovereign territory that may harm another state, and that if a state has prior notice of non-state actors utilizing its sovereign territory the state may be held responsible for those acts. This subsequent state practice bolstering the claims made in this study. In the instant issue though, this theory is not fully supported by the acts of the Security Council, as instead of condoning Lebanon for its lack of action regarding the securing of its territory and preventing Hezbollah from taking action against Israel, the Security Council in S.C. Res. 1701 (2006) seems to defer blame from the Lebanese government and while not necessarily blaming Israel for its actions, does not explicitly support their invasion of Lebanon despite the obvious violation of art. 51. This is most likely due to the inability of Lebanon to secure its sovereign territory and the internal Security Council politics regarding Israel (Israel had isolated most of its supporters on the Security Council by its seeming disproportionate response and overwhelming use of force against civilians) but whatever the reason the lack of full endorsement for the actions of Israel regarding its invocation of art. 51 fails to support the

134 Ruys, *infra*.

theories posited herein.[135] At best the Israel actions support the theory posited herein but the lack of an endorsement by the Security Council for those actions detracts, so this study cannot invoke this state practice in the affirmative but at the same time it does not detract from the claims made herein either. As such, this study will continue to argue that the customary international law of state responsibility has been slightly altered by the holding of Afghanistan responsible for the actions of the Taliban outside of the CIL of state responsibility. However, this study acknowledges that this debate is far from settled.

7.3. Application to Malicious Cyber-Attacks

This exception to the existing rules of state responsibility would allow a state to be held responsible for the malicious cyber-attacks that originated from the state's cyberinfrastructure if the state had prior notice that its territory had been utilized as an initiation point for a malicious cyber-attack or an attack was traced to its territory and the state had not taken action, investigated the attack, or handed over the parties believed responsible for the requesting state or international body.

This exception to the existing rules of state responsibility is attractive in the cyber context as technical attribution to the IP level address in many cases is possible.[136] This attribution to the IP level, with a fair degree of confidence, allows the wounded state to seek out the state from which the attacks were initiated and seek out assistance to end the attacks. If the state whose territory has been used to initiate the attacks fails to cooperate then that state, under this theory, could be held responsible for the malicious cyber-attacks.

---

135 Per Ruys the Security Council debated the Israel-Lebanon conflict on 14 July 2006 and the majority of the Security Council supported Israel's invocation of art. 51 with only China and Qatar arguing that Israel was the aggressor. *See*, Ruys, *id*. at 270.

136 *See e.g.*, Robert Deibert, *The DHS/FBI Report on Russian Hacking was a Predictable Failure, Just Security* (Jan 4. 2017). https://justsecurity.org/35989/dhsfbi-report-russian-hacking-predictable-failure/. (Discussing how 40% of the exit IP nodes relating to the purported Russian hacking campaign against the U.S. elections were traced to Tor exit node IP addresses.)

This rule would greatly simplify the attribution of malicious cyber-attacks as the wounded state need only demonstrate a connection between the state and the state's cyber-territory and the state's failure to comply with stopping the attacks or handing over the parties responsible for the attacks for this theory to apply. As discussed in Chapter Six, a state need only cooperate with the injured state to stop the attacks or demonstrate that its territory was not utilized and the attacks were initiated from another state, or that the state from which the attacks did originate did not have the infrastructure in place to prevent the attacks.

Support for this rule may also be seen in current state practice of states in the cyber context. If we look at the actions of the United States, and other states[137] in regards to the attribution of malicious cyber-attacks, attribution appears to depend in large part on where the attack originated from.[138] Therefore, this study believes that this rule may be emerging as a matter of CIL for the purposes of holding states responsible for the use of their territory to the detriment of another state particularly for those acts occurring in cyberspace.

137 *See, e.g.,* James Scott*, It's the Russians!...Or Is It? Cold War Rhetoric in the Digital Age* (2017), http://icitech.org/its-the-russians-or-is-it-cold-war-rhetoric-in-the-digital-age/. (" It's common knowledge among even script kiddies that all one needs to do is compromise a system geolocated in Russia and use it as a beachhead for attack so that indicators of compromise lead back to Russia.")

138 *Id.*

Chapter Eight: Concluding Remarks: Where Do We Go From Here?

8. Conclusion

Chapter Eight concludes this study with a brief discussion regarding how the international community and individual states may prevent future malicious cyber-attacks. This study will briefly address two issues related to preventing malicious cyber-attacks, one, the idea of a cyberweapons treaty as a means to prevent cyber-attacks (both malicious and militarized) and the second, the idea of self-help and the theory of "hackingback" by states. This study will then conclude with a brief discussion on the study as a whole.

This study has demonstrated the difficulties involved with both technical and legal attribution of malicious cyber-attacks to the responsible state or non-state actor. As true legal or technical attribution is difficult, if not impossible, this study has put forth theories for holding states responsible for malicious cyber-attacks originating from a state's sovereign territory. This study has posited that there are alternative methods of achieving state responsibility which arguably would be more effective in preventing malicious cyber-attacks and helping to preserve international peace and security by diminishing the possibility of kinetic spillover resulting from malicious cyber-attacks.

However, the theories posited herein, standing alone, cannot be effectively implemented without international cooperation; it goes without saying that states are stronger when working together. How to best achieve the needed international cooperation is of great importance. This study will briefly address the issue of gaining international cooperation and preventing malicious cyber-attacks, whether through an outright ban on all forms of malicious cyber-attacks or whether a cyber weapons type treaty is a viable option.

8.1. Gaining International Cooperation: Is A Cyber Weapons Treaty Viable?

Many commentators have called for an arms control-style treaty for cyber weapons.[1] While such an idea is an attractive one, this study posits that banning or outlawing cyber weapons,[2] whether malicious or those that may rise to the level of U.N. Charter Art. 2(4) force, in itself, is not realistic or achievable. First, such a ban would have to be able to quantify and define what constitutes a cyber-attack. Hathaway et al. discussed the idea that states cannot seemingly agree as to what constitutes a cyber-attack, thus making it impossible to agree on a treaty.[3] Second, any ban would fall prey to the issues discussed *supra*, regarding both technical and legal attribution of malicious cyber-attacks. That is, irrespective of the legality of the act, if you cannot attribute the attack to the responsible state, it is moot whether or not the act was illegal (as discussed *supra*, this study contends that malicious cyber-attacks are an internationally wrongful act under CIL, hence already illegal without the need for an international treaty). In addition, such a treaty would bind state actors from such conduct as creating cyber weapons, leaving it to the individual state to ban such conduct domestically. Lastly, a cyber weapons ban would do nothing for the issues relating to malicious cyber-attacks as discussed in this study, as they are not, per se, militarized and are created in most instances by non-state actors and proxies.

Another theory for controlling malicious cyber-attacks, which focuses on the tools utilized by groups to create the tools for such attacks, has been put forth via the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and

---

1 Kenneth Geers, *Cyber Weapons Convention*, 26 Computer L. & Sec. R. 547 (2010). (Calling for a cyber weapons convention styled after the Chemical Weapon Convention.) *But cf.*, Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 Fletcher Sec. Rev. 55, 73 (Spring 2014). ("[T]here is little prospect for establishment of a treaty regime to deal with the use of proxy cyber actors. States that turn to them will be hesitant to embrace such a regime and, absent their consent, treaties do not bind states. Therefore, the reality is that states can only shape understanding of the current law through their practice.") *See also*, Stephan Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C.J. Int'l L. & Com. Reg. 223 (2014). Oona A. Hathaway, *et al., The Law of Cyber-Attack*, 100 Cal. L. Rev. 817, 881-884 (2012). Rex Hughes, *A Treaty For Cyberspace*, 86 Int'l Aff. 523 (2010).

2 Manish Singh, *US Govt <sic> Proposes to Classify Cybersecurity or Hacking Tools as Weapons of War* (n.d.) http://betanews.com/2015/05/23/us-govt-proposes-to-classify-cybersecurity-or-hacking-tools-as-weapons-of-war/.

3 Oona A. Hathaway, *et al., The Law of Cyber-Attack*, 100 Cal. L. Rev. 817, 881-884 (2012). Rex Hughes, *A Treaty For Cyberspace*, 86 Int'l Aff. 523 (2010).

Technologies (WA).[4] The forty-one states' members of the WA, have agreed to have certain cyber tools used mainly in zero-day exploits, IP surveillance, and intrusion software, listed and placed upon export control lists where purchasers would have to be licensed by states prior to purchasing. While this may be a step in the right direction, it suffers from multiple issues that must be addressed lest it harms legitimate researchers and end users of such tools.[5]

While the WA arrangement, in theory, is a good idea, it only would apply to those entities that are attempting to legitimately utilize security tools and ignores the reality of deep web exchanges where such tools are routinely bought and sold. In addition, zero-day exploits[6] are normally reported in journals, mass media, and specialized forums as soon as they are discovered, hence making the control of such information challenging at best. This attempt to regulate tools is, in theory, a good idea, but in reality, the control of information such as this goes against the very principles that the Internet is based upon, i.e., the free exchange of information and the control of information may operate as a prior restraint on information exchange and free speech and therefore be more dangerous than the danger it is trying to stop.

Additionally, ideas on control, as put forth by the WA, suffer from the same issues as similar treaties, that of the definitional challenges posed by controlling such tools through an international arrangement. The tools in the arrangement and prohibitions on transfer must be written as to be narrow enough to protect such tools from those with malicious

---

4 Bureau of Industry and Security, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, in,* Office of the Federal Register (United States) (May 20, 2015), https://www.federalregister.gov/articles/2015 /05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

5 Jennifer Granick, *Changes to Export Control Apply to Computer Exploits and More*, CIS Stanford (15 Jan. 2014), http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more.

6 *See,* Webopedia, *Zero-Day Exploit,* (n.d.), http://www.webopedia.com/TERM/Z/Zero_Day _exploit.html. (A zero-day exploit is "an exploit that takes advantage of a security vulnerability on the same day that the vulnerability becomes publicly or generally known. Zero-day exploits are usually posted by well-known hacker groups. Software companies may issue a security bulletin or advisory when the exploit becomes known, but companies may not be able to offer a patch to fix the vulnerability for some time after.")

intent, yet broad enough to allow for legitimate use by security researchers worldwide.[7] This issue may be addressed by the WA or written into a cyber security treaty as discussed *supra*.

While an in-depth exploration of the issues regarding a proposed cyber treaty and alternative control methods such as the WA is beyond the limits of this study, this study argues that in addition to states adopting the theories discussed *supra*, states need to embrace and expand international cooperation and the sharing of information regarding malicious cyber-attacks, the authors of said attacks, and the routes of transmission, much like what was put forth in the Convention on Cybercrime.[8] However, such international cooperation agreements would need to expand the definition of what constitutes a malicious cyber-attack; strengthen the cooperation between states and investigating agencies; establish an assistance program for underdeveloped states in regards to their cyber infrastructure and their technical abilities regarding cyber forensics; ensure that software providers provide timely and free patches to their software to ensure future security flaws are patched and ensure for continuing education of end users.[9] Again, this study holds that the only way to prevent further expansion of malicious cyber-attacks is through international cooperation.[10] However, it cannot be stressed enough though that any enforcement activity must be balanced against the freedom of expression and speech that the individual enjoys in international law.

The issues relating to malicious cyber-attacks and militarized cyber-attacks, in general, do not have a quick nor easy solution. As was discussed in Chapter Three, malicious cyber-

---

7 *See, id.* n.4. (Briefly discussing the need to protect legitimate researchers).

8 Council of Europe, Convention on Cyber Crime, ETS. 185 (23 Nov. 2001).

9 *See,* Benjamin Brake, *Strategic Risks of Ambiguity in Cyberspace*. Council on Foreign Relations, Contingency Planning Memo. No. 24, 4 (2015). ("Unilateral and bilateral steps offer the most immediate path for preventing and mitigating risks of ambiguity [for cyber-attacks]. Diverse interests and challenges that inhibit verification [attribution] limit the likelihood and effectiveness of a comprehensive international agreement in the near term.")

10 *But Cf.* Thomas Franck, *Iraq and the Law of Armed Conflict*, 80 Int'l L. Studies 16, 19 (2015). (Discussing terror financing legislation put into place by the United States and how other states may not implement the regime, as they do not feel the need to do so as they are not, per se, under the threat of terrorism.)

attacks respond and evolve just like their namesake biological viruses do; they adapt to the technology arranged against it. Like a biological virus, the best manner for containing such a pathogen is to constrain the possible number of hosts and to prevent transmission as much as possible. This idea translates to computer science, but it takes international cooperation and time. If the international community works together, this issue may be addressed and minimized, but if the international community does not address the issue through a treaty regime, the issues addressed herein will continue to get worse, and the likelihood of kinetic spillover will increase.[11]

Absent a united international community effort; states do have a range of options for confronting this issue via self-help either collectively or singularly. This study will briefly address the issue of self-help prior to concluding this study.

8.2. Self-Help for the Victim States

Countermeasures (self-help) are an important topic within the overall subject of both malicious and militarized cyber-attacks. There is much debate in the literature regarding how injured states may respond to malicious cyber-attacks (militarized cyber-attacks are subject to *jus ad bellum*/*jus in bello* principles and as such, will not be addressed herein). Countermeasures are legal responses to internationally wrongful acts and specifically addressed in Chapter II of the ARS and are subject to the CIL as put forth in the ARS. As discussed *supra* in Chapter Two of this study, while certain aspects of the CIL for state responsibility are unworkable in the cyber context, the majority of CIL is still applicable, and countermeasures are one of those areas where it applies fully.

States have an expectation that their sovereignty and people will be safe from unlawful acts arising from another state. As Franck posited:

> [w]hen that expectation is not met, there is moral force to the argument that those aggrieved by the failure should themselves be allowed to enforce their legal entitlement as best they can…self-help arises when, a state having refused

11 Benjamin Brake, *Strategic Risks of Ambiguity in Cyberspace.* Council on Foreign Relations, Contingency Planning Memo. No. 24, 4 (2015). ("Due to the difficulty of determining whether certain activity is intended for espionage or preparation for an attack, cyber operations run the risk of triggering unintended escalation.")

> to carry out its legal responsibilities and the international system having failed to enforce the law another state, victimized by that failure, takes countermeasures to protect its interests. [12]

The idea of self-help for states and to some extent, non-state actors[13] who are harmed by malicious cyber-attacks is much debated in the literature at present. Many commentators have focused on the idea of active defense against malicious cyber-attacks through self-help via the theory of hacking back or hackback, as a means available to states and non-state actors who are victims of malicious or militarized cyber-attacks.[14] Hackback is defined simply as the victim of a malicious cyber-attack attempting to trace the route of the cyber-attacks and hacking the IP addresses at the end of the attack through a variety of methods including the reverse use of the attack vector. That is, if the hacker is launching a DDoS attack, then the victim responds to the attacker with a DDoS attack of his or her own against the traced IP address or attempts to shut down the system at the end IP address through other means.

Kesan and Majuca posited that:

> Self-defense springs from the natural instinct for self-preservation and hackback should not be banned outright-it is generally accepted that one has the right to defend one's self and one's property and, towards this end, use reasonable force.[15]

Jayaswal, Yurcik, and Doss discussed the idea of hackback in 2002,[16] recognizing that an offensive response to active DDoS attacks or other malicious cyber-attacks might be a legal

---

12 Thomas Franck, *Recourse to Force: State Action Against Threats and Armed Attacks* 109 (2002).

13 *See, e.g.*, Martin Arnold, Tom Brathwaite, and Hannah Kuchler, *Davos 2015: Banks Call for Free Rein to Fight Cyber Crime*, Financial Times, (Jan. 22, 2015). http://www.ft.com /intl/cms/s/0/d94e855c-a209-11e4-bbb8-00144feab7de.html? siteedition=uk#axzz3bTTBru53. (Discussing the idea of active defense for banks, which would allow banks impacted by cybercrime to actively go after the hackers that attacked them without government oversight.)

14 *See e.g.*, Jay P. Kesan and Ruperto Majuca, *Optimal Hackback*, 84 Chi.–Kent L. Rev. 831 (2010). (Discussing theories of self-help "using reasonable force in self-defense against hackers…" in cyber law.) *See also*, Vikas Jayaswal, William Yurcik, and David Doss, *Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?*, 2002 Int'l Symp. Tech. & Soc. 380 (2002). Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 Mil. L. Rev. 1 (2009).

15 *Id.* at 833.

16 Vikas Jayaswal, William Yurcik, and David Doss, *Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?*, 2002 Int'l Symp. Tech. & Soc. 380 (2002).

and a practical response. However, as Jayaswal, Yurcik, and Doss stated (and as demonstrated by numerous other researchers since), the inability to accurately traceback the route and attribute the attacks make the theory of hackingback unworkable and potentially violative of international law. As the theory of hackingback suffers from the same attribution issues that this study has discussed in depth *supra*, this study rejects the theory in toto. This study recognizes that states have the right to respond to malicious or militarized cyber-attacks in self-defense and self-help. However, the responding state is subject to the same international law constraints that the attacker is violating and may not in return violate international law to stop the cyber-attacks.[17]

As commentators and states continue to promulgate theories regarding active defense and hackback via closer state and non-state actor cooperation in response to malicious cyber-attacks,[18] states must recognize that CIL must be adhered to and respected in relation to all types of conflict.

There are other forms of self-help available to states and non-state actors that are easily implemented, do not violate international law, and may stop the illegal activity. However, the theories put forth herein are a form of collective punishment that may impact a range of individuals whether guilty or not of participating in the cyber-attacks and may economically harm the entity attempting to stop the cyber-attacks. As such, the theories posited herein must be balanced against the need to stop malicious cyber-attacks versus the potential harm done.

The first theory is that of embargoing a range of IP addresses that a state or non-state actor has linked through recursive traceback to malicious cyber-attacks. A state may block all data traffic from a range of IP address from entering into its cyber infrastructure. Such actions would take coordination between a state and those stakeholding individuals who manage the flow of Internet traffic (depending on the state and its control over domestic

---

17 *See generally*, International Law Commission, *Draft Articles of Responsibility of States for International Wrongful Acts*, ch. II, arts.49-53, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

18 *See e.g.*, United States Department of Defense, *Department of Defense Cyber Strategy 2015*. (Discussing the need to coordinate and build partnerships both internationally and domestically to better respond to cyber threats.)

cyberinfrastructure). But it would enable states to protect its cyber infrastructure from attacks from a specific range of IP addresses associated with a specific geographical area. This idea is actively used in "greylisting"[19] and is easily implemented on an individual basis,[20] however, the concept, as used in this study, would expand the idea to all commercial activities within a state, therefore electronically embargoing a state from being able to access specific information and businesses within another state, thus encouraging the attacking state to take matters into their own hands and deal with the issue after the appropriate notice has been given by the blockading state.

Another method short of hackback or digitally embargoing/blockading a country would be to effectively slow all the data into or out of a country. This is theoretically possible as all data providers share the same Internet backbone, which is primarily controlled by major telecommunication companies (who ironically suffer major malicious cyber-attacks routinely). These providers have, until recently, worked under the jurisdiction of the United States. However, as it is presumed that the UN will assume control of Internet regulations, it is not beyond reason to think that the Security Council could, under UNC Art. 49, direct that states in which said corporations reside enforce a Security Council resolution to throttle down the bandwidth upstream and downstream of a state, effectively slowing all digital communication in order to get a state to comply. While this is purely theoretical, it is not beyond reason to believe that states may respond to malicious cyber-attacks short of force just as with any other countermeasure allowed in international law. A state does not have to resort to illegal acts such as hackingback to solve issues with non-compliant states. The issue, however, must be balanced against the individual's theoretical right to Internet access and freedom of expression.

States have a right to protect themselves and their domestic concerns but must do so in concordance with existing CIL. While this study posits that certain aspects of malicious cyber-attacks do not fit squarely within parts of the CIL for state responsibility, all other areas of CIL still control particular areas concerning self-help and self-defense.

---

19 Greylisting is a concept of blocking specific email addresses to prevent spamming of email.

20 *See e.g.*, Free BSD, Host Access (5), n.d., https://www.freebsd.org/cgi/man.cgi?query=hosts_access&sektion=5. (Discussing how to configure access/blocking based upon host name/address/user name.)

8.3. Study Conclusion

This study recognizes as Travalio and Altenburg posited, "[m]ost [S]tates have accepted, at least implicitly, a paradigm that recognized that the *Nicaragua*…case[] do[es] not reflect the prevailing standard of state accountability for [cyber-attacks]…"[21] While Travalio and Altenburg were discussing state responsibility for terror attacks and state support for terrorism,[22] this idea of the inapplicability of prevailing CIL to malicious cyber-attacks is a growing realization for states and commentators. This study recognizes this issue and posits multiple ways to hold states responsible for their own acts and the acts originating from within their sovereign territory.

This study holds that the existing CIL of state responsibility as put forth by the ILC in the ARS, does not allow for the anonymity or complexity of malicious cyber-attacks as a matter of CIL and as a pre-cyber age document; the ARS is not malleable enough, per se, to bring malicious cyber-attacks under the umbrella of CIL as put forth by the ILC regarding attribution and the effective control test. This study holds that the CIL put forth in the ARS is still applicable to kinetic state responsibility, but must be expanded to include the nuances and specialized needs of the digital age. As this study discussed in Chapter Seven, state practice post-9/11 has altered aspects of the CIL of state responsibility in response to a new style of terror group and attack. Consequently, state practice regarding malicious cyber-attacks will also evolve and alter the CIL applicable to it.

This study believes that until the ability to technically attribute a malicious cyber-attack (to the end user/state, not just to an IP address) is readily available, accurate, and accomplished in near real-time, states must have an alternative method of holding states responsible for malicious cyber-attacks via means of rough technical attribution or circumstantial attribution; that is, malicious cyber-attacks that are recursively traced to an originating IP address or are circumstantially attributed to a state. This alternative method of state

21 Greg Travalio and John Altenburg, *Terrorism, State Responsibility, and the Use of Military Force*, 4 Chi. J. Int'l L. 97, 119 (2003).

22 *See generally, id.*

responsibility is one of strict liability. States should be held responsible for malicious cyber-attacks that originate from within their domestic cyberinfrastructure, just as they would be for any other harm that would originate from their territory if it were something other than a cyber-attack. This study holds that there should be no differentiation between kinetic harms and cyber-harms and as such, embraces the theories posited in customary international environmental law and CIL and applied them to the problem of malicious cyber-attacks. This theory of strict liability, however, is not absolute, as a state has an affirmative defense if it can show that the accused cyber-attacks did not originate from its territory, or if it is able to show that it does not have the technical ability to detect or prevent cyber-attacks.

This study argues that the primary focus for holding a state responsible for malicious cyber-attacks is the harm that the malicious cyber-attacks cost in kinetic and digital terms. The harms caused by malicious cyber-attacks are tangible; whether through monetary loss, loss of privileged information, loss of personal information, or the loss of confidence in a system, states, and their citizens are harmed by malicious cyber-attacks. As such, malicious cyber-attacks create a real cause of concern for injured states and increase the likelihood for kinetic overflow from purely cyber-attacks, as states may be forced to respond with force to stop the continued harm, thus creating an impetus for the international community to act.

A key to holding states responsible is the knowledge that cyber-attacks are originating from a state's territory. As discussed in Chapter Six, CIL has evolved to where states may incur responsibility for the acts of non-state actors when the state has a knowledge of the acts of the non-state actor and does not prevent further acts. As discussed in Chapter Five, this study argues that CIL post-9/11 is evolving to embrace this idea of knowledge as a precursor to state responsibility, particularly when accompanied by demand from the injured state or states that the harboring state takes action. If the harboring state refuses to take action, then the injured state may, in concordance with existing IHL and CIL, take action to bring the harboring state into compliance with its international obligations.

Finally, this study has demonstrated that a state has a duty to prevent malicious cyber-attacks. This duty to prevent, however, is not an absolute duty as it is dependent upon the states' technical abilities to identify and stop the actors behind the malicious cyber-attacks.

This study holds that states have a duty to prevent malicious cyber-attacks, and failure through either an act or an omission makes a state responsible for the malicious cyber-attack, conditioned on the technical ability of the state. To this end, other states who have the technical abilities to identify and prevent malicious cyber-attacks should offer aid and training to those states that do not, as it is in the best interest of the international community to enhance all states' abilities to prevent malicious cyber-attacks.

In conclusion, this study holds that malicious cyber-attacks are an important, but often overlooked aspect of international cyber security law. While the focus of the international community has been, and seemingly continues to be, on the threat of cyber warfare, a real and immediate danger to international peace and security is being greatly ignored. The international community must address the issues relating to malicious cyber-attacks and hold states responsible so as to ensure that one potential trigger for cyber warfare is removed.

Bibliography

Aghaei-Foroushani, Vahid, and A. Nur Zincit-Heywood, Deterministic Flow Marking for IPV6 Traceback *1, Network and Service Management (CNSM), 11th Int'l Conf. on IEEE (2015), https://www.semanticscholar.org/paper/Deterministic-flow-marking-for-IPv6-traceback-DFM6-Foroushani-Zincir-Heywood/ 49c12809fb3776bda0260aef561d3f8924463 517/pdf.

Al Jazeera, *Fatah and Hamas to Form Unity Government* (18 Jan. 2017), http://www.aljazeera.com/news/ 2017/01/ fatah-hamas-form-unity-government-17011803 1339203.html

Allan, Collin S., *Attribution Issues in Cyberspace*, 14 Chi-Kent J. Int'l & Comp. L. 56(2014).

Allen, Laymen E. & C. Rudy Engholm, *The Need for Clear Structure in "Plain Language" Legal Drafting*, 13 U. Mich. J. L. Reform 455 (1980).

Amanpour, Christine, *America Under Attack: Talk with French President Jacques Chirac* (Transcript), (Sept. 13, 2001), http://archives.cnn.com/ TRANSCRIPTS/0109/13/se.31.html.

Anderson, Nate, *Massive DDOS Attacks Target Estonia; Russia Accused*, ARS Technica (May 14, 2007), http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/.

Andress, Jason, and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners* (2011).

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 2007 I.C.J. Rep. (26 Feb. 2007).

Arimatsu, Louis, *The Law of State Responsibility in Relation to Border Crossings: An Ignored Legal Paradigm*, 89 Int'l L. Studies 21, 36 (2013).

Arnold, Martin, Tom Brathwaite, and Hannah Kuchler, Davos 2015: *Banks Call for Free Rein to Fight Cyber Crime*, Financial Times, (Jan. 22, 2015). http://www.ft.com/intl/cms/s/0/d94e855c-a209-11e4-bbb8-00144feab7de.html?siteedition=uk#axzz3bTTBru53.

Ashmore, William C., *Impact of Alleged Russian Cyber Attacks* (2009).

Associated Press*, A Look at Estonia's Cyber Attack in 2007*, NBC News (http://www.nbcnews.com/id/ 31801246/ ns/technology_and_science-security/t/look-estonias-cyber-attack/#. V2BUFjZdE2x).

Aust, Anthony, *Handbook of International Law* (2nd ed. 2011).

Avena and Other Mexican Nationals (Mex. v. U.S.A), Judgment, 2004 I.C.J. Rep. 12.

Back in Time: Russian Agency Seeks Typewriters for Secret Documents, Spiegel Online International (July 11, 2013), http://www.spiegel.de/international/ world/russian-intelligence-seeks-typewriters-for-secret-documents-a-910677.html

Baena Ricardo et al., Judgment, Inter-Am. Ct. H.R., (Ser. C) No. 104, ¶ 102 (November 28, 2003).

Banks, William C., *Developing Norms for Cyber Conflict, in*, Research Handbook on Remote Warfare (Forthcoming), (J. Ohlin ed, 2016), http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2736456.

Beal, Vangie, *Internet*, Webopedia (2014), http://www.webopedia.com/ TERM/I/Internet.html.

Bears in the Midst: Intrusion into the Democratic National Committee, CrowdStrike (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Bencsáth, Boldizsár, *Duqu, Flame, Gauss: Followers of Stuxnet* (Presentation), RSA Conf. Eur. (2012), http://www.rsaconference.com/writable/presentations /file_upload/br-208_bencsath.pdf.

Bishop, Matt, Carrie Gates, and Jeffrey Hunker, *The Sisterhood of the Traveling Packets*, 59 Proceedings of the Workshop on New Security Paradigms (Sept. 2009).

Black's Law Dictionary, 9th ed. (2011).

Boebert, W. Earl, *A Survey of Challenges in Attribution*, 41 Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy (2010).

Borda, Aldo Zammit, *A Formal Approach to Article 38(1)(d) of the ICJ Statute from the perspective of the International Criminal Courts and Tribunals*, 24 Eur. J. Int'l L. 649 (2013).

Boyle, Alan E., *State Responsibility and International Liability for Injurious Consequences of Acts Not Prohibited by International Law: A Necessary Distinction?* 39 Int'l Comp. L. Q. 1, 13 (1990)

Brake, Benjamin, *Strategic Risks of Ambiguity in Cyberspace*, Council on Foreign Relations, Contingency Planning Memo. No. 24, 4 (2015).

Bratspies Rebecca M., and Russell A. Miller, *Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration* (2006).

British Broadcasting Corp., *Georgia Profile – Timeline*, (December 24, 2014), http://www.bbc.com/ news/world-europe-17303471.

British Victims of September 11, The Guardian (10 Sept. 2002), http://www.theguardian.com/ world/2002/sep/10/september11.uk.

Brown, Gary and Keira Poellet, *The Customary International Law of Cyberspace*, Strategic Studies Quarterly 126 (Fall 2012).

Brown, Gary D., *What International Humanitarian Law Gets Wrong About Cyber Warfare*, Seminar Presentation, University of Glasgow (10 June 2014).

Brown, Marshall, *The Rights of States Under International Law*, 26 Yale L. J. 85 (1916).

Brown, Phillip Marshall, *The Rights of States Under International Law*, 26 Yale L. J. 85 (1916).

Brownlie, Ian, *Principles of Public International Law* (6th ed. 2003).

Brownlie, Ian, State Responsibility and the ICJ, in, The Clifford Chance Lectures Vol. II: Issues of State Responsibility Before International Judicial Institution (7 ed., 2004).

Brownlie, Ian, *System of the Law of Nations State Responsibility* (Part I) 36 (1983).

Buchan, Russell, *Cyber Espionage and International Law, in, Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias & Russell Buchan eds., 2015).

Buchholz, Florian P., and Clay Shields, *Providing Process Origin Information to Aid in Network Traceback*, 1 CERIAS Tech Report 2002-22, Center for Education and Research in Information Assurance and Security (2002).

Bureau of Industry and Security, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, in*, Office of the Federal Register (United States) (May 20, 2015), https://www.federalregister.gov/ articles/2015 /05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

Burton, Kelly, *The Conficker Worm* (n.d.), https://www.sans.org/security-resources/malwarefaq/conficker-worm.php. National Public Radio, The Worm That Could Bring Down the Internet (Sep. 27, 2011), http://www.npr.org/2011/09/ 27/140704494 /the-conficker-worm/

Bush, George W., *The Collected Speeches of George W. Bush* (2013).

Caron, David D., *The ILC Articles on State Responsibility: The Paradoxical Relationship Between Form and Authority*, 96 Am. J. Int'l L. 857 (2002).

Carr, Jeffrey, *Responsible Attribution: A Prerequisite for Accountability* 1, Tallinn Paper No. 6 (2014).

Carroll, Ward, *Israel's Cyber Shot at Syria*, DefenseTech (Nov. 26, 2007), http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/.

Case Concerning Avena and Other Mexican Nationals (Mex. V. USA), 2008 Gen. List (16 July).

Case Concerning the Difference Between New Zealand and France Concerning the Interpretation or Application of Two agreements, concluded on 9 July 1986 Between the Two States and Which Related to the Problems Arising from the Rainbow Warrior Affair, XX Rep. Int'l Arbitral Awards 215 (30 Apr. 1990).

Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. US), 1986 I.C.J. 4 (June 27).

Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia) 1997 I.C.J. Rep. 7 (Sep. 25).

Cassese, Antonio, *International Law* (2nd ed. 2005).

Cassese, Antonio. *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 Eur. J. Int'l L. 649 (2007).

Chaliand, Gerard & Arnaud Blind, *Zealots and Assassins 55-57, in, The History of Terrorism: From Antiquity to Al Qaeda* (Gerard Chaliand ed., 2007).

Charme, Joni S., *Transnational Injury and Ultra-Hazardous Activity: An Emerging Norm of International Strict Liability*, 4 J. L. & Tech. 75(1989).

Charter of the United Nations (1949).

Cheng, Bin, *United Nations Resolutions on Outer Space: "Instant" International Customary Law*, 5 Indian J. Int'l L. 23 (1965).

Christenson, Gordan A., *Attributing Acts of Omission to the State*, 23 Mich. J. Int'l L. 312 (1990).

Clark, David D., and Susan Landau, *Untangling Attribution*, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010).

Clutterbuck, Lindsay, *The Transatlantic Impact of 9/11* (Sept. 13, 2011), The Rand Corp., http://www.rand.org/blog/2011/09/the-transatlantic-impact-of-911.html.

Combating the Criminal Misuse of Information Technologies, G.A. Res. 55/63 ¶ 1 (A-J) (22 Jan. 2001).

Comer, Douglas E., *Internetworking with TCP/IP, Principles, Protocols and Architecture* (5th ed. 2006).

Comments of President Barack Obama, Joint Press Conference by President Barack Obama of the United States and President Xi Jinping of China (25 Sep. 2015), http://www.cctv-america.com/ 2015/09/25/full-text-of-presidents-obama-and-xis-joint-press-conference-during-state-visit.

Condemnation of Terrorist Attacks in the United States of America, G.A. Res. 56/1 (VIII), U.N. GAOR 55th Sess., U.N. Doc. A/Res/56/1 (18 September 2001).

Condorelli, Luigi, and Claus Kress, *The Rules of Attribution: General Considerations, in*, The Law of International Responsibility 221 (James Crawford, Alain Pellet, and Simon Olleson ed. 2010)

Consolidated Rail Corp. v. Gottshall, 512 U.S. 532 (1994).

Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 974 U.N.T.S. 14118 (23 Sept. 1971).

Convention on Cybercrime, ETS No., 185 (2001).

Convention on the Prevention and Punishment of the Crime of Genocide, 78 U.N.T.S. 277 (12 Jan. 1951).

Convention to Prevent and Punish the Acts of Terrorism Taking Form of Crimes Against Persons and Related Extortion That Are of International Significance, OAS Treaty Series, no. 37, 27 U.S.T.S. 3949 (2 Feb. 1971).

Cook, Alan, et al., *Attribution of Cyber Attacks on Industrial Control Systems*, ICST Transactions (Preprint) (2017).

Corfu Channel Case (U.K. v. Alb.) Judgment, 1949 I.C.J. Rep. 4 (April 9).

Council of Foreign Relations, US Led Attack on Afghanistan Begins (n.d.), http://www.history.com/this-day-in-history/us-led-attack-on-afghanistan-begins.

Covenant of the League of Nations (28 June 1919).

Crawford, James, *Brownlie's Principles of Public International Law* (8th ed. 2012).

Crawford, James, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (2002).

Criminal Complaint, *United States v. Su Bin*, Case No. 14-1318M (C. D. Cal. June 27, 2014).

D'Amato, Anthony, *The Concept of Custom in International Law* (1971).

D'Amato, Anthony, Transboundary Pollution (2001), http://anthonydamato.law.northwestern.edu /IELA/Intech08-2001-edited.pdf.

D'Amato, Anthony, *Trashing International Law*, 81 Am. J. Int'l L. 101 (1987).

Dahlman, Christian, *The Function of Opinio Juris in Customary International Law*, 81 Nordic J. Intl L. 327 (2012

Daily, James, *Is Batman a State Actor? Law and the Multiverse* (Nov. 30, 2010), http://lawandthemultiverse.com/2010/11/30/is-batman-a-state-actor/.

Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Outer Space, G.A. Res. 1962 (XVIII), U.N. GAOR, 18th Sess., U.N. Doc. A/5656 (13 Dec. 1963).

Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/25/2625 (24 Oct. 1970).

Deeks, Ashley, *The Geography of Cyber Conflict: Through A Glass Darkly*, 89 Int'l L. Studies 1 (2013).

Deibert, Robert, *The DHS/FBI Report on Russian Hacking was a Predictable Failure, Just Security* (Jan 4. 2017). https://justsecurity.org/35989/dhsfbi-report-russian-hacking-predictable-failure/.

De Hoogh, Andre J.J., *Article 4 and 8 of the 2001 ILC Articles on State Responsibility, The Tadic Case and Attribution of Acts of Bosnia Serb Authorities to the Federal Republic of Yugoslavia*, 72 Brit. Y.B. Int'l L. 255 (2002).

deLisle, Jacques, *9/11 and U.S.–China Relations*, Foreign Policy Research Inst. (Sept. 2001), http://www.fpri.org/enotes/2011/201109.delisle.911.html#note2.

Digital Forensic Investigator (DFI) News, *Increase in Strange Traffic, Cyber Attacks Utilizing Tor* (Oct. 31, 2013), http://www.dfinews.com/news/2013/10/ increase-strange-traffic-cyber-attacks-utilizing-tor.

Dinham, Abby, *Hackers 'Recycling Code' to Spread Worms*, ZDNet (June 1, 2004), http://www.zdnet.com/article/hackers-recycling-code-to-spread-worms/.

Douligeris, Christos, and Aikaterini Mitrokotsa, *DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art*, 44 Computer Networks 643, (2004).

Draft Articles on Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

Draft Declaration on Rights and Duties of States G.A. Res. 375(IV) (6 Dec. 1949).

Drumbl, Mark A., *The Taliban's 'Other' Crimes*, 23 Third World Qrtl'y 1121 (2003).

Dupuy, Pierre-Marie, & Cristina Hoss, *Trail Smelter and Terrorism: International Mechanisms to Combat Transboundary Harm, in*, Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration 225 (Rebecca M. Bratspies & Russell A. Miller eds. 2006).

Economides, Constantin P., *Content of the Obligation: Obligations of Means and Obligations of Results, in*, The Law of International Responsibility 378 (James Crawford, Alain Pellet, and Simon Olledon eds. 2010).

Electronic Frontier Foundation, *State Sponsored Malware* (n.d.), https://www.eff.org/issues/state-sponsored-malware.

Ellen Nakashima, The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace, Wash. Post. (Sep. 25, 2015), https://www.washingtonpost.com /world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9edce8a2a2a679_story.html? Wpisrc =al_alert-COMBO-world%252Bnation.

Estes, Adam Clark, *The Sony Pictures Hack Was Worse than Everyone Thought*, *Gizmodo*, (Dec. 3, 2014), http://gizmodo.com/the-sony-pictures-hack-exposed-budgets-layoffs-and-3-1665739357/1666122 168.

Evans v. Newton, 382 U.S. 296, 299 (1966).

Falliere, Nicolas, Liam O Murchu, and Eric Chien, *W.32 Stuxnet Dossier v1.4*, Symantec (Feb. 2011).

Federal Assembly of the Russian Federation Resolution by the State Duma, *On the Struggle Against International Terrorism* (Sept. 19, 2001), http://www.mid.ru/bdomp/brp_ 4.nsf/e78a48070f128a7b43 256999005bcbb3/489a88b06710998d43 256ad1 0056 f420!OpenDocument.

Fellmeth, Aaron X., and Maurice Horwitz, *Guide to Latin in International Law* (2011).

Flook, Kara, *Russia and the Cyber Threat*, AEI (May 13, 2009), http://www.criticalthreats.org/russia/russia-and-cyber-threat.

Follath. Erich, and Holger Stark, *The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor*, Spiegel, (Nov. 2, 2009), http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

Franck, Thomas, *Iraq and the Law of Armed Conflict*, 80 Int'l L. Studies 16 (2015).

Franck, Thomas, *Recourse to Force: State Action Against Threats and Armed Attacks* 109 (2002).

Free BSD, *Host Access* , n.d., https://www.freebsd.org/cgi/man.cgi?query= hosts_access&sektion=5.

Frizell, Sam, *Off the Battlefield, Hackers Are Waging Cyberwar Against Israel and Palestine*, TIME (Aug. 7, 2014), http://time.com/3089473/israel-gaza-hackers/.

Fry, James D., *Coercion, Causation, and the Fictional Elements of State Responsibility*, 40 Vand. J. Transnat'l L. 611, 612 (2007).

G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/RES/56/10 (Dec. 12, 2001).

G.A. Res. A/49/60, *Declaration on Measures to Eliminate International Terrorism* (09 Dec. 1994).

Gabčíkovo-Nagymaros Project (Hun. / Slov.), Judgment, 1997. I..C..J. 7 (25 Sept.).

Gallagher, Sean, *Sony Pictures Hack Gets Uglier; North Korea Won't Deny Responsibility,* ARS Technica, (Dec. 2, 2014), http://arstechnica.com/security/ 2014/12/sony-pictures-hack-gets-uglier-north-korea-wont-deny-responsibility/.

Gao, Zhiqianq, and Nirwan Ansari, *Tracing Cyber Attacks from The Practical Perspective*, IEEE Comm. Mag. (May 2005).

Garrie, Daniel, and Shane R. Reeves, *So You're Telling Me There's a Chance: How the Articles on State Responsibility Could Empower Corporate Responses to State-Sponsored Cyber Attacks*, Harv. Nat. Sec. J. 10-12 (Dec. 17, 2015), http://harvardnsj.org/2015/12/so-youre-telling-me-theres-a-chance-how-the-articles-on-state-responsibility-could-empower-corporate-responses-to-state-sponsored-cyber-attacks/.

Greenwood, Christopher, *International Law and the 'War on Terrorism*.' 78 Int'l Aff. 301 (2002).

Geers, Kenneth, *Cyber Weapons Convention*, 26 Computer L. & Sec. R. 547 (2010).

Geiß, Robin, and Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus Away from Military Response Toward Non-Forcible Countermeasures and Collective threat-Prevention, in,* Peacetime Regime for State Activities in Cyberspace: International Law, International Relations, and Diplomacy (Katharina Ziolkowski ed. 2013).

Gerdwin-Meyer, Tony, *What Probability is Involved in "Beyond Reasonable Doubt" in Criminal Trials?* Kings College London (2014), http://www.ucl.ac.uk/ ~ucgbarg/doubt.htm.

Goldsmith, Jack L. & Eric A. Posner, *The Limits of International Law* (2005).

Goldsmith, Jack, *The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance*, LAWFARE (Dec. 19, 2014), https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance.

Goldsmith, Jack, *Yet More Thoughts on the DNC Hack: Attribution and Precedent*, LAWFARE, (July 27, 2016), https://www.lawfareblog.com/yet-more-thoughts-dnc-hack-attribution-and-precedent.

Gong, Ghao, Trinh Le, T. Korkmaz, and K. Sarac, *Single Packet IP Traceback in AS-Level Partial Deployment Scenario, in*, Proceedings of the IEEE Globocom (2005).

Goodin, Dan, *Researchers Crack Open Unusually Advanced Malware That Hid for 5 Years*, ArsTechnica (08 Aug., 2016), http://arstechnica.com/ security/2016/08/researchers-crack-open-unusually-advanced-malware-that-hid-for-5-years/.

Gorman, Siobhan, *Annual U.S. Cybercrime Costs Estimated at $100 Billion*, Wall St. J. (July 22, 2013), http://www.wsj.com/articles/SB1000142412788 73243289045 7862 1880966242990.

Graeme Wearden, BP Oil Spill Costs to Hit £40-billion, The Guardian (2 Nov. 2010), http://www.theguardian.com/business/2010/nov/02/bp-oil-spill-costs-40-billion-dollars.

Graham, David E., *Cyber Threats and the Law of War*, 4 J. Nat. Sec. L. & Pol. 87 (2010).

Greenwood, Christopher, *Sources of International Law: An Introduction* (2008), http://untreaty.un.org/cod/avl/pdf/ls/ greenwood_outline.pdf.

Gross, Laurence M., *The Legal Implications of Israel's 1982 Invasion into Lebanon*, 13 Cal. W. Int'l L. J. 458 (1983).

Grotius, Hugo, *On The Law of War and Peace*, Bk. 2 (A.C. Campbell trans. 1814).

Gutteridge, H.C., *The Meaning of Article 38(1) of the Statute of the International Court of Justice*, 38 Problems of Public and Private Int'l L. 125 (1952).

Guzman, Andrew T., *Saving Customary International Law*, 27 Mich. J. Int'l L. 115, 157-159 (2006). (Discussing that custom needs some span of time to form.)

Hagen, Andreas, *The Russo-Georgian War 2008, in*, A Fierce Domain: Conflict in Cyberspace, 1986-2012, 196 (Jason Healey ed., 2013).

Harper, Jacob M., *Technology, Politics, and the New Space Race: The Legality and Desirability of Bush's National Space Policy Under the Public and Customary International Laws of Space*, 8 Chi. J. Int'l L. 681, 690-691 (2010). (

Harris, Shane, *U.S. Poised to Indict China's Hackers for Cyber Blitz, The Daily Beast*, Sept. 9, 2015, http://www.thedailybeast.com/articles/2015/09/09/u-s-poised-to-indict-china-s-hackers-for-cyber-blitz.html.

Hathaway, Oona A., et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817 (2012).

Hathaway, Oona A., et al., *Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors*, 95 Tex. L. Rev. 539, 545-547 (2017).

Healey, Jason, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council Issue Brief (2011).

Healey, Jason, *Concluding Assessment*, in A Fierce Domain: Conflict in Cyberspace 1986 to 2012 (2013 Jason Healey ed.).

Heathcote, Sarah, *State Omissions and Due Diligence, in*, The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case (Karine Bannelier, Theodore Christakis, and Sarah Heathcote eds. 2012).

Herzog, Stephen, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 J. Strategic Sec. 49 (2011).

Hess, Charlotte, *The Virtual CPR: The Internet as a Local and Global Common Pool Resource* (May 1995), http://dlc.dlib.indiana.edu/dlc/bitstream /handle/10535/234/ iascp-95-II.pdf?sequence=1.

Hessbruegge, Jan Arno, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. Int'l L. & Pol. 265 (2003-2004).

Hollis, David, *Cyberwar Case Study: Georgia 2008*, Small Wars J. (2011), http://smallwarsjournal.com /blog/journal/docs-temp/639-hollis.pdf.

Hughes, Rex, *A Treaty for Cyberspace*, 86 Int'l Aff. 523 (2010), DOI:10.1111/j.1468-2346.2010.00894.x.

Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/20/L.13 (June 29, 2012).

ICANN, *A Beginners Guide to Internet Protocol Addresses* (n.d.).

Inclan, Javier, *Advanced Malware Detection Through Threat Intelligence*, HP (2014).

Ingersoll, Geoffrey, *Cyber Attack On Tor Could Contain A Secret Message From The NSA*, Business Week (Aug 5, 2013), http://www.businessinsider.com/tor-exploit-leads-right-back-to-the-nsa-2013-8#ixzz2wGQ2IFQf).

International Co-operation in the Peaceful Uses of Outer Space, G.A. Res. 1721 (XVI), U.N. GAOR, 16th Sess., Annex., U.N. Doc. A/5026 (20 Dec. 1961).

International Law Association, ILA Study Group on Due Diligence in International Law First Report (07 Mar 2014).

International Law Associations Committee on Formation of Customary (General) International Law, Statement of Principles Applicable to the Formation of General Customary Law (as amended by the London Conference)(2000).

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, U.N.G.A. A/56/10 (2001).

International Law Commission, Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities, U.N. GAOR, 53rd Sess. at 148, U.N. Doc. A/56/10 (2001).

International Law Commission, Draft Code of Offences Against the Peace and Security of Mankind, 2 Yrbk Int'l L. Comm. 134 (1951).

International Law Commission, Identification of Customary International Law, Draft Conclusions, U.N. Doc. A/CN.4/L.872 (30 May 2016).

Internet Growth Statistics, *The Global Village Online* (15 Sept 2015), http://www.internetworldstats .com/emarketing.htm

Jamnejad. Maziar, and Michael Wood, *The Principle of Non-Intervention*, 22 Leiden J. Int'l L. 345 (2009).

Jayakumar, Kirthi, *Where Does Article 38 Stand Today?*, E-Ir, (Oct. 12 2011), http://www.e-ir.info/2011/10/12/where-does-article-38-stand-today.

Jayaswal, Vikas, William Yurcik, and David Doss, *Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?*, 2002 Int'l Symp. Tech. & Soc. 380 (2002).

Jennifer Granick, Changes to Export Control Apply to Computer Exploits and More, CIS Stanford (15 Jan. 2014), http://cyberlaw.stanford.edu/publications/ changes-export-control-arrangement-apply-

Jensen, Eric Talbot. *State Obligations in Cyber Operations*, (April 2, 2014). Baltic Y.B. Int'l., forthcoming. Available at SSRN: http://ssrn.com/abstract=2419527 (cited with author's permission).

Joel Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare *548 (Kindle ed. 2011).

Joint Chiefs of Staff, *Joint Terminology for Cyberspace Operations*, attch. I, Cyberspace Operations Lexicon, Department of Defense (2009).

Joint Press Conference by President Barack Obama of the United States and President Xi Jinping of China (25 Sep. 2015), http://www.cctv-america.com/ 2015/09/25/full-text-of-presidents-obama-and-xis-joint-press-conference-during-state-visit.

Joshua, Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

Kammerhofer, Jörg, *Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems*, 15 Eur. J. Int'l L. 523 (2004).

Kane, Robert B., *The Corfu Incident 1923*, *in*, War in the Balkans: An Encyclopedic History from the Fall of the Ottoman Empire to the Breakup of Yugoslavia (Richard C. Hall ed., 2014).

Kansas v. Colorado, 185 U.S. 125 (1902).

Kaspersky Lab, *Regin: Nation-state Ownage of GSM Networks* (Nov. 24, 2014), https://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/.

Kaspersky Labs, *Kaspersky Security Bulletin 2012: Cyber Weapons* (18 Dec. 2012), https://www.securelist.com/en/analysis/204792257/Kaspersky_Security _Bulletin_2012_Cyber_Weapons.

Keegan, Rebecca, *Sony Hack 'Unprecedented, Damaging and Unique' Cyber Security Firm Says*, L.A. Times, (Dec. 6 2014), http://www.latimes. com/ entertainment/envelope/cotown/la-et-ct-sony-hack-20141206-story.html

Keizer, Greg, *Why Did the Stuxnet Worm Spread?*, ComputerWorld, (Oct. 1, 2010), http://www.computerworld.com/article/ 2516109/security0/why-did-stuxnet-worm-spread-.html.

Kelsey, Jeffrey T. G., *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 Mich. L. Rev. 1427 (2008).

Kerr, Dara, *Ferguson, Mo., Police Site Hit with DDoS Attack*, CNET (Aug. 14, 2014), https://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/.

Kesan, Jay P., and Ruperto Majuca, *Optimal Hackback*, 84 Chi. – Kent L. Rev. 831 (2010).

Kijewski, Piotr, et al. *The Never-ending Game of Cyberattack Attribution, in*, Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities (Babak Akhgar and Ben Brewster eds., 2016).

Kirgis, Jr., Frederic L., *Custom on a Sliding Scale*, 81 Am. J. Int'l L. 146 (1987).

Kiss, Alexandre and Dinah Shelton, *Strict Liability in International Environmental Law 1131, in* Law of the Sea, Environmental Law and Settlement of Disputes: Liber Amicorum Judge Thomas H. Mensah (Tafsir Malick Ndiaye and Rüdiger Wolfrum, eds. 2007), http://ssrn.com/abstract=1010478.

Knake, Robert K., *Untangling Attribution: Moving to Accountability in Cyberspace, Subcommittee on Technology and Innovation*, Committee on Science and Technology, United States House of Representatives 2nd Session, 111th Congress (July 15, 2010).

Knox, John H., *The Flawed Trail Smelter Procedure: The Wrong Tribunal, the Wrong Parties, and the Wrong Law, in*, Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration (2006), http://papers.ssrn.com/ sol3/papers.cfm?abstract_id=665682.

Koh, Harold H., Legal Advisor, U.S. Department of State, *Address to the United States Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace* (Sept. 18, 2012). As prepared: https://www.state.gov/s/l/releases/remarks/197924.htm.

Koivurova, Timo, *Due Diligence*, Max Planck Encyclopedia of Law (Feb. 2010).

Kostadinov, Dimitar, *The Attribution Problem in Cyber Attacks*, *INFOSEC Institute* (1 Feb 2013), http://resources.infosecinstitute.com/attribution-problemin-cyber-attacks/.

Kozlowski, Andrzej, *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, 3 Eur. Scientific J. (Feb. 2014).

Kumar, Krishan, A.L. Sangal, and Abhinav Bhandari, *Traceback Techniques Against DDOS Attacks: A Comprehensive Review*, 491 Proceedings 2nd IEEE Int'l Conf. on Computer and Comm. Tech. (2011).

Kunig, Phillip, *Prohibition of Intervention, in*, Max Planck Encyclopedia of Law (2015), http://opil.ouplaw. com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?rskey=4krYZ6&result=5&prd=EPIL.

Kushner, David, *The Real Story of Stuxnet*, IEEE Spectrum 49 (Mar. 2013).

Langille, Benjamin, *It's "Instant Custom": How the Bush Doctrine Became Law After the Terrorist Attacks of September 11, 2001*, 26 B.C. Int'l & Comp. L. Rev. 145 (2003).

Langner, Ralph, *Cracking Stuxnet, a 21st-Century Cyber Weapon*, TED Talks (transcript) (Mar. 2011), http://www.ted.com/talks/ralph_langner_cracking_ stuxnet_a_21st_ century_cyberweapon/transcript.

Langner, Ralph, *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE Sec. & Privacy 49 (May/June 2011).

Langner, Ralph, *To Kill a Centrifuge* (Nov. 2013), http://www.langner.com/en/wp-content/ uploads/2013/11 /To-kill-a-centrifuge.pdf.

League of Nations, 12 League of Nations Off. J. 1759 (1934).

League of Nations, 4 League of Nations Off. J 1349 (No.11, November 1923).

League of Nations, 5 League of Nations Off. J. 525 (1924).

Legality of the Threat or Use of Nuclear Weapons, Advisory Op., 1996 I.C.J. Rep. 22 (8 Jul.).

Leiner, Barry M. et. al., *Brief History of the Internet,* Internet Society (n.d.), http://www.internetsociety.org/ internet/what-internet/history-internet/brief-history-internet.

Letter Dated 7 October 2001 From the Chargé d'affaires of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations Addressed to the President of the Security Council, U.N. Doc. S/2001/947.

Letter Dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations Security Council Addressed to the President of the Security Council, S/2001/946.

Lindblom, Anna-Karin, *The Responsibility of Other Entities: Non-Governmental Organizations, in,* The Law of International Responsibility 358 (James Crawford, Alain Pellet, and Simon Olledon eds. 2010).

Mackinnon, Mark, China's Chance: *How 9/11 played into Beijing's Plans in Asia*, The Globe and Mail (Sept. 6, 2012), http://www.theglobeandmail.com/news /world/chinas-chance-how-911-played-into-beijings-plans-in-asia/article593666/.

Majoran, Andrew, *The Illusion of War: Is Terrorism a Criminal Act or an Act of War,* Mackenzie Inst. (July 31, 2014), http://mackenzieinstitute. com/illusion-war-terrorism-criminal-act-act-war/.

Makovsky, David, *The Silent Strike How Israel Bombed a Syrian Nuclear Installation and Kept it Secret*, The New Yorker (Sept. 17, 2012), http://www.new yorker.com/ magazine/2012/09/17/the-silent-strike.

Mandiant, APT1 Exposing One of China's Cyber Espionage Units, (Feb. 2013), http://intelreport.mandiant. com/Mandiant_APT1_Report.pdf.

Marauhn, Thilo, *Customary Rules of International Environmental Law–Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace, in,* Peacetime Regime for State Activities in Cyberspace (Katharina Ziolkowski ed. NATO 2013) (internal citations and quotations omitted).

Mark A. Drumbl, *Pluralizing International Criminal Justice*, 103 Mich. L. Rev.1295 (2005).

Mark Bowden, Worm: The First Digital World War (Kindle ed. 2011).

Markoff, John, and David E. Sanger, *In a Computer Worm, a Possible Biblical Clue*, N.Y. Times (Sept. 29, 2010), http://www.nytimes.com/2010/09/30 /world/middleeast/30worm.html? pagewanted=all&r=0.

McAfee, *Net Losses: Estimating the Global Cost of Cybercrime* 2 (June 2014), http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf.

McAfee, The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies (July 2013).

Medellín v. Texas, 552 U.S. 491 (2008).

Mellor, Justin S.C., *Missing the Boat: The Legal and Practical Problems of the Prevention of Maritime Terrorism*, 18 Am. Univ. Int'l L. Rev. 341 (2002).

Merrill, Thomas W., *Golden Rules for Transboundary Pollution*, 46 Duke L. J. 931 (1997).

Microsoft v. i4i Ltd., 131 S.Ct. 2238 (2011) (Thomas J. Concurring).

Milanovic, Marko, *State Responsibility for Genocide*, 17 Eur. J. Int'l L. 553 (2006).

Miles v. United States, 103 U.S. 304 (1881).

Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J. 14 (June 27).

Ministry of Foreign Affairs of the Russian Federation, Press Release: UN Security Council Statement Regarding Terrorist Acts in USA (Sept. 12, 2001), http://www.mid.ru /bdomp/brp_ 4.nsf/e78a48070f128a7b43256999005bcbb3/ 65016b35f6a5140e43 256ac6002f8eb1!OpenDocument..

Ministry of Foreign Affairs of the Russian Federation, Press Release: Decision No. 438 by the Permanent Council of the Organization for Security and Cooperation in Europe on the Acts of Terrorism in New York City and Washington, D.C. (Sept. 14, 2001), http://www.mid.ru/bdomp/brp_4.nsf /e78a48070f128a7b43256999005bcbb3 /f85a74e6866e14e443256aca003ae7cf!OpenDocument.

Missouri v. Illinois, 200 U.S. 496 (1906).

Montevideo Convention on the Rights and Duties of States, in, U.S. Dep't of State, Pub. 1983, Peace and War: United States Foreign Policy, 1931-1941 (1943). http://www.ibiblio.org/pha/paw/.

Moore, Stephan, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C.J. Int'l L. & Com. Reg. 223 (2014).

Morton, Chris, *Stuxnet, Flame, and Duqu – the Olympic Games, in*, A Fierce Domain: Conflicts in Cyberspace, 1986-2012, 223-231 (Jason Healey ed., 2013).

Moya, Vanessa Ballesteros, *The Privatization of the Use of Force Meets the Law of State Responsibility*, 30 Am. U. Int'l L. Rev. 795, 796 (2015).

National Commission on Terrorist Attacks, *The 9/11 Commission Report* (2004).

NATO Update, *High-Level US Official at NATO HQ*, 26 Sept. 2001, http://www.nato.int/ docu/update/2001/0917/e0920a.htm.

Nicholson, Andrew, et al., *A Taxonomy of Technical Attribution Techniques for Cyber Attacks*, *in*, Proceedings of the 11th European Conference on Information Warfare and Security (Eric Filiol & Robert Erra, eds. 2012).

Nick Moore, The Information Society 271-272, in, World Information Report 1997-1998, UNESCO, http://www.unesco.org/webworld/wirerpt/ wirenglish/chap20.pdf.

Nieto-Navia, Rafael, *International Peremptory Norms (Jus Cogens) and International Humanitarian Law*, ICCNow, (n.d.), http://www.iccnow.org/ documents/ WritingColombiaEng.pdf.

Nollkaemper, André, *Concurrence Between Individual Responsibility and State Responsibility in International Law*, 52 Int'l Comp. L. Q. 615, 616 (July 2003).

Nollkaemper. Andre, *The Security Council and the Use of Force (Legal Aspects of International Organization)* (Niels Blokker and Nico Schrijver eds., 2015).

North Atlantic Treaty Organization, *Relations with Georgia* (June 7, 2016), http://www.nato.int/cps/en/natolive/topics_38988.htm.

North Atlantic Treaty Organization, *Statement by NATO Secretary-General, Lord Robertson* (2 Oct. 2001), http://www.nato.int/docu/speech/2001/s011002a.htm.

North Atlantic Treaty Organization, *Statement by the North Atlantic Council*, PR/CP (2001) 122 (11 Sep. 2001), http://www.nato.int/docu/pr/2001/p01-122e.htm.

North Atlantic Treaty Organization, *Statement by the North Atlantic Council*, PR/CP (2001) 124 (12 Sep. 2001), http://www.nato.int/docu/pr/2001/p01-124e.htm.

North Atlantic Treaty Organization, Statement issued at the Ministerial Meeting of the North Atlantic Council held at NATO Headquarters, Brussels, 6 December 2001, M-NAC-2 (2001) 159, http://www.nato.int/docu/pr/2001/p01-159e.htm.

North Atlantic Treaty Organization, *Statement to the Press by NATO Secretary-General, Lord Robertson on the North Atlantic Council Decision On Implementation Of Article 5 of the Washington Treaty Following the 11 September Attacks Against the United States*, 4 Oct. 2001, http://www.nato.int/docu/speech/2001/s011004b.htm.

North Sea Continental Shelf (Fed. R. Ger. v. Den., Fed. R. Ger. v. Neth.), 1969 I.C.J. 3 (Feb. 20).

O'Connell, Mary Ellen, *Cyber Security Without Cyber War*, 17 J. Conflict Sec. L. 1987 (2012).

O'Donnell, Daniel, *International Treaties Against Terrorism and The Use of Terrorism During Armed Conflict and by Armed Forces*, 88 Int'l Rev. Red Cross 853 (Dec. 2006).

O'Loughlin, John, et al., *A 'Risky Turn'? Putin's 9-11 Script and Ordinary Russians*, 56 Europe-Asia Studies 3 (2004).

On Russian President Vladimir Putin's Telegram of Condolence to US President George Bush (Sept. 11, 2001), http://www.mid.ru/bdomp/ brp_4.nsf/e78a48070f128a7b43256999005bcbb3/196ef 713841ec63b432 56ac60 02f8ea7!OpenDocument. (Unofficial translation from Russian).

Oppenheim, Lassa, *International Law: A Treatise* vol. 2 (Kindle ed. 2010).

Oxford Dictionaries (2016), https://en.oxforddictionaries.com/

Oxford Dictionary of Law, *Sic Utere Tuo ut Alienum Non Laedas* (7ed., Jonathan Law and Elizabeth A. Martin eds. 2014). http://www.oxfordreference.com /view/10.1093/acref/9780199551248. 001.0001/acref-9780199551248-e-3646.

Oxford Economics, *Cyber-Attacks: Effects on UK Companies*, Centre for the Protection of National Infrastructure (July 2014).

Panda Security, *Panda Security Detects Over 225,000 New Malware Strains Per Day in the First Quarter of the Year*, May 28, 2015, http://www.pandasecurity.com/ mediacenter/press-releases/panda-security-detects-over-225000-new-malware-strains-per-day-in-the-first-quarter-of-the-year/.

Panetta, Leon, U.S. Sec'y of Def., *Speech Concerning Cyber Security to Business Executives for National Security in New York City*, (October 11, 2012). As published in, Council of Foreign Relations (October 12, 2012). http://www.cfr.org/ cybersecurity/secretary-panettas-speech-cybersecurity/p29262.

Parrish, Austin L., *Sovereignty's Continuing Importance? Traces of Trail Smelter in the International Law Governing Hazardous Waste Transport, in*, Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration (2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_ id=765404.

Pernik, Piret, *Different Tactics, Same Story*, Int'l Center for Def. Studies (March 28, 2014), http://blog.icds.ee/article/255/different-tactics-same-story. See also, Piret Pernik, A Playbook for Hybrid War in Cyberspace? Int'l Center for Def. Studies (Aug. 29, 2014), http://blog.icds.ee/article/cyber-security/a-playbook-for-hybrid-war-in-cyberspace.

Pineda, Mikka, Fukushima Vs. Three Mile Island Vs. Chernobyl, Forbes (17 Mar 2011), http://www.forbes.com/2011/03/16/japan-disaster-nuclear-opinions-roubini-economics.html.

Pipyros, Kosmas, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostopoulos, *Cyberoperations and International Humanitarian Law: A Review of Obstacles, in*, Applying International Law Rules in Cyber Warfare, 24 Info. & Comp. Sec. 38, 45 (2016).

Prabowo, Hendi Yogi, *Terrorist Financing, Cybercrime and the Underground Economy*, Jakarta Post (July 9, 2012), http://www.thejakartapost.com/ news/2012/07/09/terrorist-financing-cybercrime-and-underground-econ omy.html#sthash.fcIafqos.dpuf.

Pipyros, Kosmas, Lilian Mitrou,, Dimitris Gritzalis, Theodoros Apostolopoulos, *Cyberoperations and International Humanitarian Law : A Review of Obstacles in Applying International Law Rules in Cyber Warfare*, 24 Information and Computer Security 38 (2016).

Press Release, Hon. Mark Kirk, Kirk, Warner to Introduce Cybersecurity Amendment to Ukrainian Aid Bill on Monday (Mar 23, 2014), http://www.kirk.senate.gov/ ?p=press_release&id=1033.

Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, U.N.G.A. Res. 3166, 1035 U.N.T.S. 15410 (14 Dec. 1973).

Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment of the Appeals Chamber (Int'l Crim. Trib. for the Former Yugoslavia 15 Jul 1999).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) Art. 49, para. 1 (June 8, 1977).

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, U.N.G.A. Res. A/RES/55/25 (2001).

Proulx, Vincent-Joël, *Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks* 23 Berkley J. Int'l L. 615 (2005).

Przetacznik, Franciszek, *Protection of Officials of Foreign States According to International Law* (1983).

Reed, Thomas C., *At The Abyss: An Insider's History of the Cold War* (Kindle ed., 2007).

Reiter, Michael K., and Ting-Feng Yen, Traffic Aggregation for Malware Detection, Detection of Intrusions and Malware, and Vulnerability Assessment 207-227 (2008).

Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. Rep. 174.

Report of the International Law Commission, 68th Sess., U.N. Doc. A/71/10 (2 May-10 June and 4 July-12 August 2016).

Report of the United Nations Conference on the Human Environment, Principle 21, Stockholm, 5-16 June 1972. http://www.unep.org/Documents.Multilingual /Default.asp?documentid=97&articleid =1503.

Rid, Thomas, and Ben Buchanan, *Attributing Cyber Attacks*, 38 J. Strategic Studies 1 (2015).

Riley, Michael, and Jordan Robertson, *Cyberspace Becomes Second Front in Russian Clash with NATO*, Bloomberg Business (Oct. 14, 2015), http://www.bloomberg.com /news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato.

Rio Declaration on Environment and Development, Principle 2, Rio, 3-14 June 1992, http://www.unep.org/Documents.Multilingual/Default.asp?documentid=78&articleid =1163.

Roberts, Anthea Eizabeth, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 Am. J. Int'l L. 757 (2001).

Rogers, James, *Was the Sony Pictures Hack an Inside Job?* Fox News, (Dec. 5, 2014), http://www.foxnews.com/tech/2014/12/05/was-sony-pictures-hack-inside-job.html.

Rogin, Josh, *NSA Chief: Cybercrime Constitutes Greatest Wealth Transfer in History*, Foreign Policy (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

Rome Statute of the International Criminal Court art. 66(3) U.N. Doc. A/CONF.183/9 (as corrected 12 July 1999.)

Rosenblatt, Seth, 13 Revelations from the Sony Hack, CNET, (Dec. 13, 2014), http://www.cnet.com/news/13-revelations-from-the-sony-hack/.

Rowe, Neil C., *The Attribution of Cyber Warfare*, *in*, Cyber Warfare: A Multidisciplinary Analysis (James A. Green, ed., Kindle ed., 2016).

Russia–NATO Statement (Sept. 13, 2001), http://www.mid.ru/bdomp/brp_4.nsf /e78a48070f128a7b43256999005bcbb3/66b3a03f8a8b608843256ac7003efef0!Open Document.

Ruys, Tom, *'Armed Attack' and Article 51 of the UN Charter Evolutions in Customary Law and Practice* (2011).

Ruys, Tom, *Crossing the Thin Blue Line: An Inquiry Into Israel's Recourse to Self-Defense Against Hezbollah*, 43 Stan. J. Int'l L. 265, 266 (2007).

S.C. Res. 1193, U.N. Doc. S/RES/1193 (28 Aug. 1998).

S.C. Res. 1214, U.N. Doc. S/RES/1214 (8 Dec. 1998).

S.C. Res. 1267, U.N. Doc. S/RES/1267 (15 Oct. 1999).

S.C. Res. 1333, U.N. Doc. S/RES/1333 (19 Dec. 2000).

S.C. Res. 1368, U.N. Doc. A/RES/1368 (Sept. 12, 2001).

S.C. Res. 1373, U.N. Doc. S/RES/1373 (28 Sept. 2001).

S.C. Res. 1377, U.N. Doc. S/RES/1377 (12 Nov. 2001).

S.C. Res. 1378, U.N. Doc. S/RES/1378 (Nov. 14, 2001).

S.C. Res. 1386, U.N. Doc. S/Res/1386 (20 Dec. 2001).

S.S. Lotus Case, 1927 P.C.I.J., (ser. A.) No. 10, (7 Sep.)

Safire, William, *The Way We Live Now: On Language: Smoking Gun*, New York Times, January 26, 2003, http://www.nytimes.com/2003/01/26/magazine/the-way-we-live-now-1-26-03-on-language-smoking-gun.html.

Santosky v. Kramer, 455 U.S. 745, 756 (1982).

Schachter, Oscar, *The Rights of States to Use Armed Force*, 82 Mich. L. Rev. 1620 (1984).

Scharf, Michael P., *Customary International Law in Times of Fundamental Change: Recognizing Grotian Moments* (2013).

Schmidt, Andreas, *The Estonian Cyber Attacks in*, A Fierce Domain: Conflict in Cyberspace, 1986-2012 (Jason Healey ed., 2013).

Schmitt, Michael N., & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 Fletcher Sec. Rev. 55, 73 (Spring 2014).

Schmitt, Michael N., *"Attack" as a Term of Art in International Law: The Cyber Operations Context, in*, 4th International Conference on Cyber Conflict 283, 284 (C. Czosseck, R. Ottis & K. Ziolkowki eds. 2012).

Schmitt, Michael N., and Sean Watts, *The Decline of Opinio Juris and the Law of Cyber Warfare*, 50 Tex. Int'l L. J. 189, 193 (2016).

Schmitt, Michael N., *Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Columbia J. of Transnat'l L. 885 (1999).

Schmitt, Michael N., *Counter Terrorism and the Use of Force*, 5 Marshal Center Papers (2002).

Schmitt, Michael N., *In Defense of Due Diligence in Cyberspace*, 125 Yale L. J. F. 68 (2015).

Schmitt, Michael N., *Responding to Transnational Terrorism Under the Jus ad Bellum, in*, Essays on Fault and War at the Fault Lines (2012).

Scott, James, *It's the Russians…Or Is It? Cold War Rhetoric in the Digital Age*, ICIT (Dec. 13, 2016), http://icitech.org/its-the-russians-or-is-it-cold-war-rhetoric-in-the-digital-age/.

September 11: Chronology of Terror, CNN.COM, http://archives.cnn.com/2001 /US/09/11/chronology.attack/.

Shackelford, Scott J., and Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo. J. Int'l L. 971 (2011).

Shamsi, Jawwad A., Sherali Zeadally, Fareha Sheikh, & Angelyn Flowers, *Attribution in Cyberspace: Techniques and Legal Implications*, Sec. Comm. Networks (2016), http://onlinelibrary.wiley.com/wol1/doi/10.1002/ sec. 1485/full

Sheffield, Kai, *Of Pulp Mills and Oil Spills: Strict State Liability Under Customary International Law When Energy and Resource Projects Cause Transboundary Environmental Harm*, Ecobulletin 4 (June 2011).

Shukla, Shantanu, & Sonal Sinha, *Use of Honeypot and IP Tracing Mechanism for Prevention of DDOS Attack*, 3 Int'l J. Sci. Engineering & Res. 94, 95 (2015).

Singh, Karanpreet, Paramuir Singh, and Krishan Kumar, *A Systematic Review of IP Traceback Schemes for Denial of Service Attacks*, 56 Comp. & Sec. 111 (2016).

Singh, Manish, US Govt Proposes to Classify Cybersecurity or Hacking Tools as Weapons of War (n.d.) http://betanews.com/2015/05/23/us-govt-proposes-to-classify-cybersecurity-or-hacking-tools-as-weapons-of-war/.

Sklerov, Matthew J., *Solving the Dilemma of State Responses to Cyberattacks: A Justification for The Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 Mil. L. Rev. 1 (2009).

Slama, Jo Lyn, *Opinio Juris in Customary International Law*, 15 Okla. City Y. L. Rev. 603 (1990).

Slouka, Zdenek, *International Custom and the Continental Shelf* (1968).

Smith, Ben and Arabella Thorp, *The Legal Basis For The Invasion of Afghanistan*, House of Commons (UK), SN/IA/5340 (2010).

Solon, Olivia, *Hacking Group Auctions 'Cyber Weapons' Stolen from NSA*, The Guardian (16 Aug. 2016), https://www.theguardian.com/technology /2016 /aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group.

Speeches of George W. Bush 2001-2008 (2010).

Springer, Paul J., *Cyber Warfare: A Reference Handbook* (2015).

State Responsibility, Second Report by F.V. Garcia (15 Feb 1957). U.N. Doc. A/CN/4/106.

State Responsibility in International Law (Rene Provost ed., 2002).

Statement by President Vladimir Putin of Russia, Moscow, September 24, 2001, http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/5e2870b37fe461dc43256ad20031b7f8!OpenDocument. (Unofficial translation from Russian).

Statement of the Euro-Atlantic Partnership Council, PR-123 (12 Sep. 2001). http://www.nato.int/docu/pr/2001/p01-123e.htm.

Statute of the International Court of Justice (1949).

Strickland, Jonathan, *How Does the Internet Work*, howstuffworks.com (2014), http://computer.howstuffworks. com/internet/basics/internet2.htm.

Symantec, *What are Crackers and Hackers?* (2010), http://www.pctools.com/security - news/crackers-and-hackers/.

Symantec, *What is a Script Kiddie?* (2010), http://www.pctools.com/security-news/script-kiddie/.

Szonyi, Michael, *Commentary No. 81: The Effects of September 11 and Its Aftermath on China, and The Chinese Response*, Canadian Security Intelligence Service (Spring 2002), http://www.csis-scrs.gc.ca/pblctns/cmmntr/cm81-eng.asp. (Archived content).

Tait, Matt, *On the Need for Official Attribution of Russia's DNC Hack*, Lawfare (July 28, 2016), https://www. lawfareblog.com/need-official-attribution-russias-dnc-hack.

Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt ed. 2013).

Tams, Christian, *The Use of Force Against Terrorists*, 20 European J. Int'l L. 359 (2009).

Tasioulas, John, *Opinio Juris and the Genesis of Custom*, 26 Aust. Y.B. Int'l L. 199 (2007).

Tenali, Naga Mani, and Bala Savitha Jyosyula, IP Traceback Scenarios, 20 Global J. Comp. Science Tech.13(E) (2013).

The Guardian, US Response: Attack on Afghanistan, (n.d.), http://www.theguardian.com/flash/0,5860,567567,00.html.

The History of Cyber Attacks–A Timeline, NATO Rev. (n.d.), http://www.nato.int/docu/review /2013/cyber/timeline/EN/index.htm. (Select April 2007).

The Tellini Case, 5 League of Nations Off. J. 525 (1924).

The Universal Declaration on Human Rights Art. 12, U.N.G.A. Res. 217A (1948).

Timber, Craig, Ellen Nakashima, and Danielle Douglas-Gabriel, *Cyberattacks Trigger Talk of 'Hacking Back",* Wash. Post (Oct. 9, 2014), http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/ 10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html.

Tor Project, Tor: Overview (n.d.), https://www.torproject.org/about/overview.html.en.

Torreon, Barbara Salazar, *Instances of Use of United States Armed Forces Abroad*, 1789-2015, 12, Cong. Res. Serv. (Oct. 15, 2015).

Transcript of statement by Russian Foreign Minister Igor Ivanov on the Results of His Meeting with US President George Bush, September 19, 2001, http://www.mid.ru/bdomp/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/78985760deef75c643256acd00616db0!OpenDocument.

Travalio, Greg, and John Altenburg, *Terrorism, State Responsibility, and the Use of Military Force*, 4 Chi. J. Int'l L. 97 (2003).

Tsagourias, Nicholas, *Cyber-attacks, Self-Defence and the Problem of Attribution*, 17 J. Conflict & Security L. 234 (2012).

Tyler, Patrick E., *A Nation Challenged: The Attack; U.S. and Britain Strike Afghanistan, Aiming at Bases and Terrorist Camps; Bush Warns 'Taliban Will Pay A Price'*. NY Times (Oct. 7, 2001), http://www.nytimes.com/2001/10/08/world/nation-challenged-attack-us-britain-strike-afghanistan-aiming-bases-terrorist.html.

U.K. Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, Cabinet Office (Nov. 2011).

U.N.G.A. res. 56/83 (12 Dec. 2001).

U.N.G.A., Information and Communication Technologies for Development, G.A. Res. 66/184, U.N. GAOR, 66th Sess. U.N. Doc. A/RES/66/184 (6 Feb. 2012).

United Nations Charter (1949).

United Nations Environmental Program, Division of Environmental Law and Conventions, Background (1 Oct. 2014), http://www.unep.org/delc/GlobalCommons/tabid/54404/Default.

United States Code, 18 U.S.C. § 2332b (LII, 2016).

United States Department of Defense, *Department of Defense Cyber Strategy* 2015.

United States Diplomatic and Consular Staff in Tehran (U.S.A. v. Iran), 1980 I.C.J. Rep. 3 (24 May).

United States v. Arjona, 120 U.S. 479, 484 (1887).

Universal Declaration of Human Rights, 27. G.A. Res. 217A (10 Dec. 1948).

Van-Hau Pharm, *Honeypot Traces Forensics by Means of Attack Event Identification*, PhD Thesis, Telecom Paris Tech (2009).

Verhoeven, Sten I., International Responsibility of Armed Opposition Groups 285-303, in, Responsibilities of the Non-State Actor in Armed Conflict and the Market Place: Theoretical Considerations and Empirical Findings (Noemi Gal-Or, Cedric Ryngaert, and Math Noortmann eds., 2015).

Vienna Convention on Diplomatic Relations, June 24, 1964, 500 U.N.T.S. 91.

Vienna Convention on the Law of Treaties, 27 Jan. 1980, 1155 U.N.T.S. 331.

Voigt, Christina *Principles of IEL* (n.d.), http://www.uio.no/studier/emner/jus /jus /JUS5520/h12/undervisningsmateriale/3.-principles-in-iel.pdf.

von Heinegg, Wolff Heintshel, *Territorial Sovereignty and Neutrality, in*, Cyberspace, 89 Int'l L. Studies 123, 124 (2013).

Waibel, Michael, *Corfu Channel Case*, Max Planck Encyclopedia of Public International Law (2015), http://opil.ouplaw.com/view/10.1093/law: epil/9780199231690/law-9780199231690e118?rskey= ryWdZN&result =1&prd=EPIL.

Wang, Xinyuan, and Douglas Reeves, *Traceback and Anonymity* (2015).

Waxman, Michael C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 Yale J. Int'l L. 422 (2011).

Weaver, Nicholas, *What Sauron Tells Us About What NSA's Up To, and What It Should Do Next,* Lawfare (Aug. 15, 2016), https://www.lawfareblog.com/what-sauron-tells-us-about-what-nsas-and-what-it-should-do-next.

Webopedia, *Zero-Day Exploit*, (n.d.), http://www.webopedia.com/TERM/Z/Zero_Day _exploit.html.

Weiss, Edith Brown, *Invoking State Responsibility in the Twenty-First Century*, 96 Am. Soc. I'ntl L. 798, 798 (2002).

What is a Packet?, Howstuffworks.com (01 Dec. 2000), http://computer.howstuffworks.com/ question5251.htm

Wheeler, David A., and Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, Institute for Defense Analysis, IDA Paper P-3792 (October 2003).

White, Michael, and Patrick Wintour, *Blair Calls For World Fight Against Terror, Special Report: Terror in the United States*, The Guardian (12 Sept. 2001), http://www.theguardian.com/politics/ 2001/sep/12/uk.september11.

Wippich, Brian, *Detecting and Preventing Unauthorized Outbound Traffic*, SANS Inst. (2007).

Wilson, Scott, *Israeli War Plan Had No Exit Strategy, Wash.* Post (Oct. 21, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/10/20/AR2006 102001688.html.

Wood, Michael, *Formation and Evidence of Customary International Law*, Report of the International Law Commission, 63rd Sess. (26 April-3 June and 4 July-12 August, 011) U.N.G.A. A/66/10/Annex 1.

Xiong, Huijun, Prateek Malhotra, Deian Stefan, Chehai Wu, and Danfeng Yao, *User-Assisted Host-Based Detection of Outbound Malware* Traffic, Information and Communications Security (2009).

Young, Ernest A., *Sorting Out the Debate Over Customary International Law*, 42 Va. J. Int'l L. 365, 372-373 (2002).

Young, Ernest A., *Sorting Out the Debate Over Customary International Law*, 42 Va. J. Int'l L. 365 (2002).

Zemanek, Karl, *Armed Attack, in, Max Planck Encyclopedia of Public International Law* (Oct. 2013).

Zetter, Kim, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, Wired, (Dec. 03, 2014).

Zetter, Kim, *The Evidence That North Korea Hacked Sony Is Flimsy*, Wired (Dec. 17, 2014), https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/

Zetter, Kim, *US and China Reach Historic Agreement on Economic Espionage*, Wired (Sept. 25, 2015), http://www.wired.com/2015/09/us-china-reach-historic-agreement

Zimmermann, Andreas, *International Law and 'Cyber Space'*, 3 Eur. Soc. Int'l L. Reflection (Jan. 10, 2014). http://www.esilsedi.eu/sites/default/files/ESIL% 20Reflections%20-%20Andreas%20 Zimmermann_ 0.pdf.