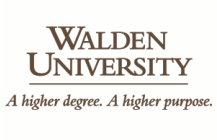

2015

Information Operations Under International Law: A Delphi Study Into the Legal Standing of Cyber Warfare

Kenneth Gualtier
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Kenneth Gualtier

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Linda Day, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Raj Singh, Committee Member,
Public Policy and Administration Faculty

Dr. Kristie Roberts, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2015

Abstract

Information Operations Under International Law:

A Delphi Study Into the Legal Standing of Cyber Warfare

by

Kenneth A. Gualtier

MPA, Troy University (2007)

MS, Troy State University (2004)

BS, University of Maryland University College (2002)

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

March 2015

Abstract

The ever-growing interconnectivity of industry and infrastructure through cyberspace has increased their vulnerability to cyber attack. The lack of any formal codification of cyber warfare has led to the development of contradictory state practices and disagreement as to the legal standing of cyber warfare, resulting in an increased risk of damage to property and loss of life. Using the just war theory as a foundation, the research questions asked at the point at which cyber attacks meet the definition of use of force or armed attack under international law and what impediments currently exist in the development of legal limitations on cyber warfare. The research design was based on using the Delphi technique with 18 scholars in the fields of cyber warfare and international law for 3 rounds of questioning to reach a consensus of opinion. The study employed qualitative content analysis of survey questions during the first round of inquiry in order to create the questions for the 2 subsequent rounds. The first round of inquiry consisted of a questionnaire composed of 9 open-ended questions. These data were inductively coded to identify themes for the subsequent questionnaires that consisted of 42 questions that allowed the participants to rank their responses on a Likert-type scale and contextualize them using written responses. Participants agreed that a computer attack is comparable to the use of force or armed attack under international law, but fell short of clearly defining the legal boundaries of cyber warfare. This study contributes to social change by providing informed opinions by experts about necessary legal reforms and, therefore, provides a basis for greater legal protections for life and property.

Information Operations Under International Law:

A Delphi Study Into the Legal Standing of Cyber Warfare

by

Kenneth A. Gualtier

MPA, Troy University (2007)

MS, Troy State University (2004)

BS, University of Maryland University College (2002)

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

March 2015

Acknowledgments

I would first like to thank my family for their patience and support during this long journey. Often they sacrificed more than I to afford me the opportunity to complete this study. I would also like to thank Dr. Linda Day and Dr. Raj Singh. Both served on my dissertation committee and were instrumental in providing stability after I endured having multiple changes in committee members. Additionally, I wish to extend my appreciation to Dr. Richard DeParis and Dr. Kristie Roberts who both served as university research reviewers during different points in the dissertation process. Lastly, I would like to thank the 18 scholars who participated in this study. These individuals, known only to me, agreed to give up their valuable time not for personal reward but for the continued pursuit of knowledge.

Table of Contents

List of Figures

Chapter 1: Introduction to the Study

Introduction

The topic of this study was the lack of regulation over cyber warfare under current international laws of war and the potential repercussions in loss of life and property. The ever growing interconnectivity of industry and infrastructure through cyberspace has increased their vulnerability to assault and potentially from anonymous threats. These threats include the use of malicious software to damage or even destroy key sectors of society. The capabilities to commit such acts are part of a modern class of warfare that has gone largely ignored by international law, even as its potential increases (Dipert, 2010). As a result, in this study I examined how the actions of states under cyber warfare may be limited in much the same way as they are under traditional warfare.

The destructiveness and suffering of civilian populations during wartime has led to the creation of numerous international laws of war that may have applicability in cyber warfare. In most cases, however, precedence will need to be established, and new laws developed by the international community. These laws will need to be agreed upon based on international standards rather than the current system of unilaterally developed policies that risks escalating interstate tensions (Sofaer, 2010). Therefore, the chief potential social implication of this study is the potential protection of human life and property as a result of the implementation of the recommendations that are presented here.

In Chapter 1 of this study, a background and summary of the literature associated with the laws of war and the gaps in the literature applicable to the use of computer viruses in cyber warfare is provided. These themes are further expanded upon in the

literature review and are accompanied by research into the application of customary law, global commons status for cyberspace, and the concept of state neutrality as it pertains to cyber warfare. Additionally, the theoretical framework of this study is introduced, based on Michael Walzer's modern adaptation of the just war theory and is expanded upon further in the literature review. Lastly, this research stemmed from a qualitative methodological tradition and was based on a Delphi method that includes snowball sampling techniques. The research paradigm is presented in Chapter 1 and described in greater detail in Chapter 3.

Background of the Problem

Over the last 150 years, the way states view the justifications for and conduct of combatants during war has changed dramatically. The St. Petersburg Declaration of 1868 stated that the only legitimate objective of war is to degrade an opponent's military capacity (Greenberg, 1998). In the Twentieth Century, the development of nuclear weapons changed military strategy from winning wars to avoiding them. The reality of warfare may again change with the advent of cyber warfare, but its potential is not yet apparent as a cyber conflict has yet to occur on the necessary scale (Geers, 2010). Notwithstanding, there is a widespread belief that developed states are unlikely to engage in cyber warfare as these states hold similar vulnerabilities and capabilities. Realistically, the threat of cyber warfare is more likely to occur from emerging states and non-state actors (Schmitt, 1999). While the immediate threat may lie in small scale adventurism, the possible repercussions of large scale cyber warfare makes limiting its scope under international law a necessity.

One potential source for limiting cyber warfare can be found in the just war theory. The just war theory is based on the paradox that, at times, it is necessary to kill to save lives (Williams, 2006). Walzer's (2000) work on the ethics of war in his interpretation of the just war theory revolve around the concepts of *jus ad bellum*, *jus in bello*, and more recently, *jus post bellum*. With these three concepts, the legality of a conflict is determinable by the justifications that lead to the decision to go to war, the actions committed during the conflict, and the conduct of combatants after the end of hostilities (Williams, 2006). These criteria are the basis for further evaluation of the legality of cyber warfare and served as a potential source for justifying its limitation within the context of this study. A specific issue that is addressed by the just war theory is attributing the appropriateness of the decision to go to war. Primoratz (2002) stated that there are wars where both parties are fighting for an unjust cause; wars where one side is fighting for a just cause and the other an unjust cause; but none where both parties are fighting for a just cause. Ultimately, any endorsement of the use of cyber warfare will have to meet the criteria of a just war.

Somehow, cyber warfare slips through the net of the just war theory and proves to be quite difficult to regulate using old, traditional ethical principles (Taddeo, 2013). Cyber warfare has been under evaluated by traditional morality and the laws of war. Most of the studies conducted in this area were done by computer scientists rather than moral theorists (Dipert, 2010). In fact, the closest analogy to limiting cyber warfare under international law may be the Biological and Toxin Weapons Convention of 1972 which banned the use of biological weapons on agricultural products (Whitby, 2002).

The unique nature of cyber warfare leaves traditional concepts within international laws of war such as perfidy, attribution, neutrality, and sovereignty unaddressed or improperly so. This ambiguity requires that greater attention be paid to the field of cyber warfare, which this research attempts to accomplish. In doing so, this study may aid in reforming the laws of war associated with cyber warfare.

Statement of the Problem

Despite the growth in cyber warfare capabilities, international law has failed to keep up with these new realities leaving the application of law ambiguous or even nonexistent (Schapp, 2009). Various international organizations have held conferences on the topic of cyber warfare including the United Nations Institute for Disarmament Research, the North Atlantic Treaty Organization, and the Organization for Security and Cooperation in Europe, but few concrete results have emerged (Kanuck, 2010). The unique nature of cyber warfare makes regulation under international law problematic (Waxman, 2011). Simply defining cyber attacks would require an expansion of the accepted definition of use of force while a failure to do so would leave some aspects outside the scope of any agreed upon international law (Barkham, 2001). Additionally, variations in legal traditions and strategic interests among leading powers limit their ability to come to a consensus (Waxman, 2011). Because of this, the Congressional Research Service stated that it was unlikely that the international community would be able to reach consensus on an applicable cyber warfare law (Hildreth, 2001).

The lack of clear regulation of cyber warfare under international law may provide states and non-state agents an opportunity to exploit the lack precedence and commit acts

of war or provoke one through their actions. A recent example of this occurred sometime before 2010 when a computer virus, later named Stuxnet, was developed and deployed against an Iranian nuclear facility. The virus appears to have had two purposes. First, it caused centrifuges used in the enrichment process to constantly change rotational speeds, which resulted in the centrifuges destroying themselves. Second, it sent signals to plant technicians masking the pending operational failure of the centrifuges. As the Stuxnet attack demonstrates, the lack of legal standing covering the use of computer viruses on commercial interests has become a more significant issue in recent years (Richmond, 2012). In order to address this problem, it is necessary to know more about the legal standing of information warfare under international law. This study provides a better understanding of the current state of international law regarding cyber warfare and where gaps in the law exist that may need to be addressed. The specific problem that is addressed is the potential for loss of life and property due to the ambiguity of international laws covering cyber warfare.

Purpose of the Study

The purpose of this study was to reach a consensus as to the current standing of cyber warfare under international law and to recommend changes to the law as needed. Traditionally, international law has developed from customary law, which is based on the actions of states. Although customary law still plays a major role today, negotiated treaties, decisions of international courts, and the actions of international organizations are also taken into consideration (Malanczuk, 1997). Because of the destructive potential

of cyber warfare it is inadequate to allow for the development of legal limitations under customary law because of the length of time this has traditionally required.

This research consisted of a qualitative analysis using the Delphi method of inquiry. The use of the Delphi method was appropriate as it allowed each participant to refine their responses based on the input provided by other participants. These reviews occured as the results of the previous round of questioning were provided to the participants in subsequent rounds, a process described by Skulmoski (2007). By using multiple iterations of inquiry with scholars in the field of cyber warfare and international law, a consensus was reached in a number of areas as to the current standing of cyber warfare under international law. The results of this research may be used as background for the development of an effective cyber warfare limiting regime.

Research Questions

The research questions were:

1. At what point do computer virus attacks elevate to the level of use of force or armed attack under international law?
2. What limitations in targeting exist with initial and reprisal cyber attacks?
3. How does the unique nature of cyber warfare affect the concept of neutrality?
4. What impediments currently exist in the development of legal limitations on cyber warfare?

Theoretical Framework

The theoretical framework for this study is based on Walzer's modern adaptation of the just war theory. Walzer (2000) theorized that the decision to go to war, *jus ad*

bellum, and actions during armed conflict, *jus in bello*, constitute legal and illegal acts of war based on the morality of these conditions. Because of this, criteria such as the defensive or offensive nature of the conflict, the composition of combatants, and the effect on the civilian population are of paramount importance when determining the justification for going to war. The protection of civilians, who are presupposed to be immune from attack, weighs especially heavy on just war theorists when determining the moral legality of war efforts. Modern international law does not yet specifically address many aspects of cyber warfare. The use of the just war theory may provide insight into future trends in the development of international agreements or the applicability of existing international laws to cyber warfare.

The just war theory is primarily concerned with limiting casualties and unnecessary damage during military engagements (Taddeo, 2013) making it suitable for utilization in this study. A principal focus of the just war theory is determining the legality of conduct during a conflict. This focus gives it applicability when determining whether an action has triggered a use of force designation and whether an act has violated the laws of war. Additionally, modern international law has been engrossed with humanitarian law as a source of legal development. Using the ethical standards of the just war theory may go a long way in determining how an international convention dealing with cyber warfare may develop. Lastly, the application of the just war theory in cyber warfare has been less than extensive. Utilizing the just war theory in this study adds to the existing body of literature and helps to fill existing gaps. A more in-depth review of the just war theory is included as part of the literature review in Chapter 2.

Nature of the Study

For this study, a Delphi method of qualitative inquiry was utilized in an attempt to find consensus among scholars as to the current legal standing of cyber warfare under international law. The use of the Delphi method was appropriate for this research specifically because of its utilization of multiple rounds of inquiry. This allowed the study to continue until consensus was reached among the participants (Hsu & Sandford, 2007) or until it became obvious that a consensus could not be reached. Based on the results of other Delphi studies it was expected that three rounds of inquiry would be sufficient (Custer, Scarcella, & Stewart, 1999) to reach these results, which it was. Additionally, as the Delphi method is designed for one-on-one investigation it allowed for more accurate assessments by respondents compared to those that would have been available in a group setting (Rowe, Wright, & Bulger, 1991).

The first round of inquiry consisted of a written questionnaire containing open-ended questions that afforded the contributors great latitude in their responses. Data analysis at the end of the first round consisted of conventional content analysis which took both the content and contextual meanings of responses and classifying them into meaningful categories (Weber, 1990). Content analysis may be used to describe a phenomenon that has not been extensively researched and aids in gathering data without preconceived notions (Hsieh & Shannon, 2005) making it ideal for this study. The categories identified in this research were then used to identify themes for subsequent rounds of questioning. Successive rounds of inquiry utilize questions narrowed based on previous responses and scored by the participant's use of a Likert-type 7-point scale. For

this study, consensus among the participants was based on scores for a minimum of 80% of the participants being within 2 categories on the 7-point scale as recommended by Ulschak (1983). The specific data collection and analysis procedures employed are described in more detail in Chapter 3 of this study.

With a Delphi study, it is recommended that researchers should use no less than 10 participants (Delbecq, Van De Ven, & Gustafson, 1975). Based on this recommendation this study commenced with 18 participants and concluded with 16 remaining. Participants were selected based on their contributions to scholarly research in the areas of international law and cyber warfare. Additional solicitations were made to individuals referred by the original pool of participants through the use of snowball sampling. The utilization of snowball sampling allows for identifying hidden populations (Sommers, 2011) which provided an opportunity to include appropriate professionals in this study who had not been previously recognized.

Definitions

Caroline standard: A legal determinate with which to judge the legality of pre-emptive military action based on necessity and proportionality (Condron, 2007).

Cyber warfare: The use of electronic means to attack and defend computerized systems and networks (Billo, 2004).

International law: The rules, principles, and decision making processes pertaining to the conduct between states and international organizations (Higgins, 1994).

Jus ad bellum: Latin for "right to war." A set of principles used to determine the legality of justification that led to the decision to go to war (Stahn, 2007).

Jus cogens: Latin for "compelling law." The principles of international law adopted based on accepted norms (Stahn, 2007).

Jus in bello: Latin for "justice during war." A set of humanitarian principles used to determine the legality of state practices during armed conflict (Stahn, 2007).

Jus post bellum: Latin for "justice after war." A set of principles governing peacemaking efforts after the end of hostilities (Stahn, 2007).

Opinio juris: Latin for "an opinion of law." The belief of a state that it has a legal obligation to act in a specific manner (Byers, 1995).

Payload: The actual data of a computer file. Within malicious software it consists of destructive, spurious, or insulating computer code (Computer Language Company, 2015).

Assumptions, Scope, Limitations, and Delimitations

The fundamental assumption of this research, which is necessary for gauging its validity, is that I have correctly identified the appropriate participants. The primary qualification for participation in the study was the contributors' knowledge and experience in the area of study as explained by Abrams (2010) which, in this case, was international law and cyber warfare. Purposive sampling in the form of an extensive review of existing scholarly literature was used to identify authors who could serve as participants in this study. The use of snowball sampling allowed for additional contributors to be included through peer-referral.

Purposive sampling requires researchers to exercise their own best judgment as to whom should serve as part of the representative subset of the population based on their shared common experiences (Abrams, 2010). For this study, the assumption was made

that the recruitment of participants based on an extensive literature review and the recommendations of these authors through snowball sampling sufficiently represented the population subset. Additionally, qualitative research often seeks out atypical cases simply because of their unique insights (Miles, 1994). Because of this, it is not only relevant but potentially valuable that some of the participants may have represented the fringe of the population group.

The scope of this study was initially delimited to those participants with backgrounds in academia and research scholarship. Additional contributors included industry and legal professionals based on the results of snowball sampling. Further delimitation occurred in that this study focused on computer virus attacks rather than all methods of cyber warfare. This delimitation was necessary in order to narrow the scope from the broad range of techniques, technologies, and results that constitute cyber warfare.

A number of limitations occurred with this study, chief of which was the level of participation. The willingness of selected interviewees to participate cannot be accurately predicted nor can their inclinations or abilities to remain involved for the duration of the research (Hsu & Sandford, 2007). Because of this, it became necessary to invite 48 individuals to participate and begin the study only after more than 15 had agreed to participate. This number was reached based on my belief that a sampling of this size would see at least 10 participants complete each round of inquiry. In the end, the study began with 18 participants and included at least 16 respondents for each round of inquiry.

Another potential limitation lay with the method of inquiry utilized and the possibility of bias. The use of a qualitative study requires the interpretation of collected data and, therefore, may be exposed to inaccurate extrapolations. This is especially problematic when factoring in potential researcher bias and the probability that being privy to all participants' responses in the earlier rounds of questioning may influence responses in future rounds (Altschuld, 1995). In order to mitigate the possibility of researcher bias, each participant was provided with a summary of results after each round of inquiry to allow for corrections and revisions.

Transferability serves an important role in the development of generalizations by the reader and, therefore, also qualifies as a limitation. This is because some researchers believe that qualitative methods lack application outside of their original context. Transferability is primarily the responsibility of the researcher through the construction of an exhaustive description of the research as well as a thorough analysis of the necessity and accuracy of assumptions made. Understanding the setting of the research, knowledge that the sample population was of sufficient size and variety, and other detailed information about the study will allow readers to make more appropriate generalizations and may also allow for transferability to their own studies (Trochim, 2007). To meet the transferability requirement, a thorough description of the methods and assumptions are provided in Chapter 3.

Significance of the Study

This study, helps fill a gap in the existing literature illustrating the lack of international norms, standards, and legal codification of cyber warfare. It also addresses

a gap as to the rights and limitations of states to respond to an act of cyber warfare. With an ever growing threat of cyber warfare serving as the battleground for proxy wars in the future, the protection of civilian industry and infrastructure during times of declared and undeclared conflicts need to be taken into account. This accounting can only take place after the legal standing of cyber warfare and its limitations can be ascertained.

With the results presented here, this study adds to the existing literature by showing where current international laws lack applicability, allowing for revision and greater coverage, and where their applicability already exists. This study may also serve as a vehicle for further research and as a catalyst towards increased academic and political debate over the need for revisions to the laws of war. In doing so, the negative repercussions on civilian populations during cyber conflicts and the proceeding reconstruction periods may be further minimized.

Summary

As with many technological advancements, the creation of cyberspace has had both practical peaceful and military applications. Civilian industry, private citizens, national infrastructure, and government agencies all find themselves accessible in the same cyberspace. This interconnectivity has served as an effective tool to increase efficiency, productivity, and the flow of ideas but, it has also created vulnerabilities to be exploited by state and non-state actors. Cyberspace is particularly susceptible to military exploitation because of the absence of appropriate international agreements as to the legality and standing of cyber warfare (Dipert, 2010). Through the application of the Delphi method of inquiry, and the use of the just war theory as a theoretical framework,

this study provides greater understanding of specific issues of legal absence and their possible future redresses.

In the following chapter, I provide an exhaustive literature review of scholarly works related to international law and cyber warfare. Chapter 3 follows the literature review and contains a detailed description of the methodology used for this study. The results of the research are presented in Chapter 4 and are followed by a summary of the study, drawn conclusions, and recommendations for further research in Chapter 5.

Chapter 2: Literature Review

Introduction

In this literature review, I demonstrate that despite the increased development of cyber warfare capabilities the international community has been unable, or unwilling, to expand the laws of war to encompass cyber warfare operations. In it, I further show that the focuses of most scholarly evaluations of cyber warfare have addressed only a specific aspect or two of the law or its applicability. In this chapter, divergent applications and scholarly views are pulled into a singular document to better address the issues of cyber warfare and the questions surrounding it legality. The literature review begins with a concise explanation of research strategies used in locating articles and to aid continuing research. From there, various concepts in international law are explored as well as their possible application in cyber warfare. These concepts include the laws of war, international humanitarian law, state sovereignty and neutrality, and ethical approaches to warfare.

With the signing of the Treaty of Westphalia in 1648, the international community recognized the nation-state as its principal entity. In doing so, the sovereignty of these nation-states became the chief factor in determining the early interpretations of use of force under international law (Best, 1983). Beginning in the Nineteenth Century, a shift occurred whereby states began to recognize the importance and usefulness of forgoing some measure of sovereignty in order to provide for greater international cooperation and stability (Jensen, 2002). This trend means that any future international agreement limiting the tools or scope of cyber warfare will require common

ground and agreement among a majority of states including those that have developed significant cyber warfare means.

Today, states throughout the world still view cyber jurisdiction as a matter of state sovereignty, domestic legal purview, and an issue for bilateral or multilateral agreement (Wilske, 1997). This leaves the physical location of the aggressor, victims, and the means of attack of central importance in making jurisdictional determinations (Flanagan, 2005). When the infrastructure and actors fall under a single jurisdiction or within an agreed upon jurisdiction, sovereign authority is exercisable leaving transnational action and questions of extraterritoriality in defense of national interests open to interpretation (Cassese, 2005). In 2006, the Shanghai Cooperation Organization reinforced its members' belief in national sovereignty over cyberspace declaring their right to manage cyberspace in accordance with each states own domestic legislation (Kanuck, 2010). This shows that states, including cyber warriors Russia and China, currently do not recognize the non-territoriality of the Internet or its associated equipment further minimizing the possibility of shared governance over cyberspace in the near future.

The unique nature of cyber warfare capabilities creates new challenges to traditional concepts in state sovereignty and the laws of war. The standards used to separate armed attack from use of force have traditionally been based on the physical effects of the action (Schmitt, 1999) making it problematic to judge a cyber attack by conventional means (Jurich, 2008). The law assumes that an attack will have physical limitations in time and space, and the effects of any attack will be visible within these confines (Rho, 2007) but, this assumption does not remain valid in cyberspace (Jurich,

2008). Cyber warfare may involve actions that go undetected for a considerable amount of time or that cause no physical or irreversible damage. Because of this what has traditionally been accepted as an armed attack or use of force will have to be reevaluated to take into consideration the distinctive traits of cyber warfare.

Research Strategies

To complete the literature review, I used numerous sources to find scholarly articles. The primary sources I utilized included the Walden University library system, Google Scholar, Lexis Nexis, and the EBSCO host database. The primary keywords used included *cyber warfare*, *information operations*, *international law*, *just war theory* and *ethics*. Additional sources were located by reviewing the references of those articles found using these techniques. Authors whose names reoccurred as sources in the references of these articles were then further researched to allow for a more comprehensive review of their works.

Theoretical Foundation

Any addition to the existing laws of war to include cyber warfare will most likely be based on philosophical grounds. One potential philosophical base may be found in the just war theory. The just war theory has developed as a tradition of thought based on core philosophical beliefs rather than a singular doctrine (Forge, 2008). Specifically, under the just war theory, armed conflict is permissible only when the duty to act towards a just goal cannot be achieved without violating the duty not to injure or kill (Baer, 2005). This does not limit states to defensive postures as numerous theorists have allowed for a narrowly defined right of intervention (Primoratz, 2002). Dilbert (2009) expanded on

this idea stating that preemptive attacks can be morally justified if the evidence exceeds a 90% likelihood of armed attack and that the provocation is expected to cause a high degree of damage. While a state may make a good faith assessment that the requisite factors for intervention or preemptive strike exist, these assessments may not meet the demands of the international community. This may stem from a difference of opinion or an inability to release intelligence data used to make the assessment without compromising sources or techniques.

In a broader sense, the just war theory is concerned with human rights and the protection of the individual during times of war. Wide recognition of the concept of human rights among theorists has led to the development of a cosmopolitan ethos which is based on commonly accepted ethical principles (Charvet, 1998). Cosmopolitan ethics has continued to develop in the last few decades towards an individual-centered ethos at the expense of the state. It proclaims that states only have those rights that serve the interest of the individual and that these states must respect the rights of all individuals equally regardless of their group affiliation or citizenship (Fabre, 2008). Based on cosmopolitan ethics, the individual has become the fundamental unit of concern with all individuals being held as equals. For just war theorists, this means there is no differentiating between sides during a conflict as civilians on all sides should enjoy the same protections.

While just war theorists are concerned with protecting civilians during times of conflict, they recognize that some civilians are not innocent. Walzer (2000) stated that civilians engaged in the business of war lose their protections and become legitimate

military targets. This can only occur when the individual forfeits their protections by their own action (Primoratz, 2002). This forfeiture is only accomplishable in one of three ways; by joining the military, by serving as a senior political leader, or by being employed in a military industry directly serving the war effort such as a munitions factory (Walzer, 2000). Some scholars, such as Green (1992), have criticized Walzer's blanket amnesty for civilian responsibility in the decision to pursue armed conflict and especially those living in democratic states. Other scholars find fault with civilians who do not actively oppose their government's pursuit of an unjust war labeling it passive support. Even though these scholars do not necessarily recognize the innocence of all noncombatants most still typically extend special protections to civilians during times of war (Primoratz, 2002). The question over who represents a legitimate target will play an important role in determining the legitimacy of cyber warfare.

An argument exists that cyber warfare is both potentially the most dangerous and the least comprehensively evaluated military technology from an ethical standpoint. Some scholars believe that technologies that make it easier to act in a destructive manner are more likely to be employed (Lucas, 2010). The defense industry's research and development of weapon systems is done within the restrains of military ethics and international law. Conversely, those who develop cyber warfare means are working primarily in software and are not as constrained as those that work in the traditional military complex (Perry, 2009). This has led some scholars to draw a correlation between the more indiscriminate planning of operations against civilian infrastructure within the cyber warfare community when compared to that of their counterparts in

traditional defense fields (Lucas, 2010). This adds an additional concern in the protection of non-combatants as the targeting of civilian infrastructure may increase causalities among civilians.

Contemporary just war theories have taken into account the costs and benefits of war when evaluating the legitimacy of armed conflicts. The problem that has vexed these theorists is how to measure cost and benefit against each other when the cost is unknown. This is of particular concern with weapons innovation as the current cost may be known, but continued justification into the future is not fathomable. Future cost might be indeterminable simply because of situational or technological changes, (Forge, 2008) or because interdependencies may cause unforeseeable indirect damage (Borg, 2005). Even with these potential problems the condemnation of cyber warfare is not universal even among those who have shown a propensity to deem it unethical or illegal. Rowe (2009) has recognized and commended some cyber tactics for their ability to damage a structure temporarily and in a reversible fashion which otherwise would have been destroyed had they been the target of a kinetic attack.

The majority of cyber weapons will most likely fail to achieve their intended result (Rowe, 2009). This stems from the fact that cyber weapons are more prone to system failures than traditional military weapons (Neumann, 1995), they may not find their intended targets, or they are ineffective because the target is not, or no longer, vulnerable to the weapon (Rowe, 2009). Cyber weapons, like all new weapons, have a high error rate (Dunnigan, 2003; Rowe, 2009). The fact that, while conventional weapons tend to improve, cyber weapon software is generally no more reliable today than

in the past further exasperates this problem (Neumann, 1995; Rowe, 2009). Additionally, cyber weapons most likely can only be used effectively once as after they produce the desired effect computer-forensic experts can typically determine what happened and devise protections against it in the future (Ranum, 2004). These realities cause potentially unreliable and uncontrollable weapons to be consistently developed and deployed leading to an endless cycle of collateral damage. For just war theorists, this will be a significant concern and a fundamental determinate in their evaluation of cyber warfare.

For the purposes of this study it was determined that the use of the just war theory may help define the future of cyber warfare legislation, however, some experts would disagree. Dipert (2006) saw both the just war theory and international law as inadequate to evaluate cyber warfare tactics either morally or legally. As with aviation and seafaring, cyber warfare operates in a realm whose focus are both military and non-military, with the boundary between the two problematic to demark. Because of this, some scholars believe it is difficult to properly determine the military aspects of cyber warfare within the current confines of either the just war theory or international law (Lucas, 2010).

Review of Literature

Defining Cyber Warfare

Cyber warfare includes both offensive and defensive computer technologies and their associated components, infrastructure, organizations and personnel (Jurich, 2008). Offensive tactics in cyber warfare can take one of two approaches: cyber attack, which causes some level of destruction and cyber exploitation, which in non-destructive and

would ideally go undetected such as obtaining information covertly through the use of Trojan Horse software. While different in their end roles, both forms require a vulnerability in the target, the ability to access the vulnerability, and a payload with which to execute. The vulnerability to be exploited most likely occurred as a design or implementation flaw but may have been intentionally created as a necessary aspect of the computer program. Ingress to the vulnerability may be done by remote access at a distance or by close access, which typically requires physical contact with the automated system being attacked (Lin, 2010). For the purposes of this research, only cyber attacks will be addressed as they are the only approach that is potentially deadly or destructive and, therefore, conceivably governable by the laws of war.

Cyber attacks are typically designed to cause problems with the integrity, authenticity, or availability of a computerized system or its data. Attacks on the integrity of a system need not cause the entire system to become inoperable, but instead could merely cause the system to respond in an atypical fashion. The most common method of performing a system integrity attack would utilize the destruction or manipulation of key system data. Questions of authenticity revolve around the masking of the true source of information leaving the user to believe in its genuineness. This can occur by the attacker being an active participant on a network generating erroneous traffic or by altering preexisting data. Lastly, availability may be the complete disabling of a system or a single component within it. Availability attacks often reduce functionality or deny services on a network rather than attempt to destroy data.

Jus Ad Bellum: The Laws of War

The United Nations Charter consists of the terms *use of force*, *threat of force*, and *armed attack* without clearly defining what each entails. Instead, states have relied on historical precedence and now recognize actions such as forms of economic and political coercion as unfriendly acts but not worthy of being elevated to the level of use of force, threat of force, or armed attack. These acts would include espionage, surveillance, denial of communication services, boycotts, the severing of diplomatic ties and the like (Lin, 2010). The International Court of Justice ruled in Nicaragua v. The United States (1986) that the use of force is not always tantamount to an armed attack and that the interference of one state into the affairs of another does not always justify the recognition of the intervention as a use of force (Jensen, 2002). Instead, the court provided three specific conditions to justify the need for a proportional response. First, the response must be directed against a state that has performed a wrong under international law. Second, the responding state must have first called on the aggressor to halt their illegal conduct and make reparations. Third, the responding state must do so in a manner proportional to the offending state's actions (Jensen, 2002). All three conditions have unique problems when applied to cyber warfare and especially the first two. Cyber attacks are often designed to mask the identity of the attacker and may not be detectable for a considerable amount of time. Additionally, the ambiguity over the current status of cyber warfare under international law may make it impossible to apply the court's first and third criteria.

Although a cyber attack may violate the legal obligations of a state, it is possible that the violation would be deemed merely a material breach of agreement rather than an

act that warrants a right to self-defense (Kanuck, 1996). Article 51 of the United Nations Charter recognizes the right of all states to self-defense if an armed attack occurs (Hoisington, 2009). The use of the term armed attack seemingly raises the minimum level of the offending action to that above a use of force (Schmitt, 1999) which does not afford the victimized state the right to reprisal but merely retorsions such as political or economic coercion (Jurich, 2008). This has led to an interpretative debate among scholars with some believing that a state must wait for an armed attack to have occurred before it invokes its right to self-defense (Barkham, 2001). Others use the *Caroline* standard as the basis for a customary law which would support preemptive force against an impending threat (Condron, 2007). Schmitt (1999) accepted the concept of anticipatory self-defense but limits it to instances when the cyber attack is a component of a greater armed assault, the armed assault is imminent, and the responding state has waited to the last possible instance to counter the impending attack. In doing so, he further explained that the counter attack must be done in response to the overall armed attack rather than merely the cyber aspect. The question that confronts theorists today is at what point cyber warfare elicits a right to self-defense under international law, especially considering that cyber weapons do not meet the accepted definition of an armed attack. This is necessary to determine whether the cyber attack is an act of war because if it fails to meet this standard, it would seemingly not be governed under the international laws of war.

Under *jus ad bellum*, a state must have proportionality, necessity, and immediacy, in order to claim self-defense. The concept of proportionality limits the nation's response

to one that is the least necessary in terms of intensity, duration, and magnitude to deter further provocation (Jensen, 2002). The victimized state must be able to identify their attacker, as well as the attacker's intent under the condition of necessity (Cordon, 2007). The question of attribution is one of whether a state can lawfully respond without conclusively knowing the identity of the attacker (Jensen, 2002). Even if the general location an attack emanated from can be determined, there still may be questions as to whether the perpetrator is a government agent (Schmitt, 1999). This problem is compounded by the strong possibility that a cyber attack will use perfidy, combatants masking their actions as genuine civilian activity, in order to avoid detection. Perfidy is illegal under international law because it encourages attacks on civilians (Rowe, 2009), as is the development of any weapon whose use cannot be reasonably kept with military personnel, or whose governments cannot be held accountable for their use (Lucas, 2010). It is necessary for states to be able to positively identify their attackers not only to avoid targeting innocents (Condron, 2007) but also because the rules governing the use of force are applied differently based on whether the aggressor is a state or non-state actor (Jensen, 2002). Even in conventional warfare there exists a fog whereby the identity of an attacker may not be immediately known. With cyber warfare, this concern is greatly magnified and is a central problem for leaders when attempting to respond to a cyber provocation.

To meet the condition of immediacy, the response cannot occur after too much time has passed (Cordon, 2007) but, as noted by Gill (2006), the response need not be immediately after the initial attack. The concept of "boiling the frog" may have

application here as it raises more questions about the requirement for immediacy. In this analogy, a frog placed in hot water will recognize the danger of his surroundings and jump out while a frog placed in cold water that is slowly brought to a boil will not recognize his predicament and be cooked. Many cyber attacks are of the same nature, as a sudden change in an automated system that has been attacked will be evident as well as its end results. Conversely, an attack that brings on a gradual response may eventually meet or even exceed the magnitude of the sudden change, but the results will only become apparent well after the attack occurred (Lin, 2010). This leaves the lesser sudden attack susceptible to a potential counterattack under the right to self-defense but the more intense gradual attack in legal limbo.

Rather than simply settle for passive defenses such as firewalls, sensors, and computer experts, governments are likely to develop active defenses that respond to recognized cyber events (Kumar, 2002). One example of this is the Blitzkrieg system which reportedly is capable of detecting and immediately responding to a cyber-born intrusion by initiating a virus attack on the offending computer system (Denning, 1998). To remain legal under international law, these active defensive systems would have to be limited in capability to reflect problems with attribution and characterization of the cyber event, as well as the neutrality of nations (Walker, 2000). The Blitzkrieg system seemingly would violate the law due to questions of attribution and neutrality. Its immediate response would not allow for positive identification of the attacker and its counter strike may pass through networks that exist in neutral third-countries. As the

Blitzkrieg system demonstrates, a lack of legal standing over cyber warfare may be exploited to deploy such system in defense of national assets.

Traditionally, there have been two approaches when determining whether an action justifies a use of force under international law. The first view sees international law, and related international organizations, as having been established to keep smaller actions from escalating into full-scale wars. Because of this they discount the method of attack and merely weigh the actual effects of the action. The second view sees any action other than military as legal under international law. Adherents to this approach weigh the quality of the force rather than the quantity of it. By extension, they discourage the use of military action while supporting diplomatic, economic, and political coercion (Sassoli, 2003). Schmitt (1998) discounted the viability of both approaches declaring that, as the means of coercion change, the law needs to evolve to recognize the new reality.

The United Nations Charter specifically omitted defining economic or political coercion as a use of force (Schmitt, 1999). Any attempt to classify cyber warfare as a use of force would make it difficult not to violate this premise as cyber attacks that cause no physical damage would have to be distinguished from acts of political and economic coercion that have the same end effects (Barkham, 2001). Hollis (2007) sees three possibilities for determining whether cyber warfare can ever constitute a use of force. First, cyber warfare cannot constitute a use of force if it lacks the physical characteristics of a traditional military attack (Kanuck, 1996). Second, cyber warfare constitutes a use of force whenever it targets critical national infrastructure (Jensen, 2002). Lastly, whenever a cyber attack is intended to cause a result similar to that of a traditional

military attack (Silver, 2002). While potentially useful, these criteria may remain too broadly defined and subject to interpretation to be the basis of a final determination as to the nature of a cyber event. A stronger approach may be found in one that possesses scientific application.

Models exist that were designed for more precise evaluation of state actions with some also potentially having applicability in evaluating cyber warfare. For example, Schmitt (1998) designed a 7-criterion tool to evaluate the actions of states through qualitative analysis. This is to be done using any fixed quantitative scale in which to calculate the severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility of the action. This would allow for a determination as to whether the cyber attack has the same predictable consequences as a kinetic attack and, therefore, meet Hollis' third criteria. Barkham (2001) sees Schmitt's approach as flawed and backwards for attempting to determine the legality of an attack based on the attack rather than the law. Conversely, numerous scholars see the effects of a cyber attack as the suitable point to judge whether the attack may be considered a use of force rather than the actual approach taken to deliver the attack (Schmitt, 1999). Barkham (2001) further sees fault on the reliance of immediately assessing the attack after its occurrence as cyber attacks often have effects unknown at the time of the event. Barkham's last critique is of singular importance when states find themselves under cyber attack. The use of a model, such as proposed by Schmidt, may be effective at evaluating cyber events and state responses to them after the engagement has occurred but, it is not a practical tool during the event. This means state actions may be criticized, or even punished after a conflict

has occurred although the state had no firm guidance as to the legality of potential responses during the event.

While acts of espionage have been deemed to be below the level of use of force, some instances of espionage utilizing military naval and air power have been categorized as armed aggression worthy of an armed response (Scott, 1999). Lin (2010) applies this same principle to cyber events, as while cyber exploitation is similar to espionage in nature, the payload delivered may also contain the ability to perform a cyber attack or be upgradeable to perform one in real time. The problem lies in the victimized state being unable to recognize the intent of the cyber intrusion. This is especially a concern considering that cyber exploitation and cyber attacks both start at the same point, taking advantage of a vulnerability, but result in very different effects. Lin points out that the situation is further complicated as some scholars believe that cyber exploitation could be considered an act of hostile intent rising to the level of use of force. This may be possible if an act of espionage is conducted for a considerable duration and collects a large volume of intelligence.

Even though they have similar results, international law takes a very different approach to economic sanctions and blockades. Economic sanctions refer to a sovereign state exercising its legal right not to trade with another sovereign state. By contrast, blockades have been deemed illegal as they infringe on the right of third-party states to trade with the state subjected to the blockade. With the increasing reliance of modern states on the Internet for commerce, cyber attacks that terminate any e-commerce functions would have to be evaluated as either sanctions or a blockade (Lin, 2010) and,

therefore, a potential use of force. On the surface, it would seem more similar to a blockade as severing e-commerce capabilities will most likely affect more states than just the belligerents. Regardless, questions about espionage and commerce are raised under cyber warfare that cannot be readily addressed by applying current understandings of the law. Like much of cyber warfare, these potential tactics represent a gray area of *jus ad bellum.*

***Jus In Bello*: International Humanitarian Law**

The effectiveness of current international humanitarian law's applicability towards cyber warfare is a matter of some debate. Numerous governments, including the United States, believe the current form is sufficient and have resisted efforts to include additional legal codification (Kelsey, 2008). They are supported by scholars such as Walker (2000) who believes the exponential growth of technology would leave any specific cyber warfare legislation obsolete shortly after it is enacted. Other scholars take the view that current law is difficult to apply to cyber warfare and have even called for an international convention to be convened to resolve the issue (Brown, 2006). These views clearly contradict. While technological growth would affect any agreed upon laws, the same has held true for conventional warfare.

Determining whether a target constitutes a legitimate military one is a difficult task under cyber warfare (Greenberg, 1998). The evolution of modern warfare has challenged the traditional categorization of military and civilian targets (O'Donnell, 2003) as acts of war no longer have the distinction of being designed to merely defeat the enemy's military force (Sassoli, 2003). The 1977 Additional Protocols to the Geneva

Convention clarifies by declaring military targets as those that make an effective contribution to military action or offers a definite military advantage (Kelsey, 2008). Because of this current international law does not deem attacks against targets that do not aid in the overall war effort, but that do have military applicability, as illegal (Brown, 2006). Civilian objects may be deemed legitimate targets if they are dual-use and have a secondary military capability that makes an effective contribution to military action (Sassoli, 2003). The interpretation of what makes an effective contribution, especially among dual-use targets, is of particular importance when attempting to legally limit cyber warfare.

There is an opinion within some segments of the military that all legal conventional military targets are also legal cyber targets as current international humanitarian law does not distinguish between modes of attack (Kelsey, 2008). This may make cyber attacks more advantageous to commanders as a cyber attack may result in less civilian collateral damage than a conventional attack (O'Donnell, 2003). Furthermore, the belief exists that nonlethal forms of cyber warfare will be more aggressively used, potentially leading to violations of international law, simply because their potentially nonlethal nature blurs the legality of their use. This stems from the conviction that the existence of nonlethal forms of cyber warfare may make it more likely that commanders will ignore the distinction requirements of international humanitarian law (Kelsey, 2008). This could leave purely civilian targets such as financial systems at greater risk (O'Donnell, 2003). More likely, it will leave dual-use industries, such as telecommunications, at risk. Cyber warfare has the potential to disrupt the activities of

these industries without causing physical damage to them. The lack of physical damage may allow leaders to justify them as legitimate wartime targets.

Rowe (2009) stated that the weapons and tactics most commonly arranged for in a cyber conflict are those that target civilians, potentially causing widespread suffering and the destruction of property. This has led him to believe that the use of cyber weapons in their current form is in violation of the laws of armed conflict. The principal of proportionality states that the loss of life and property related to an attack may not be disproportionate in relation to the military advantage gained by attacking the target (O'Donnell, 2003). This may leave some targets that are protected from conventional attack open to cyber attack if they minimize the loss of life and property (Schmitt, 2002). One example of this may be the targeting of the Internet itself.

The Internet began as a military project under the auspices of the Advanced Research Programs Agency as a means to create redundant channels of communication in the event of an attack on the United States (Walker, 2000). It has grown so quickly that providers have had to establish a hub-and-spoke configuration throughout various cities to handle the volume of use. This system improves operability but also leaves it more susceptible to attack and gives the sender and receiver little control over how their packets are transferred. With longer messages, the signal may be sent in multiple packets and reassembled at its destination. This most likely involves each packet taking a different path from the sender to the receiver (Kelsey, 2008). As the military relies on public communication infrastructure for an estimated 95% of its current communication transmissions (Intoccia, 2006), a case could be made that civilian infrastructure that sends

and receives Internet signals is a legitimate military target. Since it would be difficult to determine which routes military signals are taking to their receivers, this could leave the entire Internet susceptible to attack.

International law has intentionally avoided labeling economic coercion as an act of war (Barkham, 2001). The 1977 Additional Protocols to the Geneva Convention bans all states from damaging or manipulating any object that has been deemed essential for the populations' survival such as water, livestock, and agricultural products in a manner that makes it unavailable. The same convention also requires combatants to protect the natural environment, man-made objects that control the forces of nature such as dams, and other objects whose damage or destruction would contaminate the environment such as with nuclear power stations (Kelsey, 2008). This seemingly limits the use of cyber warfare and kinetic attack alike if the results contravened this convention. Again, the problem may lay in the fact that cyber warfare means could disable without physical damage these categories of targets. In theory, a nuclear power plant could be taken off line by a cyber attack to keep it from supplying power to the military at the expense of the civilian population it also serves.

Jus Post Bellum: The Aftermath of War

International law has recognized the need to safeguard populations when conflicts lead to the collapse of the state's sovereign authority. These laws are enshrined in the Conservation Principle which prohibits substantial changes to the legal, political, economic, or social institutions of a state by an occupying power (Cohen, 2007). However, the degree to which humanitarian law is applicable over civilian activities after

the secession of violence is not clear (Stahn, 2007). Furthermore, there is a disagreement between scholars as to whether *jus post bellum* already exists within the rules of *jus in bello* and *jus ad bellum* (Evans, 2005). In reality, *jus post bellum* is still in its infancy and requires further development before it can be applied to any form of warfare at the same levels as *jus in bello* and *jus ad bellum*. The debate as to whether there is even a need for a separate *jus post bellum* may serve to slow the process of legal determination.

The outcome of each war differs and may end in any of a number of scenarios ranging from surrender, occupation, regime change, armistice, transition to guerilla resistance, and the like. Just as the outcome of each conflict differs, so do the requirements to ensure a just peace (Williams, 2006). Under *jus post bellum* states that were not party to hostilities may still be involved in post-conflict activities (Osterdahl, 2009). Contemporary *jus post bellum* theorists believe a just peace occurs when all those involved in the conflict have more secure human rights than before the outbreak of hostilities. For this to occur, the victor, and potentially states not involved in the conflict, must restore order, rehabilitate damaged economies, restore sovereignty and self-determination as well as punish human rights violations that occurred during the conflict (Williams, 2006). Contemporary theorists have also speculated whether the concept of *jus post bellum* may serve as an incentive which guides how states pursue their goals during hostilities or lead them to avoid armed conflicts entirely so as not to limit their ability to forge a durable peace (Stahn, 2007). This may be visible in regards to cyber warfare in that it is a violation of international law to continue hostilities against a party that has surrendered. Cyber attacks tend to lack the necessary controls to adhere to this

stipulation and especially when the attack impedes the necessary communication to terminate it (Rowe, 2009). Conversely, the damage caused by cyber attacks is often much easier to reverse, making some cyber weapons more appropriate when considering post war operations.

While the conditions necessary to wage a just war have been debated to a considerable length, the circumstances needed for a just peace have gone largely ignored (Kegley, 1999). In fact, Walzer (2004) has defined it as the least developed aspect of the just war theory. Few, if any, conventional arms have had their development limited because of a need to more readily establish a just peace. The lack of limitations on conventional arms will most certainly carry over to cyber warfare as military planners and political leaders remain more focused on winning wars, rather than winning the subsequent peace.

Customary Law

One potential source for any international laws of war covering cyber warfare may be found in customary law. Customary international law has developed very slowly over time which has led some to dismiss it as impractical for the formation of international cyber law (Schmitt, 1999). The reality is that modern agreements have been negotiated, codified, and implemented in a short span of time such as with the laws governing outer space (Cody, 2002). More recent evaluations of customary international law formation have focused on the realist perspective that all those bound by the law should have some say in it. This logic would include non-state actors such as international organizations, nongovernmental organizations, and even multinational

corporations. Others have argued that many of these organizations are overly politicized and fail to properly represent civil societies (Ochoa, 2007). Unlike conventional military weapons, cyber weapons can be developed by all these entities and even individuals. This means any internationally agreed upon limitation on the use of cyber attacks will require taking these bodies into consideration. This may well lead to some of them demanding a say in the formation of the law and standing within the regulatory regime.

Historically, states have reacted to changes in the tools and tactics of war by the use of analogy. This has occurred by applying previous and related laws to new situations and technologies, by developing laws and making agreements regulating or prohibiting an act or technology, or by updating and revising existing laws and agreements (Hollis, 2007). Traditionally, the formation of customary law has been based on state practice and *opinio juris*, relying heavily on resolutions and declarations (Meron, 1996). State practice refers to the general and consistent actions of a state which forms a precedence that can be applied to the law. Conversely, *opinio juris* is the belief that states follow a set practice because of a feeling of legal obligation to do so rather than their own views (Byers, 1995).

Some scholars have questioned the validity of the view that customary law is based on the beliefs and actions of the state (Ochoa, 2007) while others have claimed that the use of custom as a source in the development of international law is nearing its end (Kelly, 2000). This view is based primarily on the belief that the nature and importance of custom's essential components are contentious (Roberts, 2001). At the same time, the use of international codifications, scholarly works, and International Court of Justice case

law have all contributed to the development of customary international law (Reisman, 1987). These seemingly contradictory viewpoints have led to opposing approaches, which Roberts (2001) labeled traditional custom and modern custom.

Traditional custom is defined as coming from specific instances of state practice as formulated by the state's belief in its legal obligations. With traditional custom, *opinio juris* becomes a secondary consideration. Dissimilarly, modern custom emphasizes *opinio juris* and general statements rather than actual practice (Roberts, 2001). Because traditional custom is based on actual practice it may better represent the actual views of the international community and, therefore, represent the way forward for the formation of laws limiting cyber warfare. The problem lies in the lack of precedence setting national policies in regards to cyber warfare. For the most part, states have intentionally failed to limit their cyber capabilities and have even made contradictory statements over their policy beliefs.

Differences between modern and traditional custom are also apparent in their development, as the former could progress rapidly while the latter would move slower through an inductive process. These differences would allow for different tests and justifications of their utility (Henkin, 1996). Traditional custom has been further criticized as inappropriate for the development of international customary law because of the increased number and diversity of states, as well as the amplified role that international forums play in addressing issues (Charney, 1993). This seemingly serves the interests of a small group of powerful states (Reisman, 1987) and may lead to laws that lack true legitimacy as they would be based on little or even conflicting state

practices (Weisburd, 1988). Modern custom is criticized as actually being an offshoot of universal declaratory law, rather than an evolution in customary international law. The premise of this idea is that modern custom develops through statements of practice, whether or not they are believed by the formulating state, and not through an analysis of regular state behavior (Bodansky, 1995). Because of the disagreements over the development of custom the utilization of a traditional or modern approach and, therefore, between *opinio juris* or state practice, may well lie in the actual activity being legislated and the reasonableness of the law. This concept is supported by the interpretive theory of law which seeks equilibrium between what laws have been and what they should be (Roberts, 2001).

While the utilization of battlefield and operational practices have gone largely ignored in the development of customary international law (Meron, 1996), the Agreement on the Prevention of Dangerous Military Activities negotiated between the United States and the Soviet Union may set precedence for the development of just such a customary law. With this agreement the two parties forbade the interference of command and control systems which would otherwise be a legitimate target under the existing laws of war (Barkham, 2001). This agreement notwithstanding, states are unlikely to limit the use of cyber weapons under international agreement because they could offer the benefit of non-lethal attack, and the full extent of their potential is unknown (Ellis, 2001). This may mean that states will not choose to limit cyber weapons until after they have deployed them and tested their potential in a real-world conflict (Kelsey, 2008). Regardless, precedence setting bilateral agreements like the Agreement on the Prevention

of Dangerous Military Activities may serve as a principal contributor to the establishment of a customary law covering cyber warfare in the future.

A Global Common in Cyberspace

Cyberspace has become an integral and integrated aspect of the global economy and human interaction. Based on this, the belief that cyberspace should be defined and managed under the guise of a global common, not unlike the high seas, Antarctica, and outer space has recently emerged. The difference here is two-fold; first, the established areas of global commons are natural formations and not an invention conceived by human beings. Second, current attitudes recognize national sovereignty over cyberspace whereas sovereignty over the existing global commons was never previously established. These means that arbitrators would be required to rule in cases of national sovereignty over cyberspace, but only after the extent of the global common had been established. This, in turn, would be possible only after international norms and standards over both jurisdictions and behavior in relation to cyberspace are established (Kanuck, 2010).

The use of wireless technologies further complicates the recognition and application of sovereign jurisdiction. One related example deals with the International Telecommunication Union (ITU) which is charged with allocating electromagnetic frequencies and enforcing a ban on unauthorized usage. The government of Cuba has used the ITU mandate to unsuccessfully charge the United States with violating its national sovereignty because of unauthorized, anti-regime television and radio broadcasts emanating from south Florida (Kanuck, 2010). The inability of the ITU to successfully

adjudicate the Cuban complaint shows that similar complaints over cyberspace may well suffer from a similar lack of authoritative controls.

Physical areas and resources that are designated global commons are done so based primarily on the scarcity of the resource, developing technologies, and the maintenance of access. This is particularly true with advancements in technology that lead to overuse and, therefore, man-made scarcities. The principal function of global common governing bodies, which are established by treaty signatories to oversee the proper implementation of the treaty's statutes, is not to assign rights but to regulate behavior in order to avoid such scarcities (Vogler, 2012). This occurs when states join regulatory regimes and adhere to their tenants specifically because they represent the minimum direction over their activities that they are willing to accept (Underdal, 1980).

One example of global common governance can be found in the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, otherwise known as the Outer Space Treaty of 1967. This treaty currently consists of 101 state parties and 89 state signatories (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, 1967). It requires states to consult with the other signatories prior to introducing anything into outer space that would interfere with its peaceful exploration or use (Hollis, 2007). As with this treaty, most successful global commons regimes are founded on a system of mutual interdependence that exacts adherence through a form of peer pressure rather than sanctions (Vogler, 2012). Based on this example, any cyber global common would likely have similar constraints on military usage. In doing so, the

deployment, but not necessarily the development, of cyber weapons would be considered a material breach of agreement but not a violation of international law. Depending on the nature of pressures allotted to the regulatory regime a global common designation for cyberspace would probably do little by itself to limit cyber warfare.

Unlike previous commons, cyberspace is a unique mixture of that which should be private, public, and under shared governance. Additionally, it exists in a nonfigurative world of ideas and information (Lukasik, 2000). As with most emerging technologies, differences appear between those technologies and the global commons. First, while distribution may be global, as in the case of cyberspace, it is not done systematically or equitably. The development of new technologies is also irreversible and inevitably leads to advancements that ultimately create new realities. This makes it necessary to anticipate areas of growth, forestall the risks involved, and adjust regulations accordingly before the global common shows any effects. Stern (2011) concludes that this problem is exasperated by global conflicts of interest, conflicts in values, and questions about the legitimacy of policies considering that governance is normally done by elites who are advised by technical experts.

Because of the dynamic nature of network technologies any treaty would require constant revision, which again separates cyberspace from the existing global commons. As new technologies are typically concentrated into increasingly fewer hands, rivalries among states and differences of opinion may hamper the necessary revision of the treaty. Lacking any real motivation to revise treaty standards to limit their utilization of these

emerging technologies, it is unlikely that the appropriate treaty revisions will occur in a timely fashion.

Neutrality in Cyberspace

The Hague Convention V states that warring parties may not move weaponry or military supplies, including air units, across the territory of a neutral state. The only exception to this rule is that naval units may pass through a neutral state's territorial waters, but may not commit a hostile act while present there. Additionally, neutral states are required to resist any attempts at violating their territorial sovereignty (Kelsey, 2008). Some scholars see the use of cyber weapons as violating neutrality as the weapons are moved across the territory of neutral states through the use of their communication systems (Greenberg, 1998). Brown (2006) also supports this belief by recognizing a distinction between the sending of military communication, which does not violate neutrality, and cyber weapons.

According to Hague Convention V neutral nations have no obligation to deny access to any of their publicly accessible communications equipment even in the event of an international conflict. This is contingent on them applying any chosen action equally and impartially as failure to do so would cause them to forfeit their neutrality. These stipulations are only enforceable in times of armed conflict and, therefore, are not applicable to cyber events that do not rise to the level of use of force (Jensen, 2002). However, whether Hague Convention V applies only to communication networks but also digital systems that are capable of creating data rather than merely relaying it is a matter of some contention (Kelsey, 2008). This dispute is an important one as military

communications can be carried by both means, but cyber attacks that employ weapons such as computer viruses are only possible using digital systems.

The primary purpose for a neutral designation is to protect noncombatant states from becoming involved in a conflict against their will. Even with this designation a neutral state may be drawn into the conflict based on their inaction. If a neutral state in unwilling or unable to halt the use of its territory for the military benefit of one of more combatants, the other belligerents may attack the enemy within the neutral state's sovereign territory (Jensen, 2002). The neutral state than may invoke a right to self-defense (Walker, 2000) pulling increasingly more states into a wider war. It is more likely that the state victimized by the cyber attack will retaliate by using the communication networks of neutral states to launch a cyber attack of their own (Kelsey, 2008). This scenario would risk expanding the conflict beyond its original belligerents and encompass a wider war, but only if the use of networks in neutral countries can be considered a military benefit. This seems unlikely because the redundancy of Internet routing theoretically would require the severing of digital communications passing through all neutral countries. The problem is further compounded by the fact that the ability of a neutral state to detect a malicious packet and prevent their passage through its communication network is very limited short of severing all outside communications (Brown, 2006). This would be an unreasonable burden on civilian and non-threatening military communications and adds yet another point of contention over the role of neutrality in cyber conflicts.

Despite the problems cyber attacks afford to the traditional notion of state neutrality, it should be noted that there is the belief that the concept of neutrality does not exist in an armed conflicts when the use of force has been authorized by the United Nations Security Council to maintain or restore the peace (Huang, 2009). This designation would have the same effect on a cyber conflict if, and when, the use of cyber weapons is legally recognized as an armed attack.

Summary

While tenets of *jus ad bellum, jus in bello* and *jus post bellum* may have applicability to cyber warfare, international law does not yet specifically address this possibility nor has it developed laws that acknowledge the unique nature of combat that cyber warfare presents. Further complicating the expansion of international law to incorporate cyber warfare is that established concepts, such as state neutrality, are blurred by the technologies utilized to wage war in cyberspace. Additionally, cyberspace holds some of the same properties as established global commons, such as outer space and the high seas, which would have to be taken into account when attempting to regulate cyber warfare.

International law has developed primarily under customary law but, with cyber warfare in its infancy, states have yet to develop clear policies on its uses and appear to be reluctant to do so until the capabilities of cyber warfare can be fully understood. Historically, the existing laws of war have been applied to new weapon systems and methods but the unique nature of cyber warfare makes this difficult. Because of this it may be necessary to develop new laws rather than attempt to apply existing laws to some

aspects of cyber warfare. One possible philosophical basis in the development of a new cyber warfare convention may be found in the just war theory, and the emphasis it places on human rights. By evaluating cyber warfare against the ethical standards of war developed under the just war theory, it may be possible to get a clearer picture of what is needed to ensure that cyber warfare does not lead to the same excesses that are currently banned under traditional warfare.

In the following chapter, I describe the research method used including the research questions, data processes and procedures, as well as commentaries on data verifications and limitations of the study.

Chapter 3: Research Methods

Introduction

In the previous chapter, the current literature on the laws of war and the historical development of international law were described. Additionally, in it a gap was shown in the literature regarding the legal standing of, or any definitive applicability of current international law, in the area of cyber warfare. In an attempt to understand the current legal context and provide recommendations for development of more adequate protections, this study sought out the knowledge and opinions of recognized experts in the fields of international law and cyber warfare. This chapter describes the qualitative research method and design used in an attempt to obtain a consensus among these scholars as to the standing of cyber warfare under international law.

Research Design and Methodology

To better clarify the legal standing of cyber warfare under international law, this study employed a method of inquiry utilizing the Delphi technique. O'Sullivan, Rassel, and Berner (2003) contended that qualitative methods are appropriate for research that produces data that are difficult or impossible to express numerically such as the replies to open-ended questions. This method allowed for the asking of initial open-ended questions, interpretation of the responses, and preparation of follow-up questions (Caudle, 1994) so as to find themes and concepts in the data (O'Sullivan, Rassel, & Berner, 2003). This approach is necessary for studies such as the one presented here where variables are difficult to discover or to measure accurately (Creswell, 2007). Because of the lack of

previous investigation into this topic, it was difficult to determine any variables to examine at the onset of this study.

The Delphi method is principally applicable for studies that require structured and organized group communication (Powell, 2003). Unlike other qualitative research methods, the Delphi technique utilizes multiple iterations to allow for the development of consensus in regards to a specified topic (Hsu & Sandford, 2007). This is especially important for a topic that is lacking in empirical evidence (Delbecq, Van De Ven, & Gustafson, 1975) as the feedback each participant receives from the researcher between rounds may increase the level of participation and discovery of new ideas (Pill, 1971). The Delphi technique's ability to combine the knowledge of the research subjects is ideal for a study of the interpretation of international laws and their applicability towards cyber warfare.

Originally, other methods and techniques of inquiry were investigated and considered for this study but ultimately deemed to be less effective in providing the desired outcome. One method examined was the use of a grounded theory study which attempts to develop a theory based on the results of a single round of interviews with enough participants to saturate a data category (Creswell, 2007). This approach was dismissed because a single round of interviews would most likely not have provided adequate data to reach a consensus of opinion. This is especially true in that a first round of questioning was required for this study to discover the themes needing to be explored further. This assumption proved accurate as subsequent rounds of questioning were necessary to develop an understanding of the topic and reach a consensus among the

participants. Furthermore, the topic most likely did not lend to the availability of sufficient experts in the field of international law and its applicability to cyber warfare to reach the requisite saturation point.

Another method considered was the use of an instrumental case study. Instrumental case studies are designed specifically to gain general knowledge of a phenomenon based on the examination of a small population (Trochim, 2007) making it initially appealing for this study. They are also designed to focus on either a single case or a grouping of similar cases (O'Sullivan, Rassel, & Berner, 2003) and are concerned with increasing the understanding of a phenomenon rather than the case itself (McNabb, 2008). Because case studies take information from diverse sources, there is a lack of focus on the case as a whole (O'Sullivan, Rassel, & Berner, 2003). The intended role of this study was to determine the existing, potentially applicable, and future direction of international law governing cyber warfare. Because of this, it was deemed that a focus on the case in its entirety was a more appropriate research approach which, therefore, disqualified the use of an instrumental case study.

Participants of the Study

The accuracy of results, when using the Delphi method, is based primarily on the qualifications of the participants involved (Powell, 2003). While there have been some negative critiques of the Delphi method's lack of random sampling (Williams & Webb, 1994) the technique does not require that contributors be a statistically representative sample, but rather selected based on their expertise and credibility in the area of investigation (Powell, 2003). Because of this, a list of potential participants was

compiled stemming from their expertise in international law and cyber warfare as determined by their inclusion in the literature review. Through the use of snowball sampling, additional contributors were referred by those participants that were previously identified and invited to partake in the study. Snowball sampling is a subset of purposive sampling, which allows for the increase of sample sizes during the course of a study based on suggestions from research participants (Sommers, 2011). These additional participants met both the expertise and credibility requirements necessary for inclusion in the population group based on their reputation and referral by their peers.

An insufficient amount has been written about international law and cyber warfare, meaning the literature review most likely does not recognize a majority of individuals knowledgeable in the field. Because of the low number of identified potential participants at the onset of the study, the use of snowball sampling was both necessary and appropriate because of its ability to find hidden populations (Sommers, 2011). By using snowball sampling, those who had published scholarly works on the subject were utilized to recommend others potential participants qualified to contribute to the study. This assisted in discovering a larger pool of participants as well as with meeting the necessary number of research subjects.

The appropriate number of contributors in a Delphi study will vary based on the research topic and the available resources (Delbecq, Van De Ven, & Gustafson, 1975). Some researchers believe that the more participants that are involved in a study, the better the potential outcomes. However, even many within this group recognize that there is little scientific evidence that an increase in participation will have any effect on the

consensus and, therefore, the reliability of results reached by the contributors (Murphy et al., 1998). The majority of researchers using the Delphi method seemingly reject the view that greater participation levels are ideal. A review of Delphi studies has shown that the majority have relied on between 15 and 20 participants (Ludwig, 1997). Similarly, Delbecq, Van De Ven, and Gustafson (1975), have proposed that between 10 and 15 contributors is sufficient for most studies. They recommend that researchers use as small a number of participants as possible to allow for the verification of results through future explorations. This is of particular importance in fields of study where a limited number of possible participants exist. Based on these recommendations the targeted number of participants for this study was 15 with the possibility that it may have exceed this number based on greater than expected participation. It was also recognized that the study may have failed to reach the target number because of difficulty finding willing and qualified contributors. Because of this, invitations to participate were offered 35 individuals, with 13 additional invitations based on the results of snowball sampling. The number of participants was deemed to be sufficient as long as it exceeded 10 for all three rounds of questioning. During the course of this study, each round consisted of no less than 16 respondents.

Research Questions

1. At what point do computer virus attacks elevate to the level of use of force or armed attack under international law?
2. What limitations in targeting exist with initial and reprisal cyber attacks?
3. How does the unique nature of cyber warfare affect the concept of neutrality?

4. What impediments currently exist in the development of legal limitations on cyber warfare?

Ethical Protection of Participants

The participants in this study consisted of volunteers whose right to choose whether to participate or not were made clear, and in writing, during the initial solicitation period. The potential contributors were told that, by agreeing to partake in this study, they would be in no way affecting their relationship with Walden University or their employers. Each participant was also told that maintaining their anonymity was both assured and of utmost importance. There was no known risk of potential physical or psychological harm to the contributors of this study. The initial solicitation letter and consent form are included in the appendix of this study.

To protect confidentiality, all electronic media related to this research was retained on a password-protected personal computer and within encrypted compression files. Any information that may have made identifying the participants possible was removed prior to data analysis. Paper copies of data and correspondences were not made during the course of this study.

Data Processes, Procedures and Collection

The following represents a sequential documentation of the processes and procedures used to solicit participants, conduct research, collect and interpret data, and validate the findings and conclusions as approved under Institutional Review Board number 02-24-14-0140351.

1. Initial solicitation letters were sent via e-mail to those potential participants identified based on their contributions to scholarly research in international law and cyber warfare as represented in the literature review. These letters detailed the purpose of the research, the protections provided to the participants, and a request to refer the names and contact information of any other known individuals whose expertise would make them ideal candidates for inclusion in this study. Those agreeing to participate were asked to sign and return the consent form included with the initial solicitation letter.

In theory, the Delphi technique may include an unlimited number of rounds of questioning ending only when a consensus has been reached (Hsu & Sandford, 2007). In reality, the vast majority of studies require no more than three rounds of questioning to establish a consensus (Custer, Scarcella, & Stewart, 1999). The questionnaire for the first round typically consists of open-ended questions, which allows the respondents the freedom to elaborate (Rowe, 1999). For the purposes of this research design, it was assumed that three rounds would be both necessary and sufficient while leaving open the possibility that additional rounds of questioning may have been necessary.

2. Each participant was provided with the first questionnaire and asked to return it within 2 weeks. The first and subsequent questionnaires are included in the appendix of this study.

Controlled feedback is an essential part of the Delphi method. Delphi studies are designed to reduce the effect of noise which Dalkey (1972) described as a type of communication that ensues in group processes. This noise may have a negative effect on data validity as participants act selfishly rather than towards a shared common goal of focusing on the question at hand. To minimize the potential for noise, feedback was controlled by providing a well-organized summary of results allowing the participants the opportunity to elaborate on, or correct, their previous responses. It is expected that after using this method over multiple rounds of questioning the views of participants will begin to converge to the point of reaching a consensus (Hsu & Sandford, 2007). As the feedback provided is the only form of communication between contributors, it is of paramount importance as a tool for the formulation of consensus (Murphy et al., 1998).

3. Each participant was provided with a summary of the results for the first round of questioning. This summary restated the original questions and provided synopses of each participant's responses.

A qualitative review of the results for the first questionnaire provides the data necessary for the formulation of questions in the second and subsequent rounds of questioning. This makes it necessary to use broad open-ended questioning in the first round while narrowing the field in the subsequent rounds (Powell, 2007).

4. The responses provided in the first questionnaire were evaluated utilizing QSR Nvivo and content analysis techniques. The results of this process led to the identification of 42 follow-up questions.

The second and subsequent rounds of questioning typically employs the use of scale scoring as the participants are asked to rate or rank previous responses (Hsu & Sandford, 2007). For the purposes of this study, an ordinal Likert-type scale was utilized for scoring responses and seeking consensus during the second and third rounds of questioning. The Likert-type 7-point scale is a popular tool for measuring attitudes because it does not rely on an expert panel (McNabb, 2008) and can use either ordinal or interval measurements (O'Sullivan, Rassel, & Berner, 2003). The scale utilized in this study is demonstrated below.

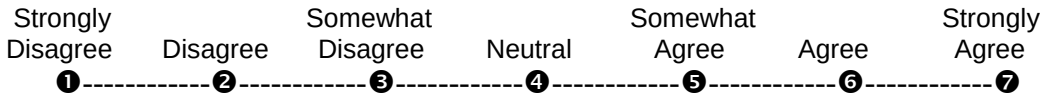

Figure 1. Scale scores used by respondents and their corresponding meanings.

5. Each participant was provided with the second questionnaire and asked to return it within 2 weeks.

The areas of agreement and disagreement between participants should become apparent based on the results of the rating system scores from the second round of questioning (Ludwig, 1994). As this study aimed to find consensus, the scores should

remain closely aligned among contributors with only a minor deviation. With the third questionnaire, the participants are to be asked to revise their responses to the second round of questioning based on the summary of results they received or to justify their position outside of the consensus of the group. This allows for further clarification of the data and the participants' perceived importance of the item (Hsu & Sandford, 2007). As positions are typically formulated in the first two rounds of questioning it was expected that there would be little to no increase in consensus during the third round of questioning as this is a common occurrence in Delphi studies (Jacobs, 1996).

Although the Delphi method has no firm procedure for establishing consensus, the final round of questioning will typically show a convergence of views (Linstone & Turoff, 1975). Some researchers believe that consensus is implied by the results (Beech, 1997) while others believe it is met when most participants in a study are in agreement (Butterworth & Bishop, 1995). Some have even theorized that consensus can be found in the stability of results over multiple rounds of questioning (Duffield, 1993). One common approach to achieving consensus is to set a percentage-level standard (Hsu & Sandford, 2007). Ulschak (1983) recommends accepting consensus if 80% of participants are within 2 categories on a 7-point scale. For the purposes of this study, Ulschak's recommendation was accepted.

6. Each participant was provided with the third questionnaire and asked to return it within 2 weeks. The third questionnaire included the scale scores for the

second questionnaires as well as summaries of the participant's justifications for their positions.

At the conclusion of the study, all the participants were debriefed. Debriefings typically occur when one or more aspects of a study were left undisclosed such as the goals, objectives, or purposes (Leech & Onwuegbuzie, 2008). As this information was provided to the participants from the onset, the debriefing was limited to presenting the findings of the study, keeping with the stated goal of expanding knowledge and finding consensus. Debriefings also allow for resolving potential tensions that arose between the participants and researchers during the course of the study (Onwuegbuzie, Leech, & Collins, 2008). This opportunity was afforded to all the participants during the debriefing.

7. Each participant was provided with the scale scores for the third questionnaires as well as summaries of the participant's justifications for their positions. Additionally, they received an e-mail correspondence thanking them for the participation and offering to answer any questions they had about the study.

Data Analysis

The method of data analysis used with the Delphi method varies according the purpose and structure of the study (Powell, 2007). The most common approach is to use content analysis techniques during the first round of questioning followed by ranking or rating techniques during the second and subsequent rounds (Jairath & Weinstein, 1994). This was the approach utilized for this study.

The use of content analysis techniques for the first round of questioning stems from the need to describe the attributes of the participants responses (Denscombe, 1998) while making inferences about variables discovered in the text through the objective analysis of it (Sproull, 1988). This allows for quantifying the participants texts in a clear and easily replicable format while eliminating contextual and implied meaning (McNabb, 2008).

Qualitative content analysis focuses on both the content and contextual meaning of responses (Tesch, 1990) and requires examining the language to classify responses into categories of similar meaning (Weber, 1990). These categories stem from both the explicit comments of participants as well as their inferred meanings (Downe-Wamboldt, 1992). One form of content analysis is conventional content analysis. It is typically used to describe a phenomenon when little or no existing theories or research literature exists. It is also beneficial for gathering data without developing preconceived notions about response categories (Hsieh & Shannon, 2005). These attributes made this approach ideal for this study based on the lack of extensive research or established theories as to the status of cyber warfare under international law.

With conventional content analysis, the researcher starts by repeatedly reading all data as a whole in order to reach a level of saturation as to the responses (Tesch, 1990). From there, responses are to be reread with specific attention paid to key terms that appear to capture the theme being conveyed. These key concepts are referred to as codes. (Morse & Field, 1995). Next, the researcher records their initial impressions and analysis of the responses, which aids in developing effective descriptive names for the codes.

These codes are then more easily sorted to reflect relation and linkage allowing for the development of meaningful categories (Patton, 2002). QSR Nvivo, a computer program designed for qualitative research, was used as an aid in the development of content analysis in this manner.

Role of the Researcher

The role of the researcher in a qualitative study may be split into a seven stage process: Thematizing, designing, interviewing, transcribing, analyzing, verifying, and reporting (Fink, 2000). Thematizing refers to determining the topic of the study, the reasoning for the topic, and the methodology to be utilized. Creswell (2007) stated that researchers should fall back on their own experiences and knowledge when creating a study. Based on Creswell's recommendation, the topic of this study was selected based on the researcher' experiences and education with information technology and international relations.

In qualitative studies, the researcher is to be considered an instrument of data collection meaning, among other things, that he or she should describe themselves in relation to the study including any biases or assumptions (Greenback, 2003). To this end, I hold undergraduate degrees in computer studies and political science as well as graduate degrees in both international relations and public administration. My educational background has permitted me to learn a number of computer programming languages and to pursue topics in international law including the laws of war. My formal education was supplemented by a background in computer programming having grown up the son of a military systems analyst. Over the last 12 years, I have instructed various courses in

computer topics and political science at the college level. My interest into a deeper understanding of the laws of war as they relate to cyber warfare was initially triggered by media reports of a successful penetration of the Iranian nuclear facility at Natanz with a computer worm later named Stuxnet.

Because of the researcher's central role in data collection and analysis it is necessary to minimize the potential for any biases, which are to be discussed further in the following section. One method used in this study to mitigate potential bias is the use of bracketing. Bracketing is the process whereby researchers recognize and subjugate their own biases and assumptions when describing a phenomenon (Given 2008). One way of doing this is to keep a research journal (Greenbach, 2003). During the course of this study, I maintained a journal which contained my feelings and reactions while interacting with participants as well as thoughts about myself and my past that surfaced in relation to the research.

Verification of Findings

The credibility of findings in a Delphi study hinges primarily on a decision trail that shows that the method of inquiry, composition of the participants, data collection procedures, justification of consensus levels, and the means of dissemination and implementation are all appropriate for the area of study (Powell, 2003). This study provides an extensive description of processes to allow for either verification through replication or application to other areas of common characteristics or traits. The use of snowball sampling also increases the credibility of this research as it further limits the potential for research bias in the selection of participants (Shenton, 2004).

Creswell (2007) described a need for researchers to clarify and announce any potential bias so as to allow the reader to understand the position of the researcher. As such, I affirm that I do not now, nor have I previously, worked in either the information technology or international law sectors. Additionally, I have no known ties to any of the participants of this study and do not have any expectation of profit based on any specific results of this study.

A question about the transferability of qualitative research exists as a potential limitation. Erlandson (1993) noted that many researchers believe that it is impossible to transfer generalizations because the observations used to form the generalizations are relevant only within the contexts in which they occur. Conversely, other researchers have proposed that while each study may be unique, they remain representative of the larger population group and, therefore, the validity of transferability cannot be summarily dismissed (Denscombe, 1998). In this study, I have provided comprehensive information on the settings, methods, and population used to allow those researchers who accept the transferability of qualitative research to apply the process utilized in this study to their own research and, therefore, further the dependability of this study through replication.

Lastly, to assist in the confirmability of results, the methodology used allowed all participants to review the results after each round of inquiry. This provided an opportunity for them to correct or expand upon their responses during the following round. In doing so, each respondent was able to confirm the accurate representation of their individual views and, therefore, the results for the group.

Issues of Trustworthiness

One limitation with the utilization of the Delphi method is the time involved and its effect on participation. Many researchers recommend a maximum of 45 days for the collection of data (Delbecq, Van De Ven, & Gustafson, 1975, Ulschak, 1983, Ludwig, 1994) with Delbecq, Van De Ven, and Gustafson (1975) stating that participants should be encouraged to respond within two weeks of receipt of a questionnaire. Compounding the problem is that weeks may pass between any two rounds of questioning (Ludwig, 1994). The length of the study and inactivity that occurs between rounds has the potential to be a challenge to participation rates. This requires that the researcher take an active role in maintaining participation levels (Hsu & Sandford, 2007). Modern technology helps to shorten the time involved and, therefore, assists in maintaining participation levels. The delivery of questionnaires and responses can occur almost instantaneously while their preparation and evaluation can be processed faster and more conveniently using electronic means (Altschuld, 1995).

Another limitation is the nature of the measures and validation used with the Delphi method. Sackman (1975) has criticized the Delphi method for its inability to utilize established scientific validation and the reliability of its measures. This argument has been countered by proponents of the Delphi method who state that it should not be held to the same scientific standards as many other methodologies as it was designed to allow for the studying of a phenomenon that lacks conclusive data (Murphy et al, 1998).

The use of researcher feedback, while imperative in the Delphi method, may have the unintended consequence of shaping the opinions of the participants by inadvertently

moving responses towards the researcher's biases (Altschuld, 1995). Studies have shown that respondents to a Delphi questionnaire will alter their answers if given erroneous feedback (Scheibe, Skutsch, & Schofer, 1975). This stems from participants potentially feeling pressure to conform to the ratings established by the group after they are made aware of the deviation of their own responses (Witkin & Altschuld, 1995). To help address this potential limitation participants were instructed at the onset of the study that divergence from consensus is an acceptable and valid response.

Summary

A Delphi method of inquiry was selected for this study primarily because this methodology allows for a more accurate assessment by the respondents than would be found in a group setting (Rowe, Wright, & Bulger, 1991). This stems from participants in group settings tending to create a hierarchy of dominance among contributors (Murphy et al, 1998) which may cause non-dominate participants to become inhibited (Rowe, Wright, & Bulger, 1991). The participants for this study are recognized as experts in cyber warfare and international law based on published scholarly works and their credibility with their colleagues. This coupled with the anonymity that this study provided the respondents should have mitigated this potential effect.

Data collection was designed to occur over a period of 8 weeks and three rounds of questioning. The first questionnaire consisted of open-ended questions that granted the respondents a wide range of freedom to elaborate and, therefore, allowed for the discovery of major themes. In subsequent rounds of questioning, the major themes were narrowed as participants revised their responses. After three rounds of questioning, a

consensus of opinion based on a Likert-type 7-point scale was expected to have been met. Consensus was measured based on 80% of responses being within 2 categories on the Likert-type scale. Possible verification of the findings reported in the following chapter has been made possible based on the extensive presentation of the methodology and decision trail used for this study. This documentation will allow for replication and application in similar studies as well as provide clarification as to any potential researcher bias.

In the following chapter, an in-depth description of the data and results of the study is provided to include methods of data collection, analysis, and trustworthiness as well as questions, responses, and scale scores for each round of inquiry.

Chapter 4: Results

Introduction

This study has explored the legality of cyber warfare operations under international law in order to fill a gap in the current literature. To meet this end, 16 scholars in the fields of international law and cyber warfare participated in three rounds of inquiry utilizing written surveys to determine their opinions on various themes affecting this topic. Specifically, this study's aim was to answer the following research questions:

1. At what point do computer virus attacks elevate to the level of use of force or armed attack under international law?
2. What limitations in targeting exist with initial and reprisal cyber attacks?
3. How does the unique nature of cyber warfare affect the concept of neutrality?
4. What impediments currently exist in the development of legal limitations on cyber warfare?

This chapter presents a focused review of the findings for this qualitative content analysis study. The process will consist of describing the participants and settings, methods of data collection, storage, and analysis, as well as the results and data verification that occurred and as described in Chapter 3. The results presented will include both quantitative data depicted in numerous figures based on responses to questions scored on a Likert-type scale as well as summaries of the written justifications for these scores as provided by the participants.

Setting and Demographics

The research proposal for this study received Walden University Institutional Review Board approval on February 25, 2014 under approval number 02-24-14-0140351 with an expiration date of February 23, 2015. Solicitation of participants began on March 12, 2014 and concluded on March 21, 2014 with affirmative responses from 18 individuals. Recruitment occurred by e-mail invitation to individuals in the fields of cyber warfare and international law based on their scholarly records in these fields. Additional participants were identified through the use of snowball sampling as those invited to participate were asked to nominate potential contributors who they deemed qualified to be included in the study.

Of the 18 original participants, 10 came from a predominantly international law background while the remaining 8 were primarily trained in information technology. One participant from each category withdrew during the course of the study. Additionally, 12 of the 18 held academic positions at the time of their solicitation while 6 principally worked in an information technology field in either the private or government sectors; 2 and 4 individuals, respectively. Both individuals who withdrew from the study came from the academia group. Lastly, the demographics of the participants included ten men versus eight women, nine and seven, respectively, at the conclusion of the study, representing three separate predominantly English speaking countries.

Data Collection

The first round of inquiry began March 22, 2014 and was scheduled to conclude on April 13, 2014. Because all participants returned their completed questionnaires by

April 9, 2014 the first round on inquiry was terminated early. Follow-up questionnaires could only be created after a thorough review of the results for the first round of questioning and an additional Institutional Review Board assessment to mitigate any potential ethical concerns. Questionnaires 2 and 3 were submitted to the Walden University Institutional Review Board on April 15, 2014 and received approval for usage on April 22, 2014. This authorization allowed for the resumption of data collection on April 22, 2014 with the second round of inquiry concluding on May 6, 2014. The third and final round of inquiry lasted from May 16, 2014 to June 6, 2014. 16 participants from the original group of 18 contributed for all three rounds of data collection with one departing between the first and second rounds of inquiry and one doing so during the course of the second round.

All three rounds of inquiry consisted of e-mail correspondence between the participants and the researcher. The questionnaire used during the third round included the results from the second round of inquiry as feedback for the participants to review before responding to the same questions. The feedback consisted of both the scale scores and a synopsis of the narratives used to justify those scores. The use of synopses rather than full text was necessary to help protect the identity of the participants. Most of the respondents had been published in peer reviewed journals leaving the possibility that specific phrases or writing patterns may have left them open to identification. All communication occurred by e-mail leaving the actual setting for the participants' completion of the questionnaires unknown.

To further ensure the respondents' anonymity, all e-mail correspondence was downloaded to a password protected home computer and permanently removed from the e-mail account. Upon downloading, each was coded with an alpha-numeric sequence that identified each participant only to the researcher and any information that could identify the contributor was expunged. Questionnaires were saved within files established for each participant using a 256 bit AES encryption algorithm. These files were not printed or transferred to another location.

Data Analysis

Analysis of the data began using nine open-ended questions during the first round of inquiry. The narratives provided were entered into QSR Nvivo to assist in locating common themes which were then again reviewed in their original form and rewritten to create the questions used during the second and third rounds of inquiry. The findings for the second and third rounds of inquiry were quantitatively analyzed through the ranking of scale scores given by the participants and included summaries of the respondents' written justifications for their scores.

Evidence of Trustworthiness

The evidence of trustworthiness for this study began with the original solicitation of the participants. As part of the solicitation, I identified myself to the potential participants and described my role as the researcher in the study. Specifically, I expressed to each contributor that I had no personal stake in the results and throughout the duration of the study did not communicate any personal beliefs or experiences that may have influenced the responses.

The credibility of findings in a Delphi study is based primarily on the decision trail. The trail must properly and thoroughly represent the method of inquiry, composition of the participants, data collection procedures, justification of consensus levels, and whether the means of dissemination and implementation are all appropriate for the area of study (Powell, 2003). To meet these ends, an exacting methodology was described in Chapter 3 of this study and adhered to rigidly. Following the given methodology should allow other researchers to mimic these procedures in an attempt to confirm or expand upon the results of this study. This includes the use of snowball sampling which Shenton (2004) stated would help to minimize research bias, as well as accepting the 80% standard recommended by Ulschak (1983) for meeting a consensus in a Delphi study.

One intended method for establishing the trustworthiness of this study that was ultimately abandoned was the release of verbatim narratives when reporting the results. It became apparent after the first round of inquiry that some of the respondents had the tendency to use specific catch phrases or syntax and a review of published works showed some of these same idiosyncrasies. It was determined that these would need to be eliminated in order to safeguard the identities of the contributors. Therefore, abridged comments were used when formulating the questions for the subsequent questionnaires and when providing feedback to the participants. This same precaution was utilized when drafting the results of this study. Altering the written responses given by the participants when providing feedback could potentially allow for the unintended incorporation of the researchers own biases but, this is already recognized as a potential

phenomenon within Delphi studies (Altschuld, 1995). The use of feedback and multiple rounds of inquiry utilizing the same questions and formats should have a mitigating effect on potential bias as all the respondents were able to review these remarks and comment on them before the conclusion of the study. Additionally, the truncated comments should remain specific enough for comparison to other like studies.

Lastly, the length of a Delphi study has been shown to have some effect on the trustworthiness of the results because of retention rates. It has been recommended that Delphi studies not exceed 45 days for this reason (Delbecq, Van De Ven, & Gustafson, 1975, Ulschak, 1983, Ludwig, 1994). This study was able to surpass this figure without any further attrition among the participants as the 2 that withdrew from the study did so early on. The retention rate for this study was 88.9%.

Results

In an attempt to answer the research questions, the questionnaires were divided into related sections based on categories similar to those reflected in the literature review found in this study. These groupings allowed for easier comparison of results to determine themes and trends in the following chapter. Each question is provided below along with a summarization of written responses and followed by a table showing scale scores for each round.

Use of Force and Armed Attack Designations

Question 1. An effective formula for determining whether a cyber attack has reached the level of use of force or armed attack under international law is by comparing its scope and effect to kinetic attacks.

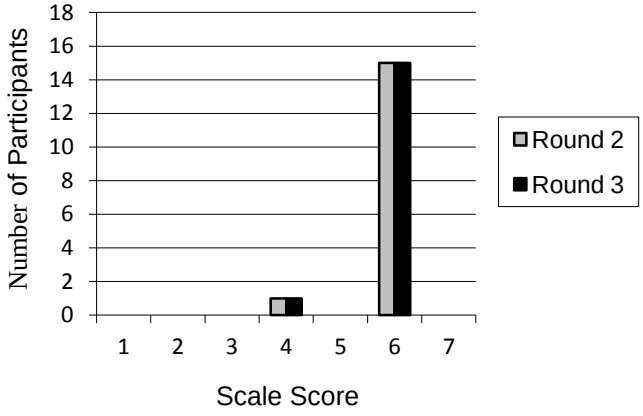

Figure 2. Scale score responses for Question 1.

During both rounds of inquiry, the consensus was to agree with this statement. Among the respondents who agreed with the statement, the belief that the laws of armed conflict do not differentiate between kinetic and cyber attacks was often referenced. Additionally, some felt that this formula had only a few areas of ambiguity which could generally be solved using scope, duration, and intensity as a measuring stick. The dissenting vote was based on the belief that attribution issues with cyber warfare and determining whether it was truly an attack rather than a hugely coincidental conflagration of errors meant that it may work in some instances but not for others.

Question 2. Although a cyber attack may fall below the standard of use of force or armed attack they most likely would still be deemed illegal under criminal law.

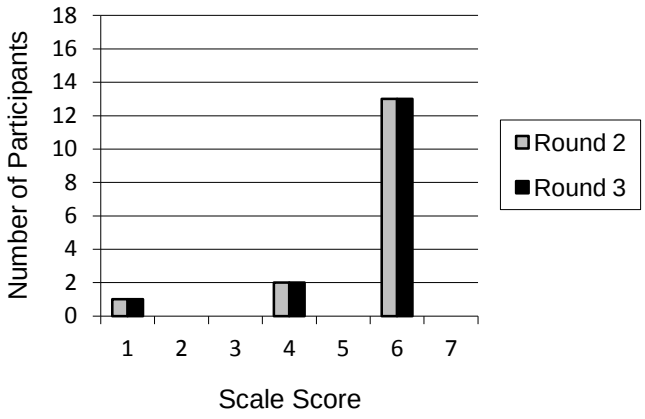

Figure 3. Scale score responses for Question 2.

During both rounds of inquiry, the consensus was to agree with this statement. The respondents' belief was based primary on the codification of certain cyber activities such as illegal access, data and system interference, and the general misuse of computer and network devices as criminal offenses under the Budapest Convention on Cybercrime (2001). Conversely, the sole dissenting opinion was based on the belief that it would be impossible to evaluate the statement without knowing more about the nature of the cyber attack, the specific criminal law paradigm that applies, and additional factors such as national jurisdiction.

Question 3. To classify a cyber attack as an armed attack under international law the cyber attack must threaten the territorial integrity or political independence of the offended state.

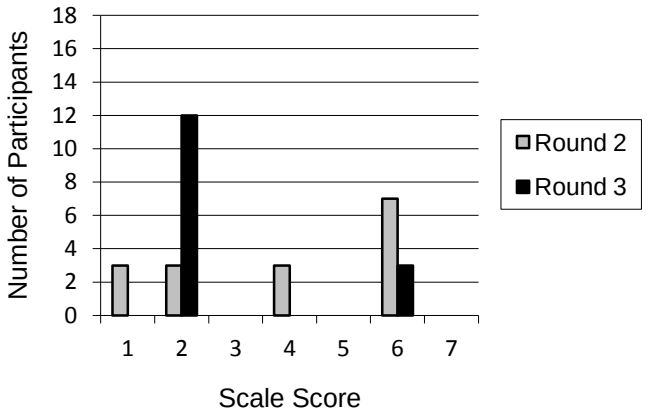

Figure 4. Scale score responses for Question 3.

During the second round of questioning, opinions varied greatly with this question as only one more participant agreed with it than disagreed and three of the respondents took a neutral position. Among those disagreeing with the premise, there was a belief that this definition would exclude certain acts such as the Japanese bombing of Pearl Harbor in 1941 or the terrorist attacks of September 11, 2001. For this reason, these respondents determined it was not an appropriate tool for measuring an armed attack. Others who disagreed with the premise did so based on the belief that the definition better fit a use of force designation than an armed attack designation under international law. While many of the proponents of this statement did so based on a belief that it was consistent with international law several waivered in this view during the third round of questioning after being exposed to the Pearl Harbor analogy. This was the primary reason given for the strong shift in opinions towards disagreeing with the question during the final round of inquiry. Based on this shift in opinion the minimum standard for consensus was met.

Question 4. A cyber attack constitutes a use of force whenever it targets critical national infrastructure.

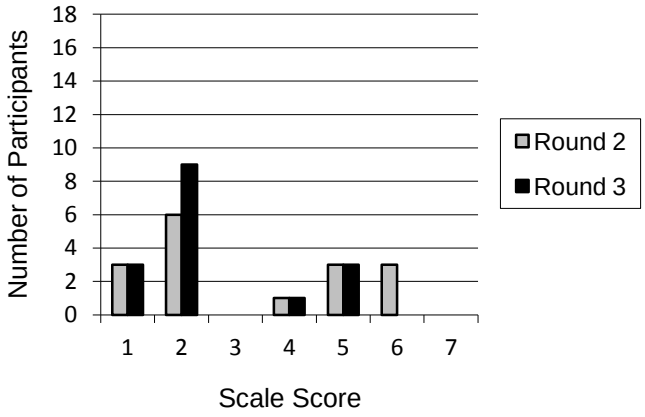

Figure 5. Scale score responses for Question 4.

During the second round of inquiry, results for this question were varied over 5 different points on the 7-point scale. Those disagreeing with the given statement did so based on the belief that it was inconsistent with international law and specifically in that Article 2(4) makes no reference to critical national infrastructure. Additionally, it was believed that there was a lack of state practice to make this assertion. Among those who agreed with the question, some opinions were qualified with statements including that the targeting of critical national infrastructure is not a sufficient criteria by itself but a factor in the overall determination of whether an attack constitutes a use of force. During the third round of inquiry a number of those who had qualified their support for the principle of the question changed their scores based on the provided feedback. This shift led to a

strong majority opinion to disagree or strongly disagree with the question but fell short of the required number of responses to reach a consensus.

Question 5. A significant loss of control over a computerized system is serious enough to warrant a use of force designation under international law.

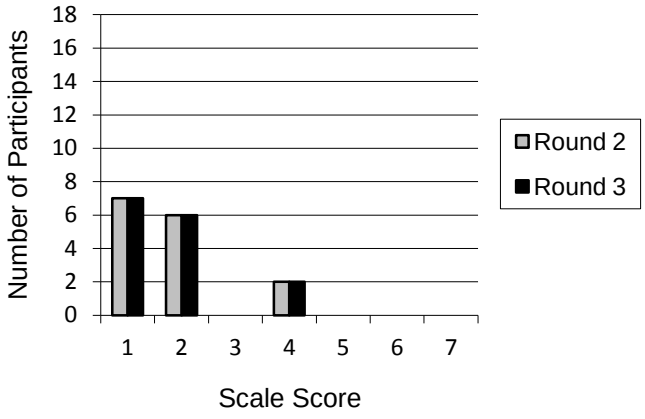

Figure 6. Scale score responses for Question 5.

A clear consensus against the given statement was achieved during both rounds of inquiry. The consensus of opinion was that the loss of a single system would be a violation of sovereignty but not a use of force under international law. Additionally, it was stated that a use of force designation needs to be based on the effects of the attack rather than just the identity of the target. Lastly, it was posited that a design flaw or bug could have led to the loss of control while the cyber attack had no intention of causing such an effect. Neutral opinions on the question were based on the need to know more about how the loss of control was achieved and whether the computerized system was civilian or government.

Question 6. Because the Stuxnet virus caused severe physical damage to equipment within the Natanz nuclear facility it would qualify as an armed attack.

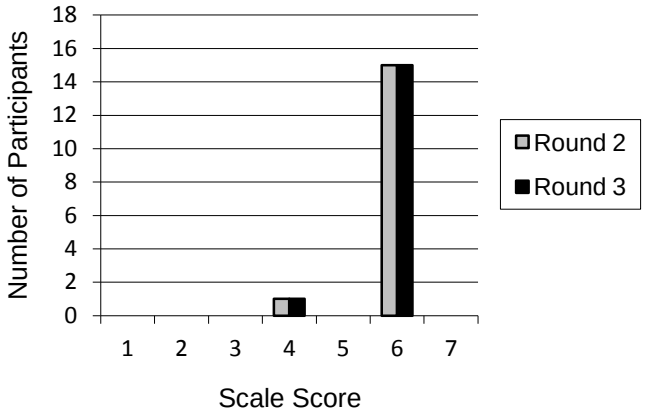

Figure 7. Scale score responses for Question 6.

During both rounds of inquiry, a consensus to agree with the question was garnered. All participants agreeing with the statement believed that the nature of the damage rather than the method of delivery was the primary principle of importance as long as the impairment was tangible. The one contributor who was neutral on the topic did so because of concerns as to how Stuxnet was introduced to a closed facility. Another respondent attempted to dispel this concern by declaring that acts of sabotage can be classified as an armed attack when the results are similar to a bomb.

Question 7. A use of force or armed attack designation can be assigned collectively to cyber attacks that reoccur in a short period of time even though the individual attacks do not warrant this designation.

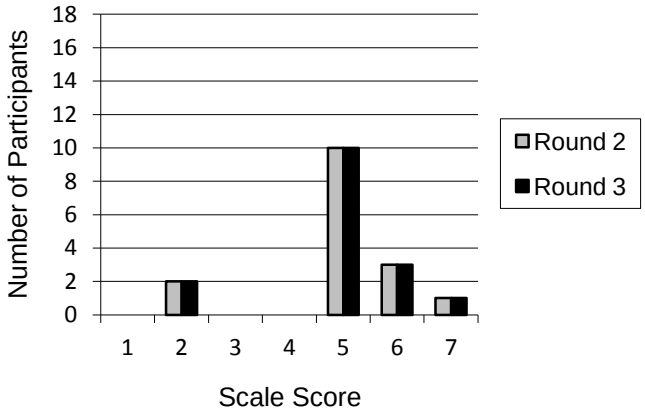

Figure 8. Scale score responses for Question 7.

A consensus to somewhat agree or agree with this question was met during both rounds of inquiry. A majority of participants somewhat agreed with the question based on the belief that the premise was reasonable with some adding that attribution would need to show the same or related actors were responsible for the related attacks. Additional respondents somewhat agreed with the caveat that their agreement was based on the cumulative effects of the attacks being serious enough to warrant either a use of force or armed attack designation. The one respondent who strongly agreed with the statement justified their response based on the belief that kinetic attacks generally comprise a set of actions in time much the same way that multiple cyber attacks do. Those who disagreed with the given question did so out of concerns as to how to delineate the starting and ending period used when determining the cumulative effects.

Question 8. A cyber attack against a major economic entity, such as the New York Stock Exchange, that results in no loss of life or physical damage may still meet the requirements of armed attack under international law.

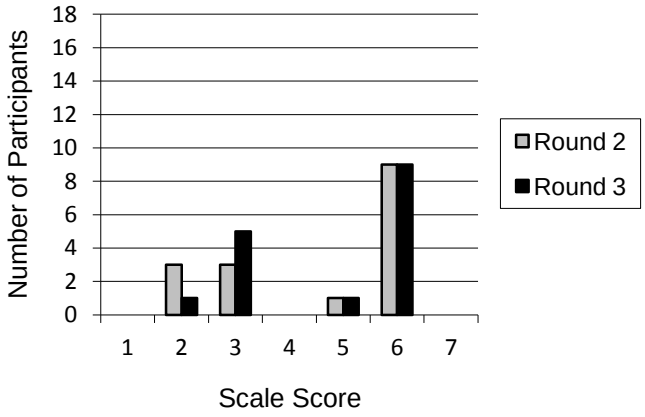

Figure 9. Scale score responses for Question 8.

After two rounds of questioning, a consensus as to the validity of this question could not be reached. The majority of respondents agreed with the premise of the question based on the belief that damage need not be physical and specifically if it was severe enough. Two respondents equated data damage with that of physical attacks and found no difference between them. Among those disagreeing with the question, there was a belief that non-physical damage would be unlikely to reach levels necessary for an armed attack designation under international law. Additionally, some felt that even if such levels could be reached the necessary significance of the entity on the national economic system would severely limit which targets could be worthy of such a designation.

Question 9. A cyber attack that alters data or the functionality of a system, but causes no direct or indirect physical damage, cannot be classified as an armed attack under international law.

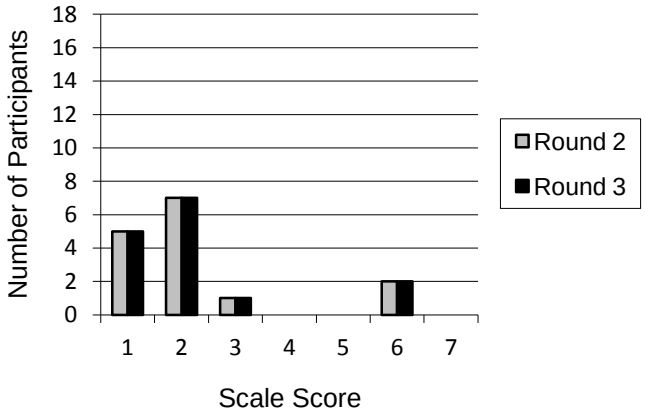

Figure 10. Scale score responses for Question 9.

During both rounds of inquiry, responses to the question were primarily to disagree or strongly disagree with the premise. A consensus was reached based chiefly on the belief that changing the functionality of a system is a form of damage since functionality of a system is part of its integrity. Some disagreeing with the statement included a caveat that the specific nature of the effects would also have to be taken into account. Dissenting opinions were based on the belief that altering data and functionalities are most likely reversible and, therefore, may not constitute damage.

Question 10. A cyber attack that has been foiled by passive defenses, and which otherwise would have resulted in serious physical damage or loss of life, may still be categorized as an armed attack.

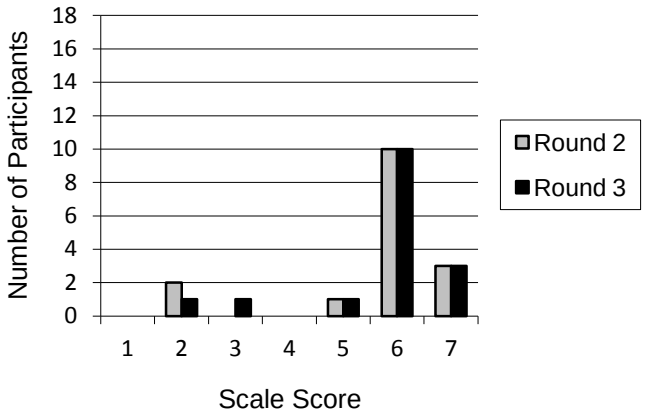

Figure 11. Scale score responses for Question 10.

During both rounds of inquiry, there was a consensus to agree or strongly agree with the question. The justifications for these opinions were based primarily on the intent of the attacker and not the end results. One participant likened this scenario to that of a missile launched against a city that falls harmlessly short of its target. Because they believed such an action would be considered an armed attack under international law, they felt the same of the failed cyber attack. Dissenting opinions were primarily based on the fact that no actual damage occurred with the failed attack.

Proportionality, Necessity, Immediacy, and Attribution

Question 11. For cyber attacks, immediacy should be predicated on the time reasonable attribution is made rather than when the effects of the attack are detected.

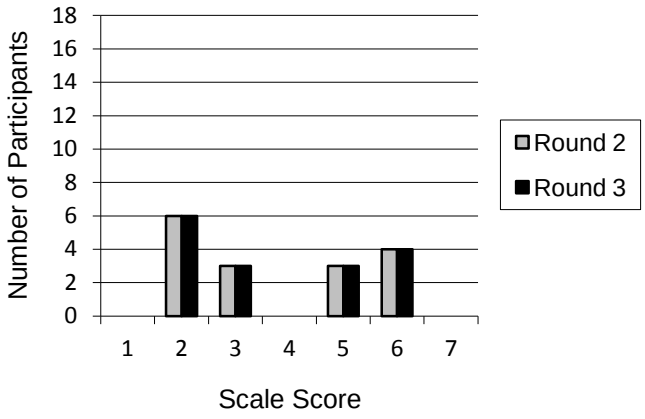

Figure 12. Scale score responses for Question 11.

After two rounds of inquiry, no consensus or clear majority opinion was achieved nor were any of the participants willing to move from their original opinions. Among those who agreed with the question there was a belief that doing so would allow underdeveloped countries time to respond as well as allow all countries the necessary time to reasonably identify the attacker and their intent. Even among those who agreed with the premise of this question there was recognition that it could lead to abuses and that current international law may not allow for it. This position was also taken by a number of participants who opposed the assertion of the question with some these individuals believing that international law requires that immediacy be predicated on the effects. Among those who somewhat disagreed with the question, there was a belief that international law is still developing in this area, and the question may be valid in the future. Lastly, one participant took issue with the belief that additional time should be afforded to underdeveloped countries because they felt that each country must be held to the same standard.

Question 12. Because the Stuxnet virus was discovered so long after it began degrading the equipment in the Natanz nuclear facility, Iran lost the legal right under international law to respond in self-defense.

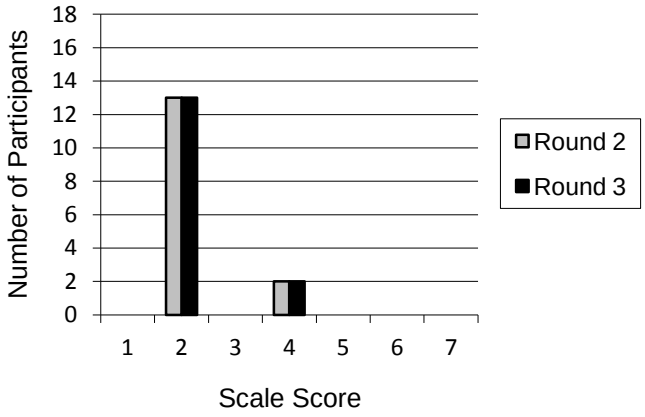

Figure 13. Scale score responses for Question 12.

During both rounds of inquiry, a consensus to disagree with the question was reached. Consensus was arrived at primarily because of the belief that immediacy should be based on the time of effects or attribution neither of which had previously occurred. One respondent equated this scenario to that of a biological attack which may have a delayed recognition of effects but still affords the victimized state the right to respond. The two participants who were neutral on the question did so for different reasons. One felt that the law wasn't fully developed enough to make a sound decision and envisioned it being set in the future based on state practice. The other neutral opinion came from a participant who took issue with the validity of the question because it assumed that the Stuxnet virus could be categorized as a weapon.

Question 13. The concept of self-defense under international law is problematic when applied to cyber attacks. The stated point of self-defense, to disarm the attacker, is difficult to accomplish in cyberspace considering that the attacker is most likely not limited to a specific computer, server, or facility.

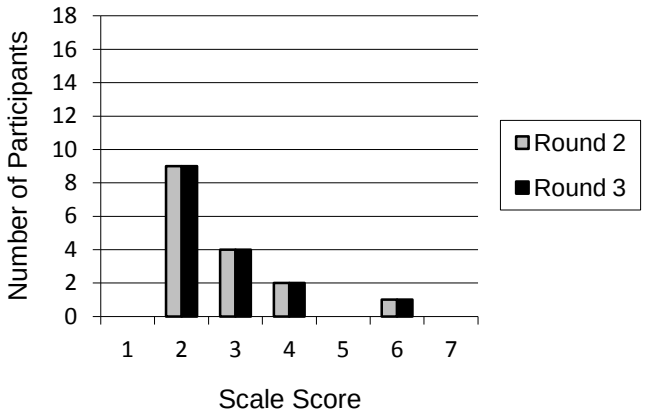

Figure 14. Scale score responses for Question 13.

During both rounds of inquiry, the consensus was to disagree or somewhat disagree with the question. Responses to this question included varying justifications even among those who scored the question the same. Among those who disagreed, there was a belief that the assumption of the question, that self-defense aims to disarm an attacker, is flawed. Some respondents added to this by stating that the role of self-defense is to prevent an attack from succeeding. This point was additionally raised by one participant who was neutral on the question. Others disagreed with the premise of the question on technical grounds stating that software will be the same across multiple systems providing a focal point for counterattack. Lastly, some felt that the question could also apply to kinetic attacks.

Question 14. The laws of armed conflict would require that any response to a cyber attack remain in the cyber arena to meet the obligation for proportionality.

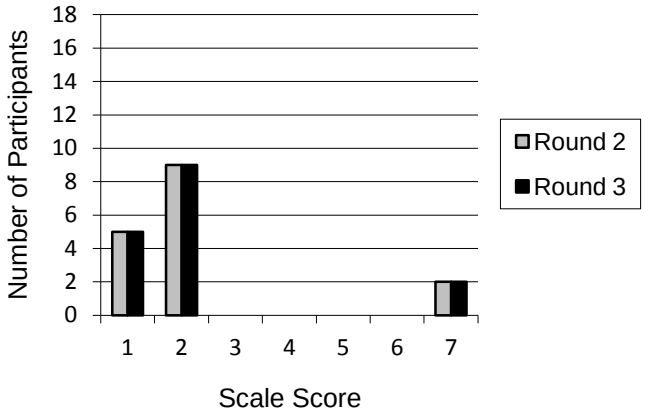

Figure 15. Scale score responses for Question 14.

During both rounds of inquiry, the consensus was to disagree or strongly disagree with the question. This position was most often justified based on the belief that the response only needs to be proportional in effects rather than in methods. Analogies were provided that other forms of attack such as assassinations or the use of nuclear, biological, or chemical weapons do not require responses in kind. Among the 2 participants who strongly agreed with the question, the belief existed that cyber warfare is too different from any other type of warfare making it difficult to justify using kinetic or other physical means in response to a cyber attack.

Question 15. Necessity would be difficult to argue in response to a cyber attack, as any response by the offended state would most likely not curb the ongoing effects of the initial cyber attack.

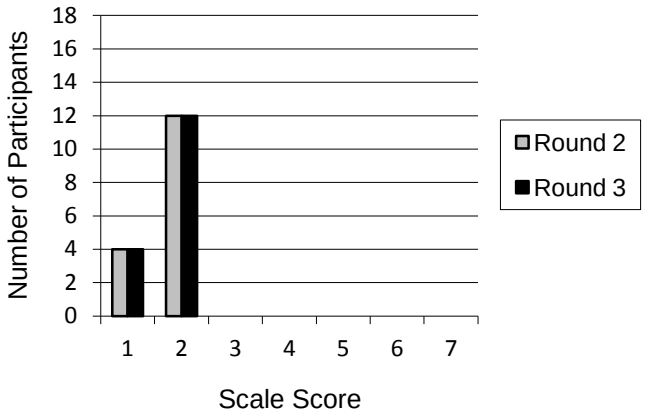

Figure 16. Scale score responses for Question 15.

During both rounds of inquiry, the consensus was to disagree or strongly disagree with the question as all participants scored their responses in one of the two categories. Participants primarily justified their score based on the belief that the response would be justified in an attempt to overcome any further provocations even if the effects of the initial cyber attack had run their course. One example of this was a counterattack that would monopolize the attacking state's resources limiting their ability to continue to attack.

Question 16. The fact that a cyber attack has originated from a government-operated computer system is not sufficient enough evidence to attribute the attack to the state or to take action against the state.

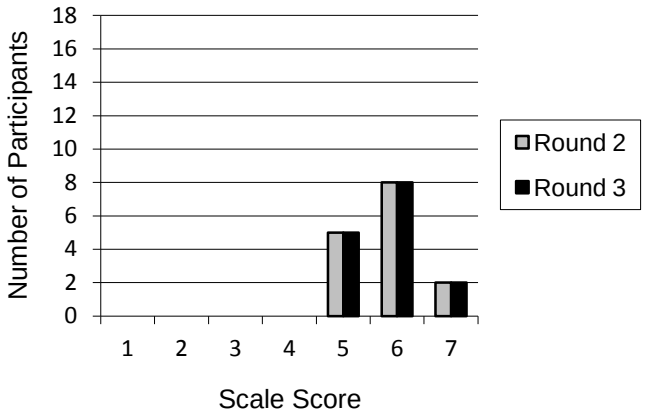

Figure 17. Scale score responses for Question 16.

During both rounds of inquiry, a consensus was reached to either agree or somewhat agree with the question. Justifications for these scores were based primarily on the belief that private individuals or foreign state actors may have commandeered the system or even spoofed it such as with distributed denial-of-service or botnets. Some respondents who somewhat agreed with the statement believed that it was possible to sufficiently determine attribution in some cases, but most would require further investigation.

Question 17. Cyber attacks may be launched for defensive purposes in the name of necessity even when the identity of the aggressor cannot be clearly attributed.

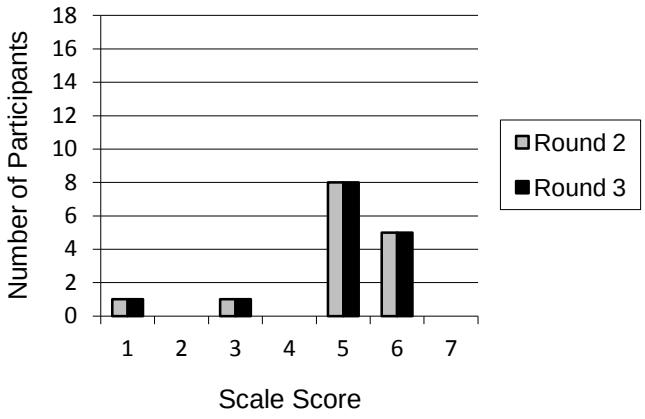

Figure 18. Scale score responses for Question 17.

During both rounds of inquiry, a consensus to agree or somewhat agree with the question was reached. Among the consensus, a number of respondents provided caveats to their determination. Some felt that the statement was true only if essential interests were involved while others questioned why means other than an attack could not sufficiently address the state's concern. Additional participants stated that attacks could be launched at source infrastructure in order to resist an attack, even if the identity of the attacker was not determinable. The participant who strongly disagreed with the question did so based on their belief that attribution requirements could not be legally weakened for counterattacks.

Means and Targets of Cyber Attack

Question 18. The concept of anticipatory self-defense only applies to instances when a cyber attack is a component of a greater armed assault.

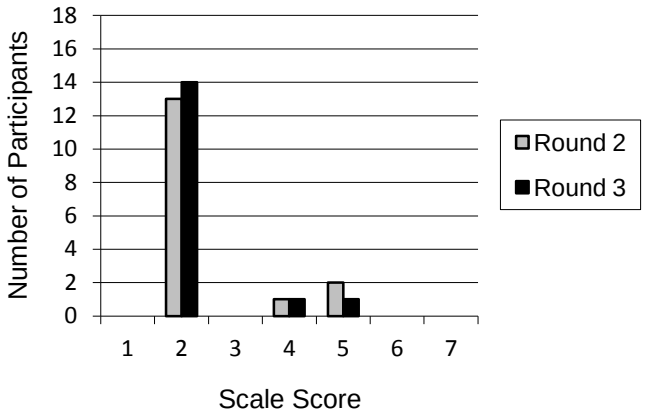

Figure 19. Scale score responses for Question 18.

During both rounds of inquiry, a consensus existed to disagree with the question. Justifications among these participants typically consisted of a belief that the standard is for an armed attack regardless of the modality. Some believed that the decision to act was solely a political one. Dissenting opinions were based on the belief that anticipatory self-defense is rarely legal under international law and additional issues with attribution would only raise a cyber attack to this level if it was a component of a larger, non-cyber attack.

Question 19. No target, civilian or government, has complete legal protection from a cyber attack if there is an overriding military necessity.

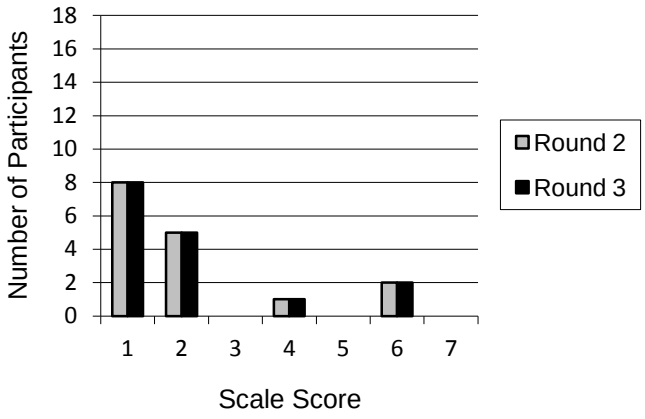

Figure 20. Scale score responses for Question 19.

During both rounds of inquiry, a consensus was reached to either disagree or strongly disagree with the premise of the question. Those within the consensus used various analogies such as replacing the word "cyber" with "nuclear" in an attempt to support their position. Other participants felt that accepting the premise of the question would violate *jus cogens* that necessity cannot justify. Other respondents who disagreed with the question felt that accepting the premise would too easily lead to abuses such as targeting medical facilities. The single neutral opinion accepted the possibility that the question may be true, but felt more information was needed as to the proportionality and soundness of the justification to claim necessity. Those agreeing with the question took the opinion that the statement was in keeping with international norms and therefore did not violate *jus cogens*.

Question 20. A cyber attack, that uses malware that cannot be controlled after being deployed, would be illegal under international law.

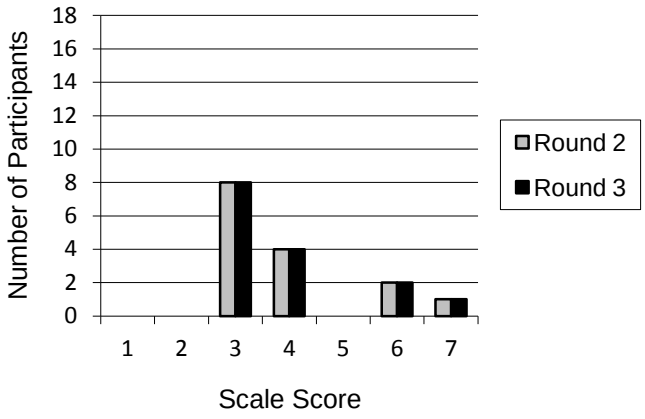

Figure 21. Scale score responses for Question 20.

During both rounds of inquiry, a consensus was reached to slightly disagree or be neutral on the question. Some of those slightly disagreeing did so based on the belief that international law only requires that states consider the possibilities of collateral damage and do what is reasonable to limit it rather than a requirement to eliminate it all together. The Stuxnet virus was used as an example as it continued to spread throughout various countries but was removable and caused no real negative effects outside of the Natanz facility. Among those neutral on the question, there was the belief that if the malware remained within military systems they may be legal under international law. Dissenting opinions were made primarily based on the belief that the effects of such attacks would violate both the proportionality and discrimination principles of the laws of armed conflict.

Question 21. To remain legal under international law, cyber-defense systems may not have an active component that automatically responds to a cyber attack with offensive measures of its own.

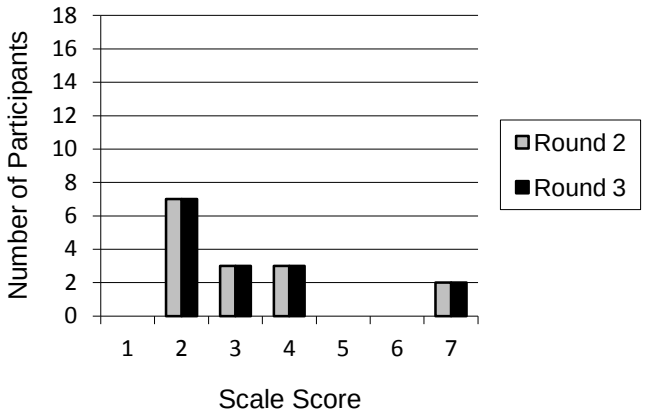

Figure 22. Scale score responses for Question 21.

After two rounds of inquiry, no consensus of opinion was reached for this question. The majority of respondents either disagreed or somewhat disagreed with the premise. Opinions among this group were based primarily on the nature of the offensive measure leaving most responses as a matter of national discretion. Neutral opinions were also based on the nature of the offensive measure but gave less credence to the concept of national discretion. Those strongly agreeing with the question cited issues with attribution as they believed that automated active components would most likely lead to responses that erroneously target neutral states. This would cause the defensive systems to be categorized as unprovoked attacks rather than defensive counterattacks.

Question 22. Cyber weapons may be illegal under international law because governments cannot reasonably maintain control over them or be held accountable for their use.

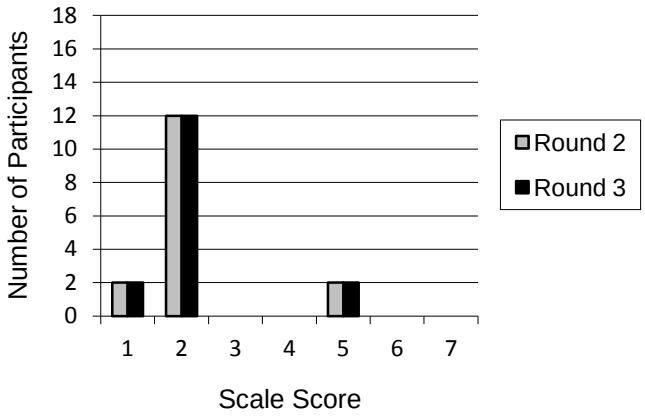

Figure 23. Scale score responses for Question 22.

During both rounds of inquiry, the consensus was to either disagree or strongly disagree with the question. Responses were primarily clustered around whether cyber weapons can be reasonably controlled. Among those in the consensus, there was a belief that the level of control that exists over most cyber weapons meets the requirement under international law. Among those agreeing with the question, it was determined that cyber weapons do not meet this requirements because they require more stringent controls that kinetic weapons. This was based on multiple factors such as their increased transferability and deployment.

Question 23. Civilians maintain their non-combatant protections under international law even when directly participating in cyber attacks.

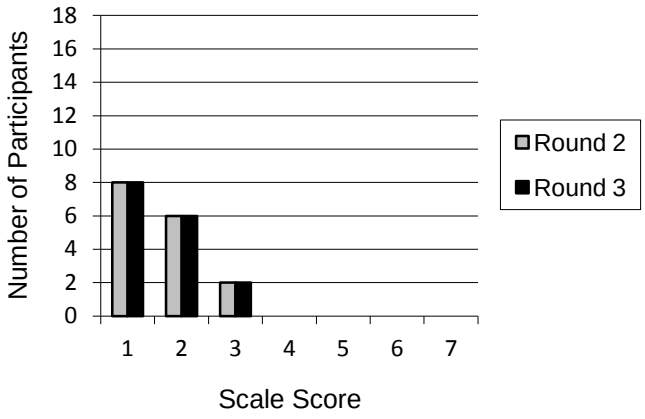

Figure 24. Scale score responses for Question 23.

During both rounds of inquiry, the consensus was to either disagree or strongly disagree with the question. The common belief among the consensus was that civilians forfeit their protections under international law when they are involved in offensive cyber operations. An example provided by one participant was that playing an active role in a cyber attack is considerably worse than working in a munitions factory but factory workers forfeit their protections under the laws of armed conflict. Among those somewhat disagreeing with the question, the decision as to the status of civilians is based on the nature of cyber attack with only those causing death or physical destruction leading to a forfeiture of legal protections.

Question 24. A cyber weapon designed to look like legitimate civilian network traffic would violate the prohibition against perfidy.

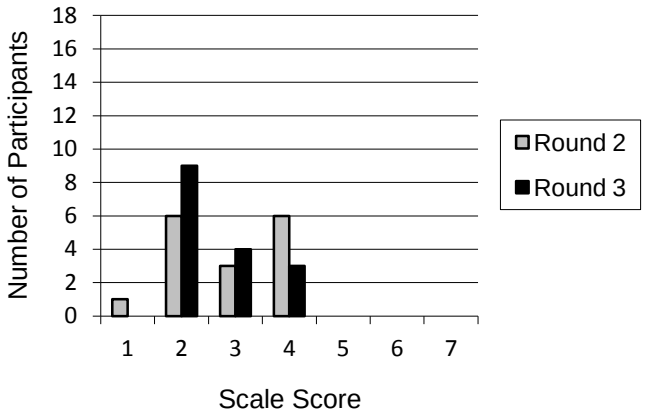

Figure 25. Scale score responses for Question 24.

Results for the second round on inquiry were inconclusive with no consensus or majority of opinion. During the third round, after the opinions of the respondents were shared with all participants, a consensus was reached to either disagree or somewhat disagree with the question. The consensus of opinion was primarily based on one of two factors. The first was to disagree based on the belief that laws of perfidy apply only to active agents and therefore do not cover network traffic. Also, some took this further to state that perfidy would only apply if the cyber attack led to a loss of life as property destruction would not be covered. The second justification was based on current engineering standards as it was said to be difficult to prove an intentional design issue rather than just a normal design. This was important to some participants because perfidy only covers acts of treachery.

Question 25. A cyber weapons designed to look like the legitimate network traffic of an international organization, such as the United Nations or Red Cross, would be illegal under international law.

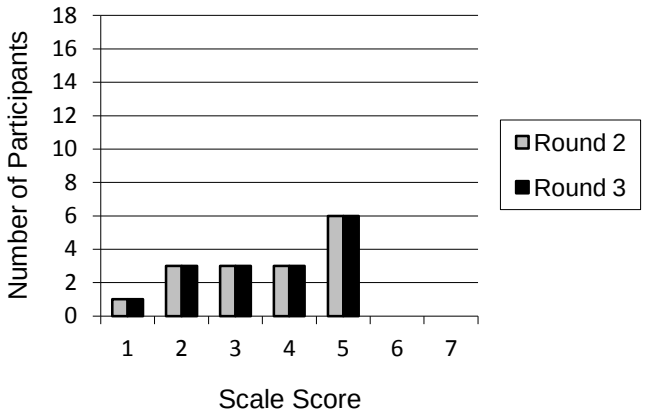

Figure 26. Scale score responses for Question 25.

For this question, no clear consensus could be reached during either round of inquiry. The most common response given was to somewhat agree primarily because the organizations mentioned have protected status under the laws of armed conflict. One caveat given was based on all network traffic looking similar as they use the same protocols, such as IP, TCP, and HTTP. Based on this some respondents felt a cyber weapon would have to be intentionally designed to look like it came from a protected organization. The one respondent strongly disagreeing felt that based on current engineering standards this could not be done. Specifically, they felt that it would be impossible to prove that it was an intentional design rather than a normal design that made the cyber weapon appear to be from one of these organizations. Among some of the remaining respondents who took a negative view of the question, there was the belief that perfidy only applies to active agents such as computer programs and not the communication to deliver it.

Question 26. It is conceptually impossible to perform an economic blockade solely by cyber means; therefore, any denial of service attack against a state's industries cannot be labeled as such.

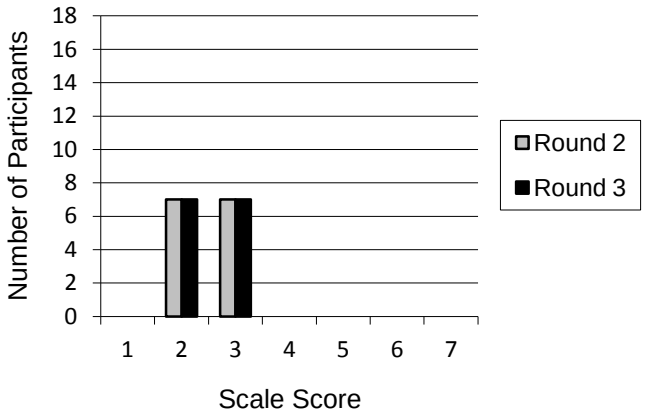

Figure 27. Scale score responses for Question 26.

During both rounds of inquiry, a consensus was reached to disagree or somewhat disagree with the question. Among the respondents, there was an opinion that a blockade of first or second world economies could be performed through cyber means but not third world economies. This was deemed especially true because a blockade need not stop all economic activity or be completely effective to be labeled a blockade. Some respondents also felt that the development of cyber weapons and online economic activities will most likely increase the ability to economically blockade a state in the future. It should also be noted that two participants whose specialization is in international law felt their knowledge of cyber operations was too limited to definitively respond to the question.

Neutrality and a Cyber Global Commons

Question 27. The Hague Convention V states that neutral states have no obligation to disrupt communications passing through their publically accessible communication systems. This would not apply to cyber weapons since they are means of attack rather than communications.

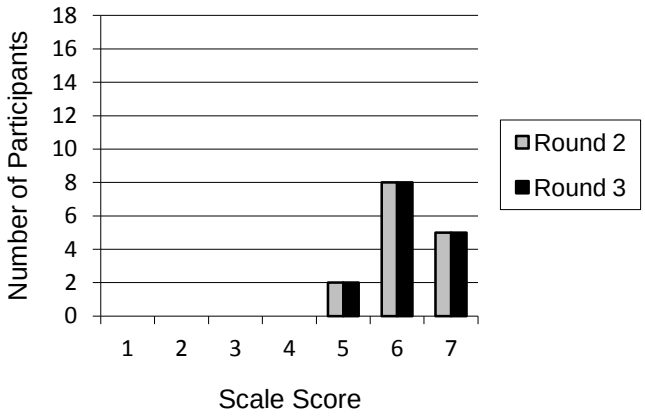

Figure 28. Scale score responses for Question 27.

During both rounds of inquiry, a consensus was reached to agree or strongly agree with the question. For some of those strongly agreeing with the question, there was a belief that accepting the premise would create an undue burden on states to monitor network traffic. The same group also tended to feel that the cyber weapon was a program running on a computer and not the communications controlling it. There was a difference of opinion on this point with one of the respondents who somewhat agreed with the question stating that a cyber weapon was both the program and the communications controlling it.

Question 28. Because it would be an undue burden on the citizens of a neutral state to disrupt network communications, a neutral state is under no legal obligation to stop the use of its public systems by states involved in an armed conflict.

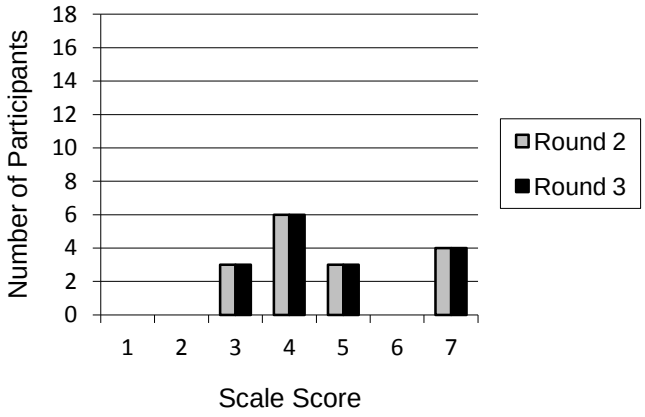

Figure 29. Scale score responses for Question 28.

After two rounds of inquiry, a consensus could not be reached for this question. The most common response was to be neutral on the question because of a perceived ambiguity in international law. Among those somewhat disagreeing with the question, there was a belief that because the state's public systems were knowingly being used that the failure to intervene may cause the state to lose its neutrality. An equal number of respondents somewhat agreed with the question primarily because they felt it was fact specific and could not be covered using a single analogy. The final group of respondents strongly agreed with the assertion for a variety of reasons but primarily because they did not classify the transfer of network data as an armed attack or the failure to interfere with such communications as vacating the states neutrality.

Question 29. Because of the redundancy built into networks and the inability to direct packets through specific paths, the travelling of packets containing cyber weapons through the territory of non-belligerents does not violate their neutrality.

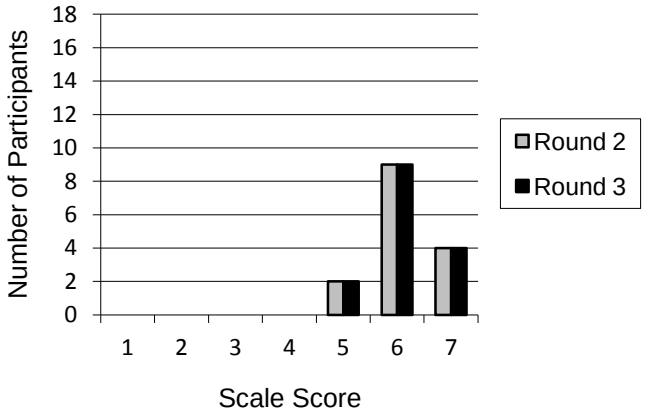

Figure 30. Scale score responses for Question 29.

During both rounds of inquiry, the consensus of the participants was to agree or strongly agree with the question. A common theme among those in the consensus was that the packets carrying the cyber weapon is a form of communication and not a weapon itself. Others in the consensus pointed out that the question also supplied the answer. Namely that the packets are routed to a destination but the path they take to get there is typically not predetermined.

Question 30. A state may legally disable or destroy network infrastructure in a neutral country if the neutral country is unable or unwilling to stop the use of its equipment to route cyber attacks.

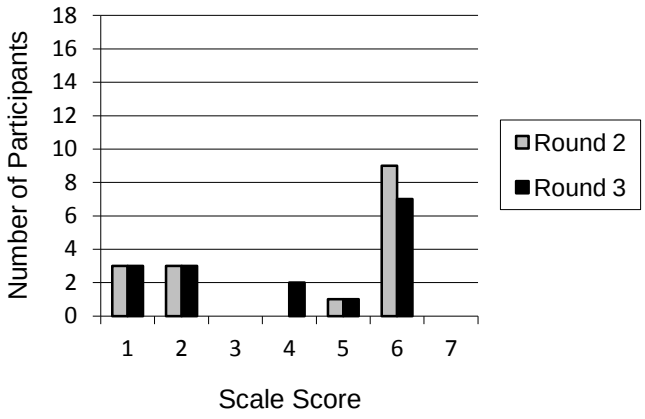

Figure 31. Scale score responses for Question 30.

After two rounds of inquiry, a consensus of opinion for this question could not be reached. The most common response was to agree with the question based on the belief that it was in keeping with the laws of neutrality. Because of the arguments provided by those disagreeing with the question, two respondents who initially agreed took a neutral position on the question during the third round of inquiry. The arguments provided centered on the belief that it is easier to block traffic than disable or destroy infrastructure in a neutral state and that taking action against a neutral state would be an unjustifiable act of war.

Question 31. Because every component of cyberspace resides in the sovereign territory of a nation-state or under its control, an international agreement designating cyberspace a global common is virtually impossible.

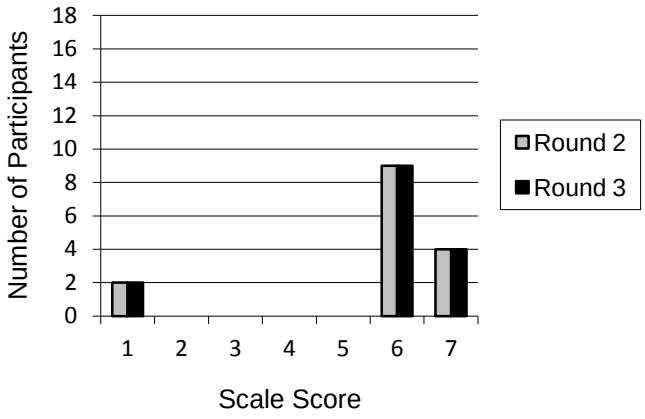

Figure 32. Scale score responses for Question 31.

During both rounds of inquiry, a consensus was reached to agree or strongly agree with little need to elaborate on the justification provided by the question. Among those disagreeing with the consensus, there was a belief that other international agreements have been made on topics such as global warming and terrorism that also had to resolve issues of sovereignty such as those present with cyberspace. One participant was unable to respond to the question because they disagreed with the premise that "every component of cyberspace resides in the sovereign territory of a nation-state or under its control" and felt it more appropriate to not respond rather than disagree.

Question 32. Designating cyberspace a global common would eliminate any concerns over neutrality or sovereignty when conducting cyber warfare operations.

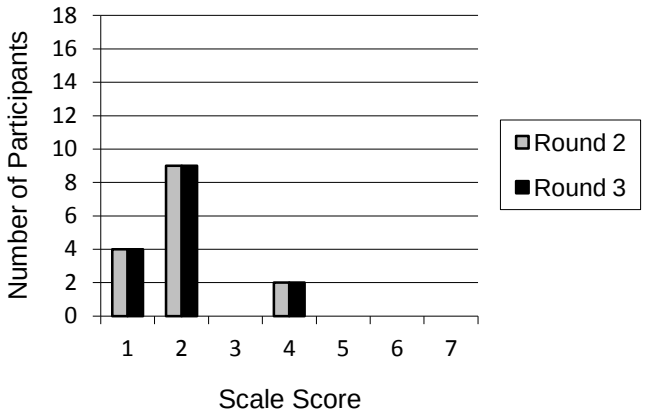

Figure 33. Scale score responses for Question 32.

A consensus to disagree or strongly disagree was reached for this question during both rounds of inquiry. These opinions were based on the belief that some measure of sovereignty exists even in a global commons. An analogy provided by one respondent was that a public park is a common but, visitors to the park still have sovereignty over their wallets. Two participants were neutral on the question because they did not feel they were informed enough to agree with or dispute the consensus of opinion.

Ethics and Cyber-Specific Legal Limitations

Question 33. The use of customary law to develop limitations specific to cyber warfare is restricted because the secrecy surrounding cyber operations has led to a lack of available state practice or *opinio juris.*

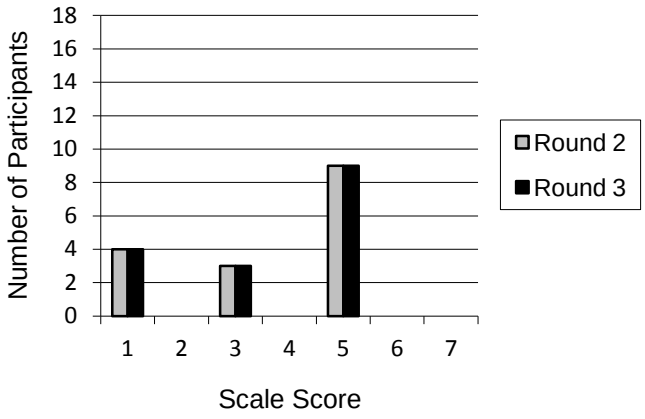

Figure 34. Scale score responses for Question 33.

After two rounds of inquiry, a consensus could not be reached on this question. The most common position was to agree with the question with some respondents adding that the issue is a temporary one that will be resolved in the future. Among those strongly disagreeing or somewhat disagreeing, the belief existed that the secrecy is only present in regards to specific issues such as targets and the vulnerabilities being exploited. This group believed that since the methods are well known there is sufficient evidence on which to base state practice.

Question 34. Because the leading cyber powers have shown no inclination towards limiting their cyber warfare potential, the use of customary law is likely the only way to develop such limitations.

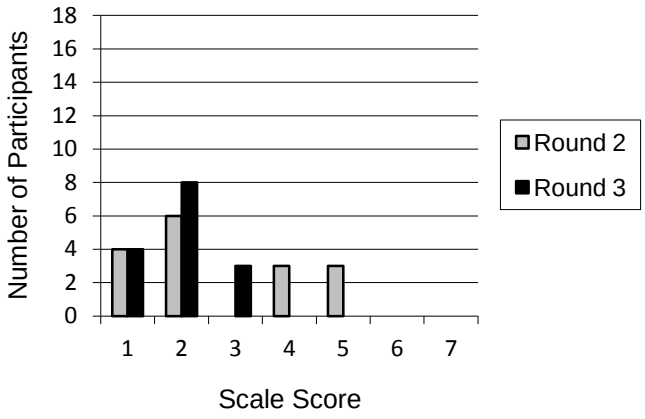

Figure 35. Scale score responses for Question 34.

While opinions were initially inconclusive for this question, by the final round of inquiry a consensus to disagree or strongly disagree emerged. Among those in the consensus, there was a belief that recent international agreements on cybercrime suggests a potential willingness among the leading cyber states to legally limit cyber warfare. Others argued that some states have recognized that the laws of armed conflict are applicable to cyber warfare. Even among those in the consensus there was the belief that a treaty limiting cyber warfare is still far off and will require a great deal of negotiation.

Question 35. States have intentionally been unwilling to address legally limiting the use of cyber weapons so as to allow for maximum flexibility in the conduct of cyber operations.

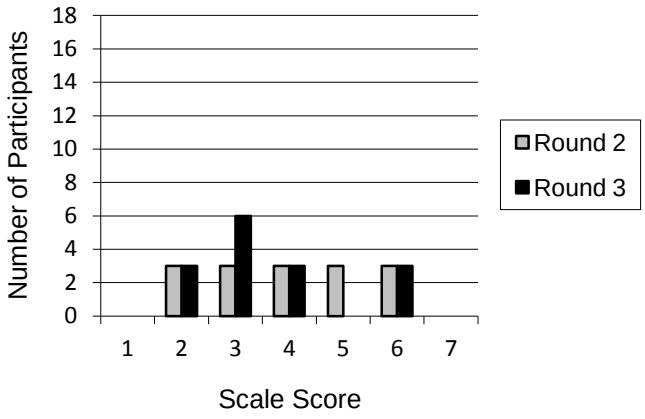

Figure 36. Scale score responses for Question 35.

After two rounds of inquiry, a consensus of opinion could not be reached for this question. Among those disagreeing or somewhat disagreeing, there was the belief that states were reluctant to depart from precedents established under international humanitarian law. This same group believed they would be more inclined to negotiate cyber warfare treaties once tangible damage had occurred following a cyber attack. Within the group of respondents who took a neutral position on the question, there was the opinion that allowing for maximum flexibility was only one of a number of components in the unwillingness of states to limit their conduct.

Question 36. The inequality of technological capabilities has been a primary reason why leading cyber states have been unwilling to address legally limiting the use of cyber weapons.

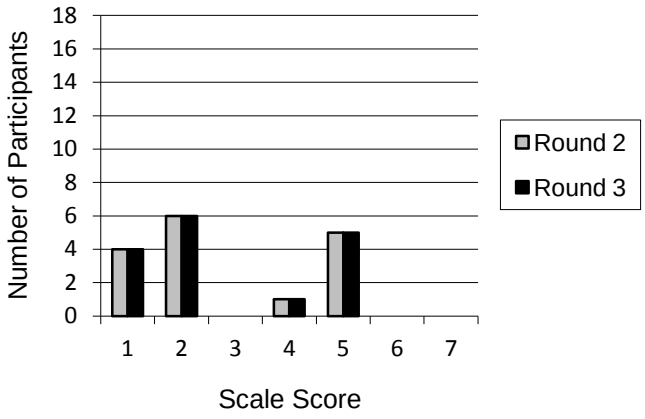

Figure 37. Scale score responses for Question 36.

During both rounds of inquiry, a clear majority of respondents scored their responses as disagree or strongly disagree but an insufficient number did so to establish a consensus. Among the majority opinion, the scale scores were based on the belief that the leading powers are also the most susceptible to cyber attack and understand the need for a treaty. There was also a belief among members of this group that competing interests and priorities among states have played a role. Among those somewhat agreeing with the question, there was the belief that a key consideration was states allowing themselves the most freedom of action as possible. Again for this question, the neutral opinion was based on the belief that technological superiority was only one of a number of components in the unwillingness of states to limit their conduct.

Question 37. The exponential growth of technology would most likely leave any specific cyber warfare legislation obsolete shortly after it was enacted.

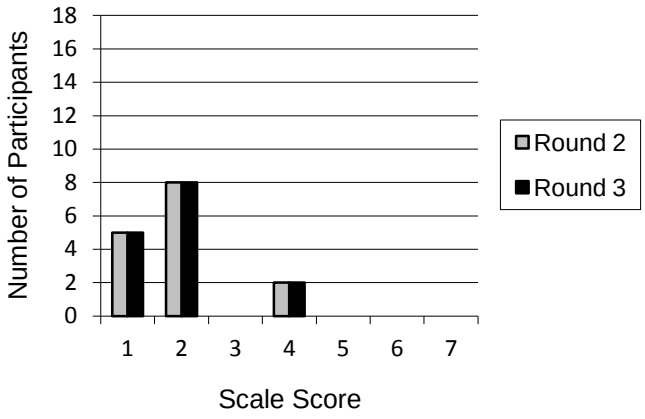

Figure 38. Scale score responses for Question 37.

During both rounds of inquiry, a consensus was reached to disagree or strongly disagree with the question. Justifications among the consensus centered on the belief that software technology has changed very little over the last 50 years even with the advent of digital devices. This was important to them specifically because of their stated belief that software is by far the most common target of cyber attack. Additionally, it was stated that cyber attack methods have not changed much over the last 20 years but merely use the same methods to exploit new vulnerabilities. Two participants responded outside of the consensus and rated a response of neutral. One was based on the belief that they did not know the technology well enough to respond while the other felt the question was very much legislature specific.

Question 38. Any international agreement to limit the use of cyber weapons is likely to be ignored during an actual conflict by those states capable of using them effectively; regardless of whether they are a signatory to the treaty.

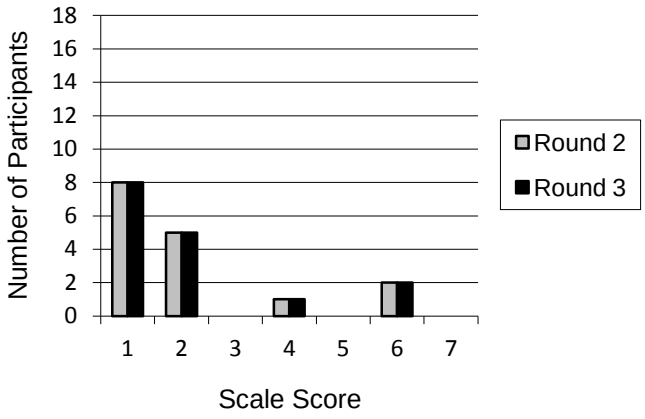

Figure 39. Scale score responses for Question 38.

During both rounds of inquiry the consensus of opinion was to disagree or strongly disagree with the question. Among the consensus, the belief existed that the question was very much state-specific with some adhering and others not. It was stated that the reasonableness of the treaty would be a strong determining factor in adherence. Also, some within the consensus felt that violating international agreements encourages escalation which most states would want to avoid; especially as the escalations would likely occur outside of cyberspace. The group of respondents who agreed with the question felt it was in keeping with state practice and therefore a valid assumption.

Question 39. Preemptive cyber attacks can be morally justified if the evidence exceeds a 90% likelihood of armed attack and that the provocation is expected to cause a high degree of damage or casualties.

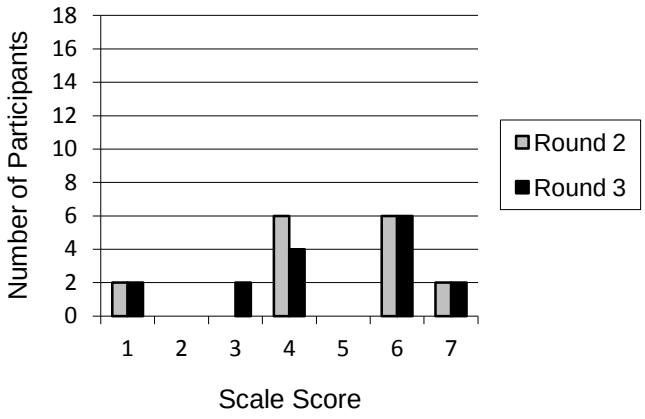

Figure 40. Scale score responses for Question 39.

After two rounds of inquiry, no consensus could be reached among the participants. Half of the respondents either agreed or strongly agreed with the question. Their opinions were based primarily on the belief that the scenario met the requirements of anticipatory self-defense under the laws of armed conflict. Conversely, those strongly disagreeing with the question believed that the laws of armed conflict only allow for preemptive attacks on a very rare basis. They felt that window was even narrower for cyber attacks because of additional difficulties with assessing danger and adversary preparations. During round three, 2 participants who were previously neutral on the question moved to the opinion of slightly disagree because of this argument. During round three, they felt it would require a case-by-case review. Neutral opinions varied from questions as to whether morally justified attacks are any different from legally justified ones and with the use of 90% as the trigger.

Question 40. States have an obligation to defend their citizens from cyber attacks even to the extent of using some illegal or unethical means to do so.

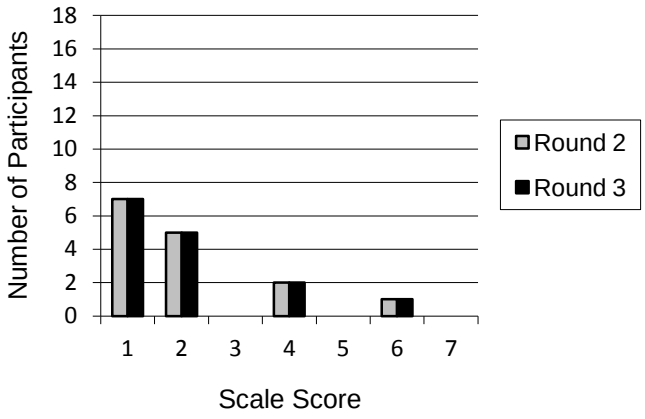

Figure 41. Scale score responses for Question 40.

The consensus of opinion for both rounds of inquiry was to disagree or strongly disagree with the premise. For many in the consensus, it came down to the belief that one can not commit a crime in order to defend themselves from another. Neutral opinions centered on the idea that the question may be true based on the effects of the cyber attacks and specifically their potential to cause great harm and destruction. The individual who agreed with the premise considered it the state's duty to defend its citizens even if the minimum necessary response exceeded legal or ethical standards.

Question 41. Each state has an affirmative duty to formally review the legality of any cyber weapon and operation prior to its deployment.

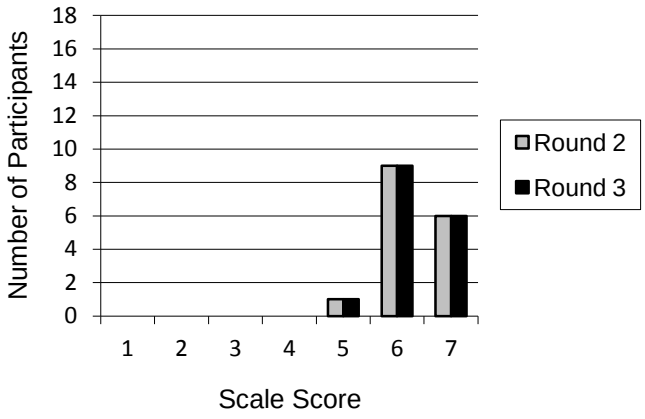

Figure 42. Scale score responses for Question 41.

During both rounds of inquiry, all respondents took a positive view of the question with the consensus being to agree or strongly agree. It was widely believed that the assertion was consistent with international humanitarian law. It was further justified based on the belief that the complexity of cyber weapons raises many collateral damage issues that are not obvious at the onset of an operation.

Question 42. Each state has an affirmative duty to continuously monitor their cyber attacks, when feasible, so as to cancel or suspend an attack if conditions change such as posing a threat to the civilian population.

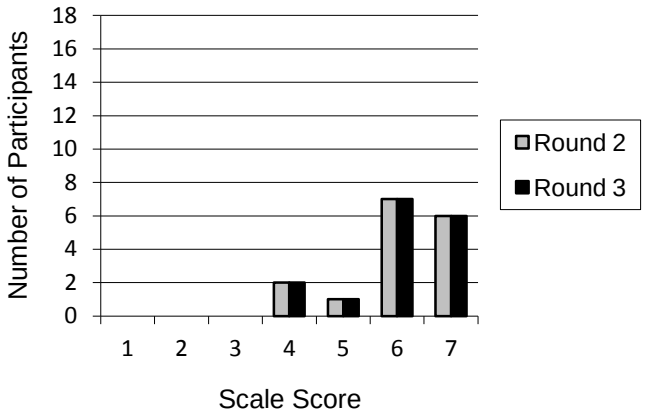

Figure 43. Scale score responses for Question 42.

For both rounds of inquiry, there was a consensus of opinion to agree or strongly agree with the question. Responses to this question centered on the belief that it was consistent with international humanitarian law with two respondents equating it to the obligation of damage assessment after a kinetic strike such as with a missile or aerial bombing. Neutral opinions were based on the belief that the requirement is only to consider the possibility while planning rather than actively monitoring during the operation. It was further stated that the continuous monitoring of a cyber attack may be impossible if it severs or interferes with communications.

Results for Research Question 1

The first research question being investigated was at what point do computer virus attacks elevate to the level of use of force or armed attack under international law. Almost unanimously, the respondents found that comparing the scope and effect of a cyber attack to a kinetic attack was an effective formula for determining whether it reached the point of use of force or armed attack under international law. There was also

a strong consensus of opinion that a use of force or armed attack designation could be assigned collectively to multiple cyber attacks committed over a short period.

The target of a cyber attack was also deemed to be of importance by the participants when determining a use of force or armed attack designation. A strong majority of the respondents felt that targeting critical national infrastructure was merely one factor in determining a use of force designation and not sufficient in and of itself. Additionally, the consensus of opinion was that the significant loss of any single computerized system was not sufficient enough for a use of force designation but would most likely be deemed a violation of sovereignty. In terms of system manipulation, the consensus of opinion among the respondents was that changing the functionality of a system is a form of damage since functionality of a system is part of its integrity. Because of this viewpoint, the participants believed that altering the data or functionality of a system may allow for an armed attack designation as damage need not be physical. This idea was expanded upon by the near unanimous opinion that cyber attacks that lead to physical damage such as that which occurred at the Natanz nuclear facility could also lead to an armed attack designation.

Another area that also received a strong consensus of opinion was the belief that the intent of the attacker and not just the results should be taken into account when making an armed attack designation. This can be seen in the results to Question 10, where most of the respondents agreed that a cyber attack foiled by passive defenses may still be designated an armed attack if it would have caused serious damage or loss of life.

Results for Research Question Two

The second research question asked what limitations exist with initial and reprisal cyber attack targeting. The consensus of opinion of the respondents was that cyber weapons were not illegal under international law and that they met the requirements for reasonable control and accountability of use. The consensus of opinion was also that any response to a cyber attack need not remain in cyberspace in order to meet the requirements of proportionality. Lastly, the participants unanimously found that the requirement for necessity was not hindered by the fact that any reprisal would most likely not alleviate the ongoing effects of the initial cyber attack.

During the first round of inquiry, the idea that each state had a positive duty to formally review all cyber weapons and operations prior to their use was posited. It was also stated that each state had an obligation to continuously monitor their cyber attacks whenever possible and suspend them if civilians were endangered. In both cases, the participants reached a consensus to agree with these concepts. Conversely, the respondents were primarily neutral or slightly disagreed with the idea that any malware that could not be controlled after deployment would be illegal under international law. The opinion of the consensus was based, among other things, on the belief that international law only requires states to consider the possibility of collateral damage rather than eliminate it entirely.

Questions about perfidy and the targeting of non-combatants were also discussed by the participants of this study. The legality of masking a cyber weapon to look like legitimate civilian traffic was a particular point of contention. While a majority of

respondents disagreed with the notion that masking the cyber weapon would violate the prohibition against perfidy, a consensus of opinion could not be reached. Even more contentious was whether masking the cyber weapon to look like the communication of a protected organization such as the United Nations or International Red Cross would be illegal. In this case, only one more contributor felt it would not be illegal than took the opposing view. Although some respondents disagreed, the consensus of opinion was that accepting the premise that no civilian or government target had full legal protection from cyber attacks would violate *jus cogens* and lead to abuses. A similar scenario existed whereby, with few objections, the participants reached a consensus of opinion that non-combatants forfeited their protections if they directly engaged in cyber operations regardless of whether they were government employees or not.

As a cyber attack may go unnoticed for a considerable amount of time, and there are additional questions with attribution involving cyber attacks, the requirement of immediacy was strongly debated by the participants. A slight majority of the respondents felt that predicating immediacy on the time reasonable attribution had been made rather than on when the effects were detected would not be legal under international law. Conversely, those arguing in favor of the proposal felt this would allow states ample time to establish reasonable attribution and mitigate the possibility of responding against the wrong state or actor. The question of reasonable attribution is significant in that all respondents agreed to some extent that tracing a cyber attack to a foreign state-owned computer system is not sufficient enough evidence to attribute the attack. The need for reasonable attribution was limited by the consensus of opinion that cyber attacks may be

launched for defensive purposes under the guise of necessity even with the identity of the aggressor is unknown.

A number of issues concerning anticipatory self-defense and active defense systems were also discussed by the participants. The consensus of opinion was that the legal concept of anticipatory self-defense applies to cyber attacks in the same way they do kinetic attacks. Furthermore, the consensus of opinion included the belief that the cyber attack need not be part of a larger attack encompassing a campaign outside of cyberspace. Half of the participants also felt that a preemptive cyber attack could be morally justified if there was a high probability that the impending attack would cause large scale damage or casualties. Lastly, the participants reached a consensus of opinion that states may not use illegal or unethical means to defend their citizens from cyber attacks.

Results for Research Question 3

The third research question investigated the effects of the unique nature of cyber warfare on the traditional idea of state neutrality. Two areas concerning the use of neutral state communication systems to conduct cyber attacks failed to meet with a consensus of opinion. The first disagreement lied with whether a neutral state has an obligation to disrupt the use of its communication infrastructure if it is aware that it is being used to conduct cyber attacks. Most respondents to this question took a neutral opinion or only slightly agreed or disagreed with the premise. Some felt that this would be an undue burden on the neutral state while others felt that failure to do so could cause the state to forfeit its neutrality. One of the issues unique to cyber warfare that was

debated was, whether the transfer of network data could be considered a cyber attack or merely communication.

The second question that the participants could not come to consensus of opinion on was, whether a state may legally attack the communication infrastructure of a neutral state if the neutral state was unwilling or unable to halt its use. During the second round of inquiry, a clear majority opinion was to agree that combatants do have the right to disable the infrastructure in neutral states. While this belief remained the majority opinion during the third round of inquiry the number of participants agreeing with it fell as some moved towards a neutral opinion.

Among the questions of neutrality that the respondents were able to find consensus was the inability to designate cyberspace a global commons. The idea that a cyber-global commons might eliminate questions of neutrality was soundly defeated by the participants. The participants agreed that the current composition of network infrastructure made such a global commons designation problematic at best and that labeling cyberspace a global commons would not eliminate questions of sovereignty over its physical components.

A final area of consensus was found in the belief that the mere transfer of a cyber weapon over a neutral states communication system did not cause that state to forfeit its neutrality. This belief stemmed from the recognition of redundancies in network communications that would make it difficult to route a cyber attack through a specific path. It was also a belief of some of the participants that the packets carrying the cyber weapon was a form of communication rather than a weapon itself.

Results for Research Question 4

The final research question asked what impediments currently exist in the development of legal limitations on cyber warfare. During the first round of inquiry, a number of ideas were posited to explain this but, by the end of the third round most of these ideas had been dismissed. A slight majority of respondents felt that the use of customary law was limited in the development of a cyber warfare regime. Even among this group there was a belief that the issues surrounding the growth of customary cyber warfare law were temporary ones that will be resolved in time. At the same time, the participants soundly disagreed with the idea that customary law was the only way such a regime will emerge. Many of the participants recognized that the growth in international cybercrime laws pointed to increased willingness to establish legal limitations on cyber warfare. They further posited that this could be accomplished through difficult negotiations but, it would not occur in the near term because of conflicting national agendas.

The contributors to this study soundly rejected the notion that the growth in cyber warfare technologies will limit the applicability of any cyber warfare limitations. This belief is documented with the results of Question 37 whereby none or the respondents agreed that technological changes would leave any such legal limitations obsolete. A majority of participants further stated that the inequality of growth in cyber warfare technology is also not a source of restriction on the development of cyber warfare legislation. This belief is demonstrated by the results of Question 36 which showed the respondents disagreeing with this premise by a 2 to 1 margin.

The most contested opinion was whether states have intentionally avoided limiting their cyber warfare options in order to allow for maximum flexibility. During the second round of inquiry, the participants were equally divided on this query. By the end of the third round, a larger number disagreed than agreed with the notion but, it was far below the threshold established for consensus.

Summary

In this chapter, the beliefs of 16 scholars in the fields of international law and cyber warfare were documented with the stated goal of finding a consensus as to the legality of cyber warfare under international law. The methodology and protocols used were specifically designed for three reasons. First, so that these scholars' own words could be utilized in developing the questionnaires, second, to provide feedback as to the beliefs of all the participants after each round of inquiry, and lastly, to allow respondents the ability to both rate their responses on a Likert-type scale as well as justify them in writing; all through an anonymous process.

The first round of inquiry consisted of a questionnaire composed of nine open-ended questions. The results for this questionnaire were entered into QSR Nvivo to aid in the identification of themes for the preparation of subsequent questionnaires. These questionnaires consisted of 42 questions that allowed the participants to rank their responses on a Likert-type scale and justify them using written responses. After both the second and third rounds of inquiry, feedback in the form of figures showing the cumulative scale scores and summaries of the given narratives were provided to each participant. This feedback played not only an important role in developing the results of

the study but also as a tool for data verification and establishing the trustworthiness of the results.

The following chapter will interpret the results of this study, detail the limitations of it, and provide recommendations for further research into the topic.

Chapter 5: Conclusions

Introduction

The purpose of this study was to reach a consensus as to the current standing of cyber warfare under international law and to recommend changes to the law whenever possible. Because of the broad scope of what encompasses cyber warfare, the research was delimited to a study of cyber attacks. Additionally, the unique nature of cyber warfare has left much ambiguity as to when cyber activities rise to the level of use of force or armed attack under international law. This categorization under the law is important to determine what cyber actions and reactions are both legal and appropriate. Failure to clearly make this determination may lead states to commit acts of cyber adventurism that result in severe damage or loss of life.

The research methodology for this study consisted of a Delphi method of qualitative inquiry. The use of the Delphi method allowed for three separate rounds of inquiry among 18 scholars in the fields of international law and cyber warfare. During each round, the identities of the contributors were kept strictly confidential with the only feedback provided by the researcher. With the first round, the participants answered open-ended questions in order to assist in developing the questions for the subsequent surveys. With the second and third rounds of inquiry, the respondents ranked their opinions on a Likert-type scale and provided a brief justification for their scores. In between each round, and at the end of the study, the results were shared with each participant to allow them to be aware of their colleagues' opinions and to refine their own.

In the previous chapter, the results of the questionnaires were presented. In this chapter, the findings are interpreted and evaluated for their limitations, recommendations for further research, as well as their implications and potential for social change.

Interpretations, Limitations, and Recommendations

In this section, a succinct interpretation of the findings for this research is provided. These results are compared to those of the scholarly works represented in the literature review in an attempt to fill gaps in the existing literature. Additionally, the limitations of the study are concisely demarked and addressed through recommendations for further research. The limitations and recommendations include not only the findings, but multiple aspects of the methodology such as the method of inquiry, participant population pool, and the theoretical framework.

Review and Recommendations for Research Question 1

Determining whether a computer attack has risen to the level of use of force or armed attack under international law was a key component of this study. Overwhelmingly, the participants agreed that comparing the scope and effects of a cyber attack to those of a kinetic attack was appropriate for making this determination. Only one of the respondents disagreed with this notion and did so because they felt it did not eliminate the possibility that what was perceived as an attack was in actuality coincidental. Some scholars have developed models to measure the characteristics of cyber attacks against those of kinetic attacks. For example, the model developed by Schmitt (1998) uses a quantitative scale in which to calculate the severity, immediacy,

directness, invasiveness, measurability, presumptive legitimacy, and the responsibility for the cyber attack.

The use of models like the one developed by Schmitt, would seemingly support the consensus of opinion of the participants in this study, but not all scholars agree with this premise. One expert who disagrees with this approach is Barkham (2001) who sees it as flawed for attempting to determine the legality of a cyber attack based on the attack rather than based on the law. Barkham further sees a flaw with trying to assess a cyber attack during, or immediately after the event, as the full effects are often unknown during this timeframe. Current international law assumes that an armed attack will have physical limitations in time and space (Rho, 2007). However, some scholars believe this does not hold true if a cyber attack is to be designated a use of force or armed attack (Jurich, 2008).

As the model used for determining whether a cyber attack has risen to the level of use of force or armed attack is of paramount importance, further studies should be conducted in this area. Specifically, studies that review existing models for their applicability and determine what characteristics these models should measure are needed. While the participants in this study clearly favored measuring cyber attacks against kinetic attacks when making a use of force or armed attack distinction, a determination as to whether existing models are appropriate for doing so should be further studied.

During the course of this study, a majority of participants determined that the targeting of critical national infrastructure was in itself insufficient to make a use of force determination. Instead, these respondents felt that the target was only a singular factor in

making such a determination. This opinion contradicts the beliefs of both Jensen (2002) and Hollis (2007) with the later listing the targeting of critical infrastructure as one of three potential criteria for making a use of force determination. Considering that a consensus of opinion could not be reached during this study, and that additional scholars have contradicted the view of the majority, the question as to whether the targeting of critical infrastructure is sufficient to make a use of force claim remains unsettled. Supplementary research should be conducted in an attempt to both definitively answer this question and to determine specifically what infrastructure would fall into this category.

The laws of war have traditionally distinguished between the use of force and armed attack based on the physical effects of the attack (Schmitt, 1999). The use of the physical effects has been shown to be problematic when attempting to evaluate cyber attacks (Jurich, 2008). One potential solution to this problem debated by the participants of this study was the classification of data manipulation as physical damage. A consensus of opinion was reached among the contributors that altering data or the functionality of a system should be considered physical damage and, therefore, warranted of an armed attack distinction. Their opinion was based in part on the belief that changing the functionality of a system is a form of damage since the functionality of a system is part of its integrity. While a consensus of opinion was reached among the participants of this study, potentially addressing the problem in this fashion needs to be researched further in order to meet the confirmability of results.

Silver (2002) stated that for a cyber attack to be considered a use of force the attack must have intended to cause a result similar to a kinetic attack. The participants in this study took this premise one step further by reaching a consensus of opinion that a failed cyber attack that would have caused severe damage or loss of life would also be considered an armed attack. As with Silver, the respondents agreed that the intention of the aggressor was a sufficient criterion with one contributor likening it to a missile falling short of its target. Opinions like these hold greater weight with cyber warfare as cyber weapons are typically no more reliable today than in the past and tend to have a higher rate of failure than conventional weapons (Neumann, 1995; Rowe 2009).

The participants of this study made one final decision in relation to designating a cyber attack a use of force or armed attack. A consensus was met that such a designation would be possible to a collective string of attacks even when each individual attack fails to meet the necessary criteria. The question among those participants that disagreed with this premise was how to determine the starting and ending points when evaluating the cumulative effects. The consensus of opinion for this question potentially has far reaching consequences and needs to be investigated further. Additional research as to the validity of the opinion expressed here and an acceptable formula for determining the duration that can be evaluated when making a use of force or armed attack designation is needed.

Review and Recommendations for Research Question Two

International law requires states to maintain reasonable control over their weapons and be held accountable for their use (Lucas, 2010). It also makes the continuation of

hostilities after a party has surrendered illegal. Some scholars such as Rowe (2009) have stated that cyber weapons might not meet these minimum requirements and especially if the weapon is designed to obstruct communications as part of its function. While discussing the legitimacy of cyber weapons, the participants of this study came to a consensus of opinion that the minimum necessary controls currently exist. Two respondents objected to this viewpoint stating that cyber weapons require more stringent controls then kinetic weapons and therefore may not be legal in their current state. The question of control after the release of a cyber weapon was more contested and failed to reach a consensus. The majority view was that controlling a cyber weapon after it is deployed is not required but merely to consider the possibility for collateral damage and to minimize the likelihood. Additionally, it was stated that if a cyber attack remained within military systems a lack of control over the weapon would not be a concern. Because questions of control over cyber weapons may affect the legitimate use of certain types of cyber weapons, further research into this question will need to be conducted.

When asked about a state's affirmative duty to formally review the legality of any cyber weapon or cyber operation the respondents unanimously agreed that it was a requirement under international humanitarian law. Similarly, a clear consensus of opinion among the respondents was reached to agree that all states have an affirmative duty to monitor and cancel attacks whenever feasible if they pose a threat to the civilian population. The remaining participants believed it was only a requirement to consider the possibility during planning and that it would be an undue burden to continually monitor an attack especially if the attack severed communication.

Under *jus ad bellum*, a state must have proportionality, necessity, and immediacy when responding to an act of aggression. In Nicaragua v. The United States, the International Court of Justice laid down three specific conditions to justify a proportional attack. The third criterion given was that the responding state must do so in a manner proportional to the offending state's actions (Jensen, 2002). To investigate this further, the participants of this study discussed whether this condition requires that states only respond to a cyber attack in cyber space. The consensus of opinion was that the requirement for proportionality only required a proportionality of effects regardless of the means. Two contributors objected to this opinion stating that cyber warfare is too different from traditional warfare to accept this premise. While the respondents overwhelming agreed that a response to a cyber attack may occur with kinetic weaponry, a lack of studies into the topic will require the results to be confirmed through additional research.

When arguing necessity, just war theorists evaluate military operations based on whether the goal of the action could be achieved by other means that would not result in injury or death (Baer, 2005). This belief has led some scholars to debate whether the just war theory would allow for preemptive attacks. Certain scholars have accepted that a narrowly defined right of intervention does not run contrary to the just war theory (Primoratz, 2002). In an effort to delineate one of the boundaries of the right of intervention, the participants of this study debated Dilbert's (2009) assertion that a preemptive attack could be deemed morally justified if the likelihood of armed attack exceeded 90% and the attack was expected to cause a high degree of damage. At the

conclusion of this study, no consensus of opinion could be reached on this question. Half of the respondents agreed with Dilbert's assertion based on the belief that it met the guidelines of anticipatory self-defense under the laws of armed conflict. The remaining respondents took either a neutral opinion based on the need to evaluate it on a case by case basis or disagreed because of a belief that the right to anticipatory self-defense is more limited in cyber space.

Schmitt (1999) has argued that a preemptive cyber attack cannot be initiated to stave off an impending cyber event unless the cyber event is to be part of a greater armed assault. While rejecting this proposition, the participants of this study reached a consensus of opinion with just two dissentions. Those in the consensus agreed that the modality of an armed attack is inconsequential as a cyber attack that reaches the level of armed attack is no different from a kinetic attack that carries the same distinction. Among those outside of the consensus, there was a concern about the additional issues with attribution that occur during cyber warfare. The question of attribution was further explored by the respondents of this study. In doing so, they reached a consensus of opinion that a state may launch cyber attacks for defensive purposes in the name of necessity even when the identity of the attacker is not clearly known. In keeping with the tenants of the just war theory, some of those in the consensus qualified their response with the caveat that it was contingent on there being no other way for the state to defend itself. As with the previous question, 2 contributors disagreed with the consensus. In this case, they did so based on the belief that attribution requirements could not be weakened for cyber attacks as the same scenario would be illegal under international law if it were

done using traditional military means. This belief is in keeping with that espoused by Cordon (2007) who stated that a victimized state must be able to identify their attacker and their intention in order to claim necessity. As the participants of this study were able to reach consensus of opinion over the legality of preemptive cyber attacks, the results will need to be confirmed through additional research.

To meet the requirement of immediacy, any response to a cyber attack must occur before too much time has lapsed (Cordon, 2007). While Gill (2006) has noted that the response need not occur immediately after the attack, a set timeframe or criteria has not been established. One criterion debated by the participants of this study was whether to fix the starting period for immediacy on the time that reasonable attribution had been made. The respondents were nearly equally split on this question with slightly more disagreeing. The proponents of this concept believed it took into consideration the additional attribution problems present with cyber warfare. Their opponents maintained that immediacy must remain with the time the effects are noticed to be legal under international law. Because the divide between the participants was nearly equal, it is difficult to make any significant assessment of the results. While current international law may favor the use of the effects, this may require a reevaluation in order to limit the use of cyber weapons as suggested by some of the contributors.

Under the just war theory, states must respect the rights of all individuals on both sides of a conflict equally (Fabre, 2008). When discussing legitimate targets for a cyber attack, the role of civilians was debated by the participants of this study. A consensus of opinion was formed that certain population groups always maintain their protections even

when an overriding military necessity may exist. Walzer (2000) wrote that civilians forfeit their protections only when they are directly engaged in the business of war such as working in a munitions factory. Primoratz (2002) expanded upon this definition by stating that civilians can only forfeit their protections by their own actions. The contributors to this study accepted this principle unanimously. In doing so, they accepted that civilians involved in offensive cyber operations have forfeited their protections. Even though there was unanimous acceptance of the argument, some of the participants qualified their responses by stating that only offensive cyber operations that cause death or physical destruction warrant forfeiture of the civilian's protected status. This addendum holds significance when coupled with the question of whether data manipulation or destruction is a form of physical destruction and should be researched further as part of this question.

The last question over cyber attack targeting covered by this study dealt with possible acts of perfidy. Perfidy is illegal under international law because it may encourage states to erroneously or intentionally target civilians (Rowe, 2009). During the course of the debate over perfidy, it was the consensus of opinion of the participants that a cyber weapon designed to look like legitimate civilian traffic would not violate this prohibition. The rationale often cited was that perfidy only covers active agents which network traffic could not be classified as. Additional justifications were based on the belief that acts of perfidy require the taking of a life which may not occur with a cyber attack.

Review and Recommendations for Research Question 3

One major point of contention over neutrality that exists after the completion of this study is whether a cyber weapon qualifies as a weapon or merely communication while being transmitted. The Hague Convention V states that nations involved in an international conflict may not move weaponry or military supplies across the territory of a neutral state. The same convention also states that neutral nations have no obligation to disrupt the military communications of warring states that utilize their communication networks. Whether the requirements of Hague V apply solely to traditional communication networks that send and receive data or also digital networks that can also create data is still a matter of much debate (Kelsey, 2008). Various scholars, such as Greenberg (1998) and Brown (2006), take the opinion that the transmission of a cyber weapon over a neutral state's communication system would violate that state's neutrality. This belief would seemingly draw the neutral state into the conflict as neutral states are required under international law to resist any attempted violations of their sovereignty (Kelsey, 2008).

For some of the participants of this study, a cyber weapon was a program running on a computer and not the communications that transmitted it or controlling it. Others viewed the cyber weapon as both the program and the communication. Regardless, of which classification the respondents used all agreed to some extent that neutral states had no affirmative duty to disrupt such communication. The key to whether a neutral state is required to interrupt the transmission of a cyber weapon may lie in whether it was aware that its infrastructure was being used. Most participants felt that it was an undue burden

for the neutral state to continuously monitor their networks for such communications. Once the question turned to the disruption of known communication, the majority of scholars turned neutral on the question or slightly agreed that states are required to disrupt the communication. It should be noted that those scholars whose primary background is in cyber warfare were more inclined to believe that the communication was a weapon and that the neutral state is obligated to disrupt the communication.

Another area that showed a clear divergence of opinion between the cyber warfare and international law scholars who participated in this study is whether a state may act forcefully against a neutral state which is unable or unwilling to disrupt the use of its communication systems. Those with a cyber warfare background tended to believe that the right to act was keeping with the laws of neutrality. Conversely, those whose primary background was in international law were more likely to disagree. While a consensus of opinion could not be reached for this question, a majority supported a state's right to physically intervene against a neutral party. Because the views of scholars differ greatly as to the obligations of neutral states, what cyber actions would violate the state's neutrality, and what right of reprisal exists, more research and discussion needs to be conducted in this area. Since views often very based on the background of the respondent, any such studies need to clearly demarcate the education and professional experience of all participants.

Review and Recommendations for Research Question 4

The results for research Question 4 did little to determine the root cause for the delay in legislation specifically targeting the limitation of cyber warfare operations. It

did however potentially abolish some causes. Possible reasons such as the rapid growth in technology and the inequality of that growth were discussed and eliminated by the respondents of this study. This view contradicts that of Walker (2000) who dismissed the appropriateness of cyber-specific legislation based on the belief that the growth in technology would leave such laws obsolete. Some of the participants in this study disregarded this notion because they believed that software technology had changed very little over the last 50 years and was unlikely to do so in the near future.

One area of disagreement that should be investigated further was whether maintaining maximum flexibility to conduct cyber operations was a leading factor in the failure to develop cyber-specific legal limitations. During the second round of inquiry, multiple responses were scored for 5 different points on the Likert-type scale. While the scale scores narrowed to 4 points during the third round, the diversity of opinion shows the level of disagreement on this point. Other scholars have seemingly taken a more positive view of this question. Ellis (2001) stated that states were unwilling to limit their cyber operations because they provided non-lethal methods of attack, and the full potential of cyber warfare is still not known. Similarly, Kelsey (2008) felt that cyber weapons would not be limited until they have been fully tested in a real-world conflict in order to determine the extent of their reach. The debate between the participants of this study centered on the present rather than the future so, little was discussed about the future potential of cyber weapons. Additional research into this specific rationale therefore, may be needed.

Kelsey (2008) wrote that numerous governments, including some cyber powers, believe that current laws are sufficient to cover cyber operations and have resisted any attempts at additions or modifications to the law. This concept was not discussed among the participants of this study and should be investigated further. Some of the respondents felt that states like China and Russia had made public statements supporting the creation of cyber-specific legislation but, other participants dismissed the legitimacy of their statements. The view among these contributors was that the statements were made solely for public consumption and that China and Russia are likely two of the most active states in terms of ongoing cyber operations.

While not eliminating the potential for the development of customary law in the field of cyber warfare, the results of this study showed a propensity of opinion that such legal limitations will result instead from negotiated treaties. It is believed that customary law has been based on state practice, resolutions, and declarations (Meron, 1996) but here too we see a difference of opinion as Ochoa (2007) disagrees with the assertion that it is based on the beliefs and actions of the state. While no consensus of opinion was achieved with this study, the majority opinion of the participants was to accept Meron's standard and find that the secrecy revolving around cyber operations limited the potential development of customary law in this area.

Another area that was not specifically addressed in this study is whether the time involved in the development of customary law was excessive. Schmitt (1999) has previously taken the view that customary law is impractical for addressing cyber operations specifically because of the time involved. Other scholars such as Kelly (2000)

view custom as no longer relevant in the development of international law. This notion may be visible with the development of what has been termed modern customary law that relies on the state's statement of practice rather than an analysis of its actual behavior (Bodansky 1995; Roberts, 2001). This view has led some scholars to see modern customary law as an offshoot of universal declaratory law rather than a progression in customary law (Bodansky, 1995). Considering that the participants of this study did not reach a consensus of opinion to dismiss customary law as insufficient for the development of a cyber warfare regime, future research may need to be specifically address whether time limitations that have traditionally occurred in the development of customary law are appropriate in this case.

According to Cody (2002), the reality of modern international law is that it is negotiated, ratified, and implemented in a short period time. Fortunately, one area that did receive a consensus of opinion during this study is that any negotiated settlement that is deemed reasonable by all signatories will most likely be adhered to in times of transnational conflict. These results may point to a belief that negotiated settlement is superior to customary law in terms of the length required in its development as well as its reception and adherence among the international community.

Limitations and Recommendations in the Methodology

This study was limited to the opinions of 18 scholars in the fields of international law and cyber warfare. It was further confined to scholars fluent in English and residing in English speaking countries. This limitation gave the results a slant towards an occidental viewpoint in terms of ethics and the interpretation of the law. The ethos of the

just war theory has also been the product of an evolution in Western ethics. By using the just war theory as a theoretical framework, the moral outlook of many states are left unexplored. Therefore, future research should attempt to gauge the opinions of scholars from other cyber powers such as China and Russia. As the most likely scenario for the development of cyber-specific laws of war will require negotiation with such powers, it is imperative that the vantage point of scholars and experts in these states be explored thoroughly.

Limitations also exist with the use of the just war theory as a theoretical framework. There is a concern among some scholars about the practicality of using the just war theory to judge cyber warfare either morally or legally (Dipert, 2006) as well as to evaluate the military aspects of cyber warfare (Lucas, 2010). Because of these reservations, additional research should attempt to employ divergent theoretical frameworks.

Additional limitations in the research exist with the delimiting of the study solely to cyber attacks. Focusing only on cyber attacks was deemed necessary at the onset of the research in order to scale the study to an appropriate and feasible size. In order to fully evaluate cyber warfare under international law, and make logical assumptions as to its future development, other forms of cyber warfare such as cyber exploitation will need to be researched and taken into consideration.

The Potential Role of the Participant's Backgrounds in the Results

Individuals involved in the development of cyber weapons tend to come from computer software backgrounds and are not as limited as those in traditional military

industries (Perry, 2009). Working primarily in the world of information technology is further given as a rationale for the more indiscriminate planning of operations against civilian infrastructure by the cyber warfare community (Lucas, 2010). The results for only three of the questions posed during the course of this study would appear to support this assertion.

Of the 16 participants that completed all three rounds of inquiry, 9 came from a background predominately in international law and 7 from a background predominately in information technology. Among those with an information technology background, there was a tendency at times during this study for some of them to take a more aggressive approach to cyber warfare operations. One example of this trend can be seen with Question 19. This question stated "No target, civilian or government, has complete legal protection from a cyber attack if there is an overriding military necessity." Only 2 respondents took a positive view of the premise of this question while the most common score was to strongly disagree. In this case, both of those agreeing came from information technology backgrounds. For Question 3, which stated "A state may legally disable or destroy network infrastructure in a neutral country if the neutral country is unable or unwilling to stop the use of its equipment to route cyber attacks" no consensus of opinion was reached. Trends for this question though showed those with information technology backgrounds almost unanimously agreed with the premise while those with international law backgrounds primarily disagreed. Lastly, with Question 40, "States have an obligation to defend their citizens from cyber attacks even to the extent of using some illegal or unethical means to do so," the sole agreeing vote and one of the two

neutral opinions came from those with information technology backgrounds. The remainder of the participants disagreed or strongly disagreed.

While this study could not validate the points raised by Perry and Lucas, it did seemingly show an opposite effect. For a number of questions, the only, or nearly all of the views outside of the consensus or majority opinion and which supported more stringent controls on cyber warfare were made by those with international law backgrounds. This phenomenon occurred with Questions 5, 6, 7, 9, 10, 12, 14, 17, 18, 20, 21, and 22. With these questions, the fringe opinions were made almost solely by those with international law backgrounds and in opposition of the beliefs held by their counterparts from both the information technology and international law fields. While the population size used for this study is too small to make any definitive claims based on these results, they do point to additional questions that need to be researched further. First, has the belief that cyber weapon designers and operational planners are more inclined to target traditionally protected objectives been overstated? Second, has a trend occurred within the cyber warfare community to more readily accept that existing international laws and norms apply to cyber warfare and have planned accordingly? Lastly, is there a strong difference of opinion among international law scholars when attempting to judge cyber warfare against traditional methods of warfare, rather than a divide between the international law and cyber warfare communities?

Implications

This study has important potential implications for state and non-state actors alike. However, because of the intransigence of many leading cyber powers, it remains chiefly

theoretical at this point. The reasoning for these pertinacious states still remains a point of contention even at the conclusion of this research. Most likely, it is a result of numerous factors that vary based on individual state beliefs and agendas. Regardless of their justification, the lack of cyber-specific limitations under the laws of war may well result in the commission of acts of war that otherwise could have been avoided. The basis for cyber-specific legislation under the laws of war can begin to be addressed by using the results of this and other related studies. Therefore, the findings contained here may help to serve as an initial point of negotiation for the international community.

State-sponsored cyber attacks have most likely already occurred. For the most part, they have been unassuming in their scope and led to little in the way of tangible damage or known deaths. This includes attacks attributed to Russia on the Estonian and Georgian governments and the Stuxnet virus attack on the Natanz nuclear facility which is most commonly blamed on Israel and the United States. As the attack on Natanz demonstrates, some states may have already become willing to escalate the use of cyber weapons and increase their destructiveness where they otherwise wouldn't with traditional kinetic attacks. Because of this, the major social implication of this study is to bring about greater attention and debate to the issue of legal limitations on cyber warfare. In doing so, it is hoped that the results of this study will hasten the development of a cyber warfare regime that will mitigate the damage and loss of life that may occur from a cyber attack.

Conclusion

To date, limitations specific to cyber warfare have failed to develop at the necessary pace and scope. To fill this void, states have taken different approaches in making their own interpretations as to what constitutes a legal action under international law. Additionally, some states have refused to negotiate cyber specific limitations claiming that current laws are sufficient while others make public declarations about their own cyber policies as they allegedly violate them. The potential for indiscriminate death and destruction that this situation presents needs to be overcome in the short term and will most likely require intense negotiation among the leading cyber powers. Towards this end, the purpose of this study is to fill a gap in the literature as identified in Chapter 2 and serve as a source document for greater debate and action in this area.

Through the use of the Delphi method of inquiry, 18 scholars in the fields of international law and cyber warfare debated numerous issues over three rounds of inquiry to assist in filling the gap in the current literature. A consensus of opinion, measured by 80% of responses being within 2 points on a 7-point Likert-type scale was met for many of the questions evaluated. These results sometimes served to confirm those opinions expressed in the literature review while others went in different directions and added to the existing literature. Perhaps most telling were areas of disagreement, such as to the criteria needed to make a use of force or armed attack designation for a cyber attack or how best to measure these criteria. It was with these questions that the current divide in viewpoints was most evident. These questions are also the requisite starting point for debate and deliberation at the nation-state level if the goal of a regime designed to limit

the use of cyber weapons is to emerge. The social change implications of such state action could lead to the protection of countless lives and property that are currently exposed to risk of cyber attack.

References

Abrams, L. S. (2010). Sampling 'hard to reach' populations in qualitative research: The case of incarcerated youth. *Qualitative Social Work, 9*(4), 536-550. doi:10.1177/1473325010367821

Altschuld, J. W. (1995). Developing an evaluation program: Challenges in the teaching of evaluation. *Evaluation and Program Planning, 18*(3), 259-265.doi:10.1016/S0149-7189(95)00014-3

Barkham, J. (2001). Information warfare and international law on the use of force. *New York University Journal of International Law and Politics*, *34*, 57-113. Retrieved from http://www.cyberconflict.org/repository/legal-issues-ofcyber/Barkham%20IW%20and%20Law%20on%20Use%20of%20Force%202001.pdf

Beech, B. (1997). Studying the future: A delphi study of how multi-disciplinary clinical staff view the likely development of two community mental health centers over the course of the next 2 years. *Journal of Advanced Nursing*, *25*(2), 331-338. doi:10.1046/j.1365-2648.1997.1997025331.x

Best, G. (1983). *Humanity in warfare*. New York, NY: Columbia University Press.

Billo, C., & Chang, W. (2004). *Cyber warfare: An analysis of the means and motivations of selected nation states*. Retrieved from http://www.ists.dartmouth.edu/docs/execsum.pdf

Bodansky, D. (1995). Customary (and not so customary) international environmental law. *Indiana Journal of Global Legal Studies*, *105*, 116-119. Retrieved from http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1511&context=fac_artchop&sei-redir=1&referer=http%3A%2F%2Fscholar.google.co.kr%2Fscholar%3Fq%3DCustomary%2B%2528and%2Bnot%2Bso%2Bcustomary%2529%2Binternational%2Benvironmental%2Blaw%26btnG%3D%26hl%3Den%26as_sdt%3D0%252C5#search=%22Customary%20%28and%20not%20so%20customary%29%20international%20environmental%20law%22

Borg, S. (2005). Economically complex cyberattacks. *IEEE Security and Privacy*, *3*(6), 64-67. doi:10.1109/MSP.2005.146

Brown, D. (2006). A proposal for an international convention to regulate the use of information systems in armed conflict, *Harvard International Law Journal*, *47*(1), 179-221. Retrieved from http://www.harvardilj.org/wp-content/uploads/2010/10/HILJ_47-1_Brown.pdf

Butterworth, T., & Bishop V. (1995). Identifying the characteristics of optimum practice: Findings from a survey of practice experts in nursing, midwifery, and health visiting. *Journal of Advanced Nursing*, *22*(1), 24-32.doi:10.1046/j.1365-2648 .1995.22010024.x

Byers, M. (1995). Custom, power, and the power of rules: Customary international law from an interdisciplinary perspective. *Michigan Journal of International Law*, *17*, 109-174.

Cassese, A. (2005). *International law* (2nd ed.). Oxford, United Kingdom: Oxford University Press.

Caudle, S. (1994). Using qualitative approaches In J. Wholey, H. Hatry, & K. Newcomer (Eds) *Handbook of practical program evaluation*. San Francisco, CA: Jossey-Bass.

Charney, J. I. (1993). Universal international law. *American Journal of International Law*, *87*(4), 529-551.

Charvet, J. (1998). The possibility of a cosmopolitan ethical order based on the idea of universal human rights. *Journal of International Studies*, *27*(3), 523-541. doi: 10.1177/03058298980270031101

Cody, J. A. (2002). Derailing the digitally depraved: An international law & economics approach to combating cybercrime & cyberterrorism. *Michigan State University-DCL Journal of International Law, 11,* 231-259. Retrieved from http://www.oblon.com/sites/default/files/news/36.pdf

Cohen, J. L. (2007). The role of international law in post-conflict constitution-making: Toward a jus post bellum for "interim occupations". *New York Law School Law Review, 51,* 498-532.

Computer Language Company (2015). Payload. PC Magazine online encyclopedia. Retreived from http://www.pcmag.com/encyclopedia/term/48909/payload

Condron, S. M. (2007). Getting it right: Protecting American critical infrastructure in cyberspace. *Harvard Journal of Law &Technology, 20*(2), 403-422. Retrieved from http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf

Creswell, J. W. (2007). *Qualitative inquiry & research design: Choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Custer, R. L., Scarella, J. A., & Stewart, B. R. (1999). The modified delphi technique: A rotational modification. *Journal of Vocational and Technical Education*, *15*(2), 1-10. Retrieved from http://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer

Delbecq, A. L., Van De Ven, A. H., & Gustafson, D. H. (1975). *Group techniques for program planning: A guide to nominal and delphi processes*. Glenview, Il: Scott, Foresman and Co.

Denning, D. E (1998). *Information warfare and security*. Boston: Addison-Wesley.

Denscombe, M. (1998). *The good research guide for small-scale social research projects*. Buckingham, United Kingdom: Open University Press.

Dipert, R. R. (2006). Preventive war and the epistemological dimension of the morality of war. *Journal of Military Ethics*. *5*(1), 32-54. doi: 10.1080/15027570500465728

Dipert, R. R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics*. *9*(4), 384-410. doi: 10.1080/15027570.2010.536404

Downe-Wamboldt, B. (1992). Content analysis: Method, application, and issues. *Health Care or Women International*, *13*, 313-321. doi:10.1080/07399339209516006

Duffield, C. (1993). The delphi technique: A comparison of results obtained using two expert panels. *International Journal of Nursing Studies*, *30*(3), 227-237. doi: 10.1016/0020-7489(93)90033-Q

Dunnigan, J. (2003). *How to make war* (4th ed.). New York, NY: Quill.

Erlandson, D. A. (1993). *Doing naturalistic inquiry: a guide to methods* London: Sage Publications.

Ellis, B. W. (2001). *The international legal implications and limitations of information warfare: What are our options?* Retrieved from http://oai.dtic. mil/oai/oai?verb= getRecord&metadataPrefix=html&identifier=ADA389043.

Evans, M. (2005). *Just war theory: A reappraisal*. Edinburgh, Scotland: Edinburgh University Press.

Fabre, C. (2008). Cosmopolitanism, just war theory, and legitimate authority. *International Affairs*, *84*(5), 963-976. doi: 10.1111/j.1468-2346.2008.00749.x

Fink, A. S. (2000). The role of the researcher in the qualitative research process: A potential barrier to archiving qualitative data. *Forum: Qualitative Social Research*, *1*(3), 1-15. Retrieved from http://www.qualitative-research.net/index.php/fqs/ article/view/1021/2201

Flanagan, A. (2005). The law and computer crime: Reading the script of reform. *International Journal of Law and Information Technology*, *13*(1), 98-117. doi: 10.1093/ijlit/eai004

Forge, J. (2009). Proportionality, just war theory and weapons innovation. *Science and Engineering Ethics*, *15*(1), 25-38. doi:10.1007/s11948-008-9088-z

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer law and Security Review*. *26*, 298-303. doi:10.1016/j.clsr.2010.03.003

Gill, T. D. (2006). The temporal dimension of self-defense: Anticipation, preemption, prevention, and immediacy. *The Journal of Conflict and Security Law*, *11*(3), 361-369. doi:10.1093/jcsl/krl018

Given, L. M. (2008). *The sage encyclopedia of qualitative research methods (Vol. 2).* New York, NY: SAGE Publications.

Goh, G. M. (2004). Keeping the peace in outer space: A legal framework for the prohibition of the use of force, *Space Policy*, *20*(4), 259-278. doi:10.1016/ j.spacepol.2004.08.002

Greenbach, P. (2003). The role of values in education research: The case for reflexivity. *British Educational Research Journal*, *29*(6), 791-801. doi:10.1080/014119203 2000137303

Greenberg, L. T., Goodman, S. E., & Soo Hoo, K. J. (1998). *Information warfare and international law*. Washington D.C.: National Defense University Press.

Hargrove, J. L. (1987). The "nicaragua" judgement and the future of the law of force and self defense. *American Journal of International Law*, *81*(1), 135-143.

Henkin, L. (1996). Human rights and state sovereignty. *The Georgia Journal of International and Comparative Law*, *25*, 31-47. Retrieved from http:// digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1386&context=gjicl

Higgins, R. (1994). *Problems and process: International law and how we use it*. Oxford, United Kingdom: Clarendon Press.

Hildreth, S. A. (2001). *Cyberwarfare*. (CRS Reports for Congress). Retrieved from George Washington University website: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-014.pdf

Hollis, D. B. (2007). *New tools, new rules: International law and information operations* (Research Paper No. 2007-15). Retrieved from Social Science Research Center website: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009224

Hoisington, M. (2009). Cyberwarfare and the use of force giving rise to the right of self defense. *Boston College International and Comparative Law Review*, 32 (16), 439-454. doi:10.2139/ssrn.1542223

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288. doi: 10.1177/1049732305276687

Hsu, C. C., & Sandford, B. A. (2007). The delphi technique: Making sense of consensus. *Practical Assessment, Research, & Evaluation, 12*(10), 1-8. Retrieved from http://pareonline.net/pdf/v12n10.pdf

Huang J. (2009). New challenges to the traditional principles of the law or war presented by information operations in outer space. *Journal of Politics and Law*, *2*(1), 39-43. doi:10.5539/jpl.v2n1p39

Intoccia, G. F., & Moore, J. W. (2006). Communications technology, warfare, and the law: Is network a weapon system? *Houston Journal of International Law*, *28*(2), 467-483. Retrieved from https://www.questia.com/read/1G1-146272030/communications-technology-warfare-and-the-law-is

Jacobs, J. M. (1996). *Essential assessment criteria for physical education teacher education programs: A delphi study* (Unpublished doctoral dissertation). West Virginia University, Morgantown, West Virginia.

Jariath N., & Weinstein, J. (1994). The delphi methodology: A useful administrative approach. *Canadian Journal of Nursing Administration, 7*(3), 29-42.

Jensen, E. T. (2002). Computer attacks on critical national infrastructure: A use of force invoking the right of self-defense. *Stanford Journal of International law*, *38*, 207-240. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=987046

Jurich, J. P. (2008). Cyberwar and customary international law: The potential of a "bottom-up" approach to an international law of information operations. *Chicago Journal of International Law*, *9*(1), 275-296. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=987046

Kanuck, S. (1996). Information warfare: New challenges for public international law. *Harvard International Law Journal*, *37*, 272-289.

Kanuck, S. (2010). Sovereign discourse on cyber conflict under international law. *Texas Law Review*, *88*(7). 1571-1597. Retrieved from https://ahab.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Kanuck.pdf

Kelly, J. P. (2000). The twilight of customary international law. *Virginia Journal of International Law*, *40*(2), 449-543. Retrieved from http://ericposner.com/Understanding%20the%20Resemblance%20Between%20Modern%20and%20Traditional%20Customary%20International%20Law.pdf

Kegley, C. W., & Raymond, G. A. (1999). *How nations make peace*. New York, NY: St. Martin's/Worth.

Kelsey, J. T. G. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review, 106,* 1427-1451. Retrieved from https://www.law.upenn.edu/institutes/cerl/ conferences /cyberwar/papers/reading/Kelsey.pdf

Kumar, P. (2002). Tactics to combat cyber-attacks. *Business Line*. Retrieved from http://www.thehindubusinessline.in/2002/01/09/stories/2002010901291300.htm

Leech, N. L., & Onwuebuzie, A. J. (2008). Debriefing In L.M. Given (Ed) *The sage encyclopedia of qualitative research methods*. Thousand Oaks, CA: Sage.

Lin, H. S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law and Policy*, *4*(64), 63-86. Retrieved from http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf

Linstone, H. A., & Turoff, M. (1975). Introduction In H.A. Linstone & M. Turoff (Eds.) *The delphi method:Techniques and applications*. Reading, MA: Addison-Wesley Publishing Company.

Ludwig, B. (1997). Predicting the future: Have you considered using the delphi methodology. *Journal of Extension*. *35*(5), 1-4. Retrieved from http://www.joe.org/joe/1997october/tt2.php/index.php

Ludwig, B. G. (1994). *Internationalizing extensions: An exploration of the characteristics evident in a state university extension system that achieves internationalization* (Unpublished doctoral dissertation). The Ohio State University, Columbus, Ohio.

Lukasik, S. J. (2000). Protecting the global information commons. *Telecommunications Policy, 24*, 519-531. doi:10.1016/S0308-5961(00)00038-0

Malanczuk, P. (1997). *Akehurst's modern introduction to international law* (7th ed). New York, NY: Routledge.

McNabb, D. E. (2008).*Research methods in public administration and nonprofit management: Quantitative and qualitative approaches* (2nd ed.). Armonk, New York, NY: M.E. Sharpe, Inc.

Meron, T. (1996). The continuing role of custom in the formation of international humanitarian law. *The American Journal of International Law, 90*(235), 238-249. Retrieved from http://www.jstor.org/stable/2203686

Michael, J. B., Wingfield, T. C., & Wijesekera, D. (2003). *Measured responses to cyber attacks using Schmitt analysis: A case study of attack scenarios for a software-intensive system.* COMPSAC '03 Proceedings of the 27th Annual International Conference on Computer Software and Applications. IEEE Computer Society: Washington, DC, USA, 621-626. doi:10.1109/CMPSAC.2003.1245406

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed). Thousand Oaks, CA: Sage.

Morse, J. M., & Field, P. A. (1995). *Qualitative research methods for health professionals* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Murphy, M. K., Black, N., Lamping, D. L., McKee, C. M., Sanderson, C. F. B., Askham J., & Marteau, T. (1998). Consensus development methods and their use in clinical guidance development. *Health Technology Assessment, 2*(3), 1-88. Retrieved from http://hdl.handle.net/10068/432579

Neff, S. C. (2000) *The rights and duties of neutrals*. Manchester, United Kingdom: Manchester University Press.

Neumann, P. (1995). *Computer related risks*. Reading MA: ACM Press.

Ochoa, C. (2007). The individual and customary international law formation. *Virginia Journal of International Law*, *48*(1), 119-186. Retrieved from http://www.vjil.org/assets/pdfs/vol48/issue1/119-186.pdf

O'Donnell, B. T., & Kraska, J. C. (2003). Humanitarian law: Developing international rules for the digital battlefield. *Journal of Conflict & Security Law*, *8*, 133-160. doi:10.1093/jcsl/8.1.133

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. T. (2008). Interviewing the interpretive researcher: A method for addressing the crises of representation, legitimation, and praxis. *International Journal of Qualitative Methods, 7*(4), 1-18. Retrieved from www.researchgate.net/profile/Kathleen_Mt_Collins/publication/228852531_Interviewing_the_interpretive_researcher_A_method_for_addressing_the_crises_of_representation_legitimation_and_praxis/links/53d96de00cf2a19eee8704f4.pdf

Osterdahl, I., & van Zadel, E. (2009). What will jus post bellum mean? Of new wine and old bottles. *Journal of Conflict & Security Law, 1*, 1-33. doi:10.1093/jcsl/krp018

O'Sullivan, E., Rassel, G.R., & Berner, M. (2003). *Research methods for public administrators* (4th ed.). New York, NY: Addison Wesley Longman, Inc.

Perry, D. (2009). *Partly cloudy: Ethics in war, espionage, covert action, and interrogation*. Lanham, MD: The Scarecrow Press.

Pill, J. (1971). The delphi method: substance, context, a critique and an annotated bibliography. *Socio-Economic Planning and Science, 5*(1), 57-71. doi:10.1016/0038-0121(71)90041-3

Powell, C. (2003). The delphi technique: Myths and realities. *Journal of Advanced Nursing*, *41*(4), 376-382. doi:10.1046/j.1365-2648.2003.02537.x

Primoratz, I. (2002). Michael Walzer's just war theory: Some issues of responsibility. *Ethical Theory and Moral Practice, 5*(2), 221-243. doi: 10.1023/A:1016032 623634

Ranum, M. (2004). *The myth of homeland security*. Indianapolis, IN: Wiley.

Reisman, W. M. (1987). The cult of custom in the late 20th century. *California Western International Law Journal, 17*, 133-145. Retrieved from http://digitalcommons .law.yale.edu/fss_papers/732

Richmond, J. (2012). Evolving battlefields: Does stuxnet demonstrate a need for modifications to the law of armed conflict. *Fordham International Law Journal, 35*(3) 843-893.

Roberts, A. E. (2001). Traditional and modern approaches to customary international Law: A reconciliation. *American Journal of International Law, 95*, 757-791. Retrieved from http://www.jstor.org/stable/2674625

Rowe, E. (1994). *Enhancing judgment and decision making: A critical and empirical investigation of the delphi technique* (Unpublished doctoral dissertation). University of Western England, Briston, United Kingdom.

Rowe, G., Wright, G., & Bolger, F. (1991). Delphi: A reevaluation of research and theory. *Technical Forecasting Social Change*. *39*(3), 235-251. doi:10.1016/0040-1625(91)90039-I

Rowe, N. C. (2009). The ethics of cyberweapons in warfare. *International Journal of Cyberethics*, *1*(1), 20-31. Retrieved from http://indianstrategicknowledge online.com/web/thrust5_cyberweaponsethcis.pdf

Rho, J. J. (2007). Blackbeards of the twenty-first century: Holding cybercriminals liable under the alien tort statute. *Chicago Journal of Internal law*, *7*(2), 695-719.

Sachman, H. (1975). *Delphi critique*. Boston, MA: Lexington Books.

Sassoli, M. (2003). Legitimate target of attacks under international humanitarian law. *Harvard Program on Humanitarian Policy and Conflict Research*. Retrieved from http://www.hpcrresearch.org/sites/default/files/publications/Session1.pdf

Schaap, A. J. (2009). Cyber warfare operations: Development and use under international law. *Air Force Law Review, 64*, 121-173.

Scheibe, M., Skutsch, M., & Schofer, J. (1975). Experiments In Delphi methodology H.A. Linstone & M. Turoff (Eds.) *The delphi method: Techniques and applications*. Reading, MA: Addison-Wesley Publishing Company.

Schmitt, M. N. (1998). Bellum americanum: The us view of twenty-first century war and its possible implications for the law of armed conflict. *Michigan Journal of International Law*, *19*(4), 1051-1090. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603792

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law, 37*, 885-937. Retrieved from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993

Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, *84*(846), 365-399. Retrieved from https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf

Silver, D. B. (2002). Computer network attack as a use of force under article 2(4) of the united nations charter. *Naval War College International Law Studies*, *76*, 73-97.

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The delphi method for graduate research. *Journal of Information Technology Education, 6*, 1-21. Retrieved from http://jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf

Sofaer, A. D., Clark, D., & Diffie, W. (2010). *Cyber security and international agreements*. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Retrieved from http://www.nap.edu/catalog/12997.html

Sommers, B. (2011). *Types of samples*. Retrieved from http://psychology.ucdavis.edu/sommerb/sommerdemo/sampling/types.htm

Stahn, C. (2007). Jus ad bellum, jus in bello…jus post bellum? – Rethinking the conception of the law of armed forces. *European Journal of International Law*. *17*(5), 921-943. doi:10.1093/ejil/chl037

Stern, P. C. (2011). Design principles for global commons: Natural resources and emerging technologies. *International Journal of the Commons, 5*(2), 213-232. Retrieved from mercury.ethz.ch/serviceengine/Files/ISN/138487/ichapter section_singledocument/e6de0254-52ca-41e0-b9f7-90fa0a00003e/en/03.pdf

Taddeo, M. (2013). Just war theory and cyber warfare. *Practical Ethics*. Retrieved from http://blog.practicalethics.ox.ac.uk/2012/06/just-war-theory-and-cyber-warfare/

Tesch, R. (1990). Qualitative research: Analysis types and software tools. Bristol, PA: Falmer.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967). Retrieved from http://disarmament.un.org/treaties/t/outer_space

Trochim, W. M. K., & Donnelly, J. P. (2007). *The research methods knowledge base* (3rd ed.). Mason, Ohio: Thomson.

Ulschak, F. L. (1983). *Human resource development: The theory and practice of needs assessment*. Reston, VA: Reston Publishing Company, Inc.

Underdal, A. (1980). *The politics of international fisheries Management: The case of the north east atlantic*. New York, NY: Cornell University Press.

Vogler, J. (2012). Global commons revisited. *Global Policy*, *3*(1), 61-71.

Walker, G. K. (2000). Information warfare and neutrality. *Vanderbilt Journal of Transnational Law*, *33*(5), 1082-1195.

Walzer, M. (2000). *Just and unjust wars: A moral argument with historical illustrations* (3rd ed). New York, NY: Basic Books.

Walzer, M. (2004). *Arguing about war*. New Haven, CT: Tale University Press.

Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of Article 2(4). *Yale Journal of International Law*, *36*(2), 421-459. Retrieved from http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf

Weber, R. P. (1990). Basic content analysis. Beverly Hills, CA: Sage Publications.

Weisburd, A. A. (1988). Customary international law: The problem of treaties. *Vanderbilt Journal of Transnational Law*. *21*(1), 1-46. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2245158

Whitby, S. (2002). *Biological warfare against crops*. Houndmills, United Kingdom: Palgrave.

Williams, R. E., & Caldwell, D. (2006). Jus post bellum: Just war theory and the principles of just peace. *International Studies Perspectives*, *7*, 309-320. Retrieved from http://faculty.pepperdine.edu/rwilliam/Jus_Post_Bellum.pdf

Wilske, S., & Schiller, T. (1997). International jurisdiction in cyberspace: Which states may regulate the internet. *Federal Communications Law Journal*, *117*, 129-144. Retrieved from http://www.repository.law.indiana.edu/fclj/vol50/iss1/5

Wilson, C. (2005). *Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress* (CRS Reports for Congress). Retrieved from Federation of American Scientists Website: http://www.fas.org/irp/crs/RL32114.pdf

Witkin, B. R., & Altschuld, J. W. (1995). *Planning and conducting needs assessment: A practical guide*. Thousand Oaks, CA: Sage Publications.

Appendix A: Consent Form

Participant Consent Form

You are invited to participate in a research study conducted to determine the legality of deploying computer viruses against specific military, civilian and dual-use targets under various international laws. The researcher is inviting adult scholars and professionals with a background in cyber warfare and international law to participate in the study. Participants are being selected based on their expertise in these fields which have given them the necessary knowledge and experience to make sound determinations of where they believe existing international laws have applicability and where a lack of coverage exists. It is the intent of this study to find a consensus of opinion among the participants and to document the individual justifications for opinions outside of the consensus.

This study is being conducted by a researcher named Kenneth Gualtier, who is a doctoral student at Walden University. The researcher is employed as a college faculty member at another institution and this study is separate from that role. Please note that while the researcher is not an agent of the United States government, he is ethically bound to report any information about illegal activities uncovered during the course of this study to the proper authorities.

Background Information:

The purpose of this study is to reach a consensus as to the current standing of cyber warfare under international law and to recommend changes to the law as needed. The use of cyber warfare is largely unregulated by international law and the applicability of current laws may be a matter of some debate. At the same time the majority of cyber weapons are designed to target civilian and dual-use industries. This creates a great risk for the loss of civilian lives and property in the event of a large scale cyber operation. By more clearly defining what limitations may exist under current international law, and finding consensus among scholars in the field as to what limitations are needed on cyber weapons to bring them in line with the existing confines on kinetic attacks, we can begin to address the legality of cyber warfare and therefore, potentially save lives and property.

Procedures:

If you agree to be in this study you will be asked to:

- Respond in writing as described in the Statement of Consent below within five days of receipt of this consent form agreeing to participate.
- Complete a nine-question narrative questionnaire and return it to the researcher within two weeks.
- Complete two subsequent questionnaires using a Lykert-type scale and return them to the researcher within ten days.

- It is expected that five to seven days will be needed between each round of enquiry to allow the researcher to compile data and perform other administrative functions.
- It is expected that the cumulative total for all three rounds of enquiry, and the time between rounds, will last approximately seven weeks.

An example of a narrative question from the first questionnaire is "What limitations exist with proportionality, necessity, and immediacy in order for a state to claim self-defense under international law, once the state falls victim to a computer virus attack directed at state, commercial, or civilian infrastructure?"

Voluntary Nature of the Study:

This study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University or your place of business will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study:

Being in this type of study involves some risk of the minor discomforts that can be encountered in daily life, especially with the first round of enquiry, such as those involved with sitting at a computer terminal and typing detailed responses to posed questions. Being in this study would not pose risk to your safety or wellbeing.

By utilizing a Delphi method with this study all participants will be able to see the (anonymous) opinions of their colleagues as well as their justifications for opinions outside of the consensus. This will allow you to possibly refine your own opinions after each round of enquiry. At the conclusion of the study, a consensus of beliefs will have been established for all participants that you can apply to your own research or employment.

Payment:

Your participation in this study will not result in the issuance of financial payment or gifts.

Privacy:

Any information you provide will be kept confidential. The researcher will not use your personal information for any purposes outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. Data will be kept secure by retaining all files on a password-protected

computer and within encrypted compression files. Data will be kept for a period of at least 5 years, as required by the university.

Contacts and Questions:

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via e-mail at XXXXXXXXXX. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is 02-24-14-0140351 and it expires on February 23, 2015. Please print or save this consent form for your records.

Statement of Consent:

I have read the above information and I feel I understand the study well enough to make a decision about my involvement. By replying to this email with the words, "I consent", I understand that I am agreeing to the terms described above.

Appendix B: Questionnaire 1

Information Operations under International Law
Questionnaire One

Please complete and return this questionnaire to Kenneth Gualtier at XXXXX no later than April 13, 2014. In consideration of your time, you may use bullet statements or short phrases and respond directly under the questions listed below.

Question 1: Under what circumstances might the use of a computer virus by a foreign government against state, commercial, or civilian targets constitute a "use of force" under the United Nations charter?

Question 2: Under what circumstances might the use of a computer virus by a foreign government against state, commercial, or civilian targets constitute an "armed attack" under the United Nations charter?

Question 3: What limitations exist with proportionality, necessity, and immediacy in order for a state to claim self-defense under international law, once the state falls victim to a computer virus attack directed at state, commercial, or civilian infrastructure?

Question 4: In what ways are international laws covering neutrality affected by the unique nature of cyber warfare? What changes to current laws governing neutrality may be needed to fully encompass cyber warfare?

Question 5: Under what circumstances might a computer virus attack against commercial or civilian targets be legal, while the same target is protected from traditional kinetic attacks under international law?

Question 6: Under what conditions might cyberspace qualify as a global common and how might such a designation affect the legal use of computer viruses as a means of cyber warfare under the law?

Question 7: Is the use of customary law sufficient for the development of legal limitations specifically aimed at cyber warfare? If so, how might such a regime develop?

Question 8: What ethical standards should be taken into consideration when developing a regime to limit the use of cyber warfare?

Question 9: What factors have contributed to the lack of legal limitations specifically addressing cyber warfare by the international community?

Appendix C: Questionnaires 2 and 3

Information Operations under International Law

Please complete and return this questionnaire to Kenneth Gualtier at XXXXXXXXXXX no later than XXXXXX. After reviewing the results of the second questionnaire, please reevaluate and score your responses to the statements below. Provide a justification for responses outside of the consensus or for statements that have not achieved a consensus.

Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
❶	❷	❸	❹	❺	❻	❼

SECTION A: USE OF FORCE AND ARMED ATTACK DESIGNATIONS

1. An effective formula for determining whether a cyber attack has reached the level of use of force or armed attack under international law is by comparing its scope and effect to kinetic attacks.
   Scale Score:
   Justification:

2. Although a cyber attack may fall below the standard of use of force or armed attack they most likely would still be deemed illegal under criminal law.
   Scale Score:
   Justification:

3. To classify a cyber attack as an armed attack under international law the cyber attack must threaten the territorial integrity or political independence of the offended state.
   Scale Score:
   Justification:

4. A cyber attack constitutes a use of force whenever it targets critical national infrastructure.
   Scale Score:
   Justification:

5. A significant loss of control over a computerized system is serious enough to warrant a designation of use of force under international law.
   Scale Score:
   Justification:

6. Because the STUXNET virus caused severe physical damage to equipment within the Natanz nuclear facility it would qualify as an armed attack.
   Scale Score:
   Justification:

7. A use of force or armed attack designation can be assigned collectively to cyber attacks that reoccur in a short period of time even though the individual attacks do not warrant this designation.
   Scale Score:
   Justification:

8. A cyber attack against a major economic entity, such as the New York Stock Exchange, that results in no loss of life or physical damage may still meet the requirements of armed attack under international law.
   Scale Score:
   Justification:

9. A cyber attack that alters data or the functionality of a system, but causes no direct or indirect physical damage, cannot be classified as an armed attack under international law.
   Scale Score:
   Justification:

10. A cyber attack that has been foiled by passive defenses, and which otherwise would have resulted in serious physical damage or loss of life, may still be categorized as an armed attack.
    Scale Score:
    Justification:

SECTION B: PROPORTIONALITY, NECESSITY, IMMEDIACY, AND ATTRIBUTION

11. For cyber attacks, immediacy should be predicated on the time reasonable attribution is made rather than when the effects of the attack are detected.
    Scale Score:
    Justification:

12. Because the STUXNET virus was discovered so long after it began degrading the equipment in the Natanz nuclear facility, Iran lost the legal right under international law to respond in self-defense.
    Scale Score:

Justification:

13. The concept of self-defense under international law is problematic when applied to cyber attacks. The stated point of self-defense, to disarm the attacker, is difficult to accomplish in cyber space considering that the attacker is most likely not limited to a specific computer, server, or facility.
    Scale Score:
    Justification:

14. The law of armed conflict would require that any response to a cyber attack remain in the cyber arena to meet the obligation for proportionality.
    Scale Score:
    Justification:

15. Necessity would be difficult to argue in response to a cyber attack, as any response by the offended state would most likely not curb the ongoing effects of the initial cyber attack.
    Scale Score:
    Justification:

16. The fact that a cyber attack has originated from a government operated computer system is not sufficient enough evidence to attribute the attack to the state nor to take action against the state.
    Scale Score:
    Justification:

17. Cyber attacks may be launched for defensive purposes in the name of necessity even when the identity of the aggressor cannot be clearly attributed.
    Scale Score:
    Justification:

SECTION C: MEANS AND TARGETS OF CYBER ATTACK

18. The concept of anticipatory self-defense only applies to instances when a cyber attack is a component of a greater armed assault
    Scale Score:
    Justification:

19. No target, civilian or government, has complete legal protection from a cyber attack if there is an overriding military necessity.
    Scale Score:
    Justification:

20. A cyber attack, that uses malware that cannot be controlled after being deployed, would be illegal under international law.
    Scale Score:
    Justification:

21. To remain legal under international law, cyber-defense systems may not have an active component that automatically responds to a cyber attack with offensive measures of its own.
    Scale Score:
    Justification:

22. Cyber weapons may be illegal under international law because governments cannot reasonably maintain control over them or be held accountable for their use.
    Scale Score:
    Justification:

23. Civilians maintain their non-combatant protections under international law even when directly participating in cyber attacks.
    Scale Score:
    Justification:

24. A cyber weapon designed to look like legitimate civilian network traffic would violate the prohibition against perfidy.
    Scale Score:
    Justification:

25. A cyber weapons designed to look like the legitimate network traffic of an international organization, such as the United Nations or Red Cross, would be illegal under international law.
    Scale Score:
    Justification:

26. It is conceptually impossible to perform an economic blockade solely by cyber means and, therefore, any denial of service attack against a state's industries cannot be labeled as such.
    Scale Score:
    Justification:

SECTION D: NEUTRALITY

27. The Hague Convention V states that neutral states have no obligation to disrupt communications passing through their publically accessible communication systems.

This would not apply to cyber weapons since they are means of attack rather than communications.
Scale Score:
Justification:

28. Because it would be an undue burden on the citizens of a neutral state to disrupt network communications in order to stop the use of public systems by states involved in an armed conflict, the neutral state is under no legal obligation to do so.
Scale Score:
Justification:

29. Because of the redundancy built into networks, and the inability to direct packets through specific paths, the travelling of packets containing cyber weapons through the territory of non-belligerents does not violate their neutrality.
Scale Score:
Justification:

30. A state may legally disable or destroy network infrastructure in a neutral country if the neutral country is unable or unwilling to stop the use of its equipment to route cyber attacks.
Scale Score:
Justification:

SECTION E: A CYBER GLOBAL COMMONS

31. Because every component of cyber space resides in the sovereign territory of a nation-state or under its control, an international agreement designating cyber space a global common is virtually impossible.
Scale Score:
Justification:

32. Designating cyberspace a global common would eliminate any concerns over neutrality or sovereignty when conducting cyber warfare operations.
Scale Score:
Justification:

SECTION F: ETHICS AND CYBER-SPECIFIC LEGAL LIMITATIONS

33. The use of customary law to develop limitations specific to cyber warfare is restricted because the secrecy surrounding cyber operations has led to a lack of available state practice or *opinion juris.*
Scale Score:
Justification:

34. Because the leading cyber powers have shown no inclination towards limiting their cyber warfare potential, the use of customary law is likely the only way to develop such limitations.
    Scale Score:
    Justification:

35. States have intentionally been unwilling to address legally limiting the use of cyber weapons so as to allow for maximum flexibility in the conduct of cyber operations.
    Scale Score:
    Justification:

36. The inequality of technological capabilities has been a primary reason why leading cyber states have been unwilling to address legally limiting the use of cyber weapons.
    Scale Score:
    Justification:

37. The exponential growth of technology would most likely leave any specific cyber warfare legislation obsolete shortly after it was enacted.
    Scale Score:
    Justification:

38. Any international agreement to limit the use of cyber weapons is likely to be ignored during an actual conflict by those states capable of using them effectively; regardless of whether they are a signatory to the treaty.
    Scale Score:
    Justification:

39. Preemptive cyber attacks can be morally justified if the evidence exceeds a ninety percent likelihood of armed attack and that the provocation is expected to cause a high degree of damage or casualties.
    Scale Score:
    Justification:

40. States have an obligation to defend their citizens from cyber attacks even to the extent of using some illegal or unethical means to do so.
    Scale Score:
    Justification:

41. Each state has an affirmative duty to formally review the legality of any cyber weapon and operation prior to its deployment.
    Scale Score:
    Justification:

42. Each state has an affirmative duty to continuously monitor their cyber attacks, when feasible, so as to cancel or suspend the attack if conditions change such as posing a threat to the civilian population.
    Scale Score:
    Justification:

********** END OF SURVEY **********