January 2012

Cyberwar and International Law: An English School Perspective

Anthony F. Sinopoli
University of South Florida, serapis10@yahoo.com

Cyberwar and International Law: An English School Perspective

by

Anthony Francesco Sinopoli

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Government and International Affairs
College of Arts and Sciences
University of South Florida

Major Professor: Harry E. Vanden, Ph.D.
Kiki Caruson, Ph.D.
M. Scott Solomon, Ph.D.

Date of Approval:
November 2, 2012

Keywords: cyber-attack, humanitarian law, information infrastructure,
information operations, international society

Table of Contents

Abstract

Cyberwar challenges future endeavors of state security. As technological capability has improved, and access to information has become more widespread the importance of the issue in today's ever-globalizing world grows each day. A primary objective is to evaluate the place of cyber-warfare against nation-states and any repercussions under an international law paradigm. Utilizing an English School perspective, emphasis will be applied to the argument that disruptive circumstances could come to fruition if international conventions are not created to bring consensus and order among nation-states on this subject. This study hypothesizes that a future application could be an agreement under international law, beyond current regional cooperative initiatives. Since cyber-related attack is a relatively new development, the issue lacks adequate historical context. In addition, since state behavior is a major contributor to the interpretation of international law, the matter is in need of a clear delineation of the norms that define the phenomena and what acceptable responses might entail. Case study analysis will highlight recent examples of state behavior and cyber-related attacks and sabotages.

Chapter One:

Introduction

An *Information Week* article states that in 2010, cyber-attacks in U.S. federal networks rose 39% since a year prior, reporting 41,776 malicious cyber incidents (Montalbano, 2011). Clarke and Knake claim that, "on average in 2009, a new type or variant of malware was entering cyberspace every 202 seconds" (Clarke and Knake, 2010). As technological capability has improved, and access to information has become more widespread the importance of the issue in today's ever-globalizing world has become more vital than ever. Cyberwar is an example of technological advancement that challenges future endeavors of state security. Cyberwar can be defined as, "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke and Knake, 2010). Cyberwar and its relevance in international security matters continues to be a pivotal issue as technological opportunity is more accessible to greater numbers of the population.

In addition to briefly exploring types of cyber-attacks for the purposes of inquiry, I look to answer an important question: Is international law currently equipped to effectively advise nation-states on the question of cyber-warfare, or does the issue of cyberwar against nation-states require new norms of international law? Emphasis will be given to the argument that disruptive circumstances, worse than those already realized, could come to fruition in today’s technologically sophisticated times, if international conventions are not created to bring consensus among nation-states on necessary protections on this subject. In light of this danger, one could ask if international law might offer an opportunity for agreement among members of the international community as to protections from various types of cyberwar and appropriate responses to cyber-attacks once they have occurred.

This effort will analyze case studies of various examples of cyber-attack on nation-states. I analyze the Estonian cyber-attack of 2007, the Russian-Georgian conflict of 2008, as well as the Stuxnet and Flame infiltrations of Iranian systems to gain a foundation for further analysis. Case studies of recent cyber-related incidents among nation-states demonstrate their relevance in today's world climate and help to identify and categorize cyber-attacks. Case studies, “permit a deeper understanding of causal processes, the explication of general explanatory theory, and the development of hypotheses regarding difficult-to-observe phenomenon” (Johnson, Reynolds and Mycoff, 2008). This study cannot reasonably claim to account for every feature of the cyber-attacks in question, for that is another endeavor entirely. Rather, the intention is to afford assessment of the examples to establish classification of the types of attack and any observable objective in the attempted attack.

This study hypothesizes that a future agreed upon norm could be an agreement within international law, beyond current regional cooperative initiatives. Through case studies, I examine behavior among states regarding cyber-related attacks and sabotages. I argue that the international community will be forced to come to consensus on the issue of cyberwar among nation-states, in the form of newly formed norms of international law. Kanuck argues, "Without any controlling legal authorities for cyber conflicts today, there remains broad room for maneuver—both diplomatically and militarily" (Kanuck, 2010). Since state behavior is a major contributor to interpretation of international law, the lack of consensus leads to the initial conclusion that cyber-related attack is a relatively new development. Therefore, the issue lacks adequate historical context and is in need of a clear delineation of the norms that define the phenomena and what acceptable responses might entail (retorsion, retaliation, sanctions).

This direction is not without precedent. Sofaer and Goodman state, "Those who support adoption of a multilateral approach to deal with this quintessentially transnational problem must be encouraged by the fact that states have consistently adopted multilateral solutions to deal with technologies that affect populations across national boundaries" (Sofaer and Goodman, 2001). British Foreign Secretary Hague has called for nations to discuss "norms for state behavior in cyberspace" (Farnsworth, 2011). Following the documented cyber-attack on Estonia of 2007, the North Atlantic Treaty Organization (NATO) was unable to act, lacking a previously agreed upon response to such an incident; however, at the 20th NATO Summit in 2008 in Bucharest, the group formally addressed cyber-attacks (Hathaway, et al. 2012). Hughes notes that following the summit, two new NATO divisions were created in order to focus on the threat of cyber-attacks: The Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence (Hughes, 2009). The example of NATO and its cyber defense initiatives created as a result of the 2008 Bucharest Summit do not necessarily qualify as a widespread and inclusive endeavor. Still, it does highlight the possibility of multilateral cooperation and agreement among states regarding the issue of cyberwar. Agreement on application is vague at this stage, but members continue dialogue on the matter (Center for Strategic and International Studies, 2012). The Budapest Convention on Cybercrime, which entered into effect in 2004, includes thirty member states, including the United States. This treaty was created to allow for interoperability among national laws and greater cooperation among member states. However, similar to the NATO initiatives, progress has been slow and direction has lacked focus. Furthermore, many other states, such as China, Brazil and Russia have not signed it, undermining its applicability in a practical sense.

In addition to the noted agreements above, the United Nations (UN) Charter states, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security" (Article 51). As it pertains to cyber-attack, Benatar shows that a broad interpretation of Article 2(4) of the UN

Charter could lead one to "…demonstrate that cyber-attacks are perhaps not a new kind of force but instead a new kind of *armed* force" (Benatar, 2009). Interestingly, *jus ad bellum* (the right to war) does not categorize which weaponry is authorized, and Benatar states that the legality or the question thereof with regards to cyber force is difficult to ascertain. However, Benatar (referencing Schmitt, Harrison, Dinniss, Wingfield and Kelsey) does reference the International Telecommunications Convention, the laws of neutrality, and international humanitarian law as those norms that may be challenged by the use of cyber force.

Conversely, some opponents argue against an international convention on cyber-warfare. These challengers claim that independent and autonomous efforts on the parts of states should be the main prospect. Any international convention only serves to limit state opportunity to create its own framework to handle cyberwar. In addition, there is the question of, "…ambiguities that will prevent any meaningful international discourse and resolution from taking place" (Muir, 2011). Muir sees the issue strictly from an American perspective, as the world leader in cyber operations. Muir claims that unilateral action on the part of the United States is the correct course of action in attaining what he sees as the four goals for, "…The development of a legal regime around cyber warfare (Muir, 2011):

1) Protect the full panoply of property rights
2) Minimize cyber-attacks and reduce their collateral damage

3) Deter the use of proxies in the commission of cyber-attacks

4) Provide legal recourse for aggrieved parties"

Muir's argument for the disadvantageousness to the United States of an international agreement, calling for the unilateral action on the part of the United States to attain the above goals clearly falls in the classical realist camp. However, enlightened realists could argue that it may be in the best interests of the state to enter into international agreements on cyber-warfare. The realist perspective will be briefly described later in this paper.

Conversely, some argue that the issue of cyberwar is not a relevant issue. Rid argues that cyberwar is not a separate threat at all. He claims that cyberwar is simply, "sophisticated versions of three activities that are as old as warfare itself: subversion, espionage and sabotage" (Rid, 2012). Citing Clausewitz on "the most concise concept of war," Rid claims that past cyber-attacks do not meet the criteria of an act of war: violent character, instrumentality as a means to an end and political nature. Rid does not believe that there will be any comparatively large-scale event on the scale of the Hiroshima attack or the Pearl Harbor attack of World War II, and to compare cyberwar to nuclear war is "misplaced and problematic" (Rid, 2012). I argue that Rid is in the marginal perspective and his argument a naïve view of the issue.

Others will find Rid in the minority. They argue that as the nations of the world continue to mature in their technological advances, the progression leads to reliance on these capabilities. Critical infrastructures can come under extreme duress, and "it is easy to imagine far more momentous and malicious information attacks that, by disabling infrastructures or causing them to malfunction, could impose economic hardship on citizens, physically harm them, impair military operations, or undermine confidence in global and national financial and commodities markets by introducing erroneous information" (Grove, Goodman and Lukasik, 2000). The authors argue that access to cheap computer processing equipment, greater network speeds and the increasing interdependency of infrastructures only exacerbate the inevitability and magnitude of such possibilities. They propose active defenses through the imposition of penalties under international law and making failure an expensive proposition, such as damaging the attacking equipment. Active defense systems may be useful in the protection of infrastructure elements, such as nuclear power plants. By extension, the authors also argue that, "Interpretations of the UN Charter and of the laws of armed combat will have to evolve accordingly in order to accommodate the novel definitions of the use of force that such attacks imply" (Grove, Goodman and Lukasik, 2000). The end result is the potentiality for consensus and establishing legal standards on this rapidly escalating issue. Such consensus is pivotal for international law to offer any guidance.

Kanuck points to the 1990s as the decade in which "efforts to analyze 'information warfare' under international law" took shape (Kanuck, 2010). He argues that states try to "exercise their sovereignty over cyberspace" (Kanuck, 2010). The challenge of cyberspace to the conception of physical boundaries that is so endemic to international law makes the effort to exercise sovereignty a unique undertaking. It is not simply a question of state government influence, but also that of private companies and sometimes a combination of the two entities. Kanuck states, "Once one appreciates that governments seek to extend their sovereign authority into this new realm, it then becomes necessary to analyze how their interests may align or conflict in regard to nonexclusive resources" (Kanuck, 2010). Therefore, Kanuck argues in favor of collective standards where unilateral action is not the answer.

Hollis reasons for these norms, claiming that attribution is a great challenge. Hollis states, "I argue that international law needs a new norm for cybersecurity: a duty to assist or DTA" (Hollis, 2011). Utilizing the classic "SOS" maritime idea, this line of reasoning removes the burden of attribution, elevating the need to mitigate harm. If norms existed that could help regulate cyber threats through a collectively agreed upon duty to assist, attackers may be deterred from trying in the first place.

As stated previously, the study intends to argue for the importance of international law in addressing future responses to cyberwar. Theoretically, this line of reasoning would incorporate liberal ideals. Cooperation, rather than direct competition or confrontation as seen from the perspective of the realist camp, would be the protocol used to respond to the issue of cyberwar. However, it should be noted that states do indeed participate in an anarchical arrangement. Still, this arrangement also includes the fact that states recognize their shared interests in many areas to promote cooperation, or at least follow a set of norms that maintains peaceful patterns of behavior.

In response to the background noted above, an English School perspective will be used in this line of inquiry. The English School stresses the idea of an international society as the object of analysis (Linklater, 2009). Scholars such as Hedley Bull, Martin Wight and more recently, Nicholas Wheeler and Barry Buzan are seen as influential English School thinkers. The English School could be best understood as a middle-ground between liberalism and realism. On one hand, the English School sees the international system as more civil than realists care to acknowledge. Conversely, the English School sees that conflict can and does occur in an international society, "at odds with utopians who believe in the possibility of perpetual peace" (Linklater, 2009). Indeed, "For Martin Wight, the theory of international society represents an alternative to realism and idealism in the study of international relations" (Griffiths, Roach and Solomon, 2009). To argue further, "Bull claims that the 'institutions' of the society of states (war, great powers, maneuvers, international law, diplomacy and the balance of power) are crucial in maintaining international order" (Griffiths, Roach and Solomon, 2009). International law aims to perpetuate orderly international relationships in an effort to create a foundation based on customary norms of behavior. This would help limit the potential for escalating tensions among states.

Nations that find that their interests do not align with a peaceful course of action or do not wish to cooperate or dialogue, may flout norms set forth among states in an international society. That would indeed fall within the theorization of an anarchical system. It could be argued that a recent proclaimed unilateral response on the part of the United States in response to an attack on its informational infrastructure would qualify as a response that the realist would certainly see as rational. However, the intention of this research is to demonstrate potential agreement and consensus, and argue that the international community must acquiesce to dialogue and cooperation in this instance.

Chapter Two:

Realism, Liberalism and the English School: Competing Perspectives on International Law

Realism and liberalism, two of the great tenets of International Relations scholarship, resonate from opposite ends of the IR field. On one hand, realism places emphasis on the anarchical affairs of states, in that there is no power that oversees states in their quests for what is in their self-interests. As a result, a self-help system permeates the international climate. Conversely, liberalism highlights progressiveness and cooperation among states, rather than competition. With this understanding, how do the competing sides see international law? How do the perspectives see international law with respect to states in a cyber-world?

Realism

Realism and its more recent iteration, neo-realism, counts among its advocates Thomas Hobbes, Niccolo Machiavelli, Hans Morgenthau, and Kenneth Waltz. These visionaries of Real Politik claimed that the world is governed not by some international authority, but by power and the continuous struggle to attain it. The solitary end lies in securing one's self-interest. In this case, the "one" is the State, and the State is the highest authority among many competing authorities. Realists agree that the product of such an arrangement is anarchy. This conception of anarchy is not to be confused with utter chaos, but is simply a situation without any single entity having absolute authority over a plethora of agents (states). In addition to this lack of governable authority over states, realism claims that the previously mentioned aspect of self-interest is what drives states towards their ends. In being selfish, a state looks out for itself, and as Waltz suggests, "puts itself in a position to be able to take care of itself since no one else can be counted on to do so" (Waltz, 1979). It has also been argued that morality itself is not to be an aim of the state. By extension, states should also not be measured in terms of their morality. Morgenthau declares, "The actions of states are determined not by moral principles and legal commitments but by considerations of interest and power" (Morgenthau, 1970).

Where does this leave the realist perspective as it relates to the concept of international law, and more specifically cyberwar under an international normative regime? Waltz and Morgenthau clearly argue on behalf of a perspective that does not sympathize with pursuing moral objectives as an end in themselves. Russell notes, "Unlike the solitary individual who may claim the right to judge political action by universal ethical guidelines, the statesman will always make his decision on the basis of the state's interest" (as cited in Donnelly, 2000). Further, Schwarzenberger emphasizes that international morality, like international law, "is both subservient to power politics and…flourishes best where it does not interfere with the international struggle for power" (as cited in Donnelly, 2000). Carr argues that, "no ethical standards are applicable to relations between states" (as cited in Donnelly, 2000). Morgenthau agrees, "…universal moral principles cannot be applied to the actions of states" (as cited in Donnelly, 2000). Under these pretenses, it would be short-sighted to ask one of the realist perspective to even consider following normative rules, unless those rules align with their perceived self-interest. Rules are not in the best interests of a state that can otherwise exercise power to achieve its aims. As it relates to cyber-warfare, any international convention limiting or prohibiting such cyber activities on the part of a state could possibly be seen as inconsequential and therefore illogical to follow. Other enlightened realists could argue that it may be in the best interests of the state to enter into international agreements on cyber-warfare. States operating under the realist perspective would follow what is in their best interests and circumvent or follow any international agreements, if they deem that to be the course of action to take.

Conversely, Carr argues, "it is an unreal kind of realism which ignores the element of morality in any world order" (as cited in Donnelly, 2000). Also, "…the rules of international law constitute treaties, which by making possible the creation of international obligations respond to one of the most serious deficiencies of Hobbesian anarchy…and regulative institutions of various sorts can substantially alter the interactions of even powerful states." (Donnelly, 2000)

This particular statement questions a great assumption found in realism: that the international landscape is one made up of an anarchical arrangement with no oversight over the states involved. The constraints and obligations found within an international society such as those of treaties found in international law indicate that there are behaviors that states are willing to agree on. Treaties may help inhibit powerful states from acting in a manner that is unacceptable to other parties under the agreement. Such inhibition hardly lines up with an entirely anarchical arrangement.

Liberalism

Another great pillar of International Relations theory is liberalism, which "emphasizes individual rights, constitutionalism, democracy and limitations on the powers of the state" (Burchill, 2009). Liberalism includes such supporters as Karl Deutsch, Francis Fukuyama, Robert Keohane, and Michael Doyle. Contrary to the outside-in approach of realism, Fukuyama argues for an inside-out approach. Fukuyama notes that domestic, internal political orders with liberal-democratic ideals are seen as the vehicle to end international conflict (Burchill, 2009). Indeed, liberalism finds the liberal-democratic world to be in a zone of peace, rather than conflict. Fukuyama claims, "a world made up of liberal democracies…should have much less incentive for war, since all nations would reciprocally recognize one another's legitimacy" (Fukuyama, 1992).

Liberalism does not acknowledge the concept of a "zero-sum" game in the way realism does. Herz states that, "the mitigation, channeling, balancing, or control of power has prevailed perhaps more often than the inevitability of power politics would leave one to believe" (as cited in Donnelly, 2000). Burchill elaborates: "Mutual benefits arising out of cooperation are possible because states are not always preoccupied with relative gains – hence the opportunities for constructing regimes around issues and areas of common concern" (Burchill, 2009). Keohane and Nye also note that states, as members of international institutions can broaden their conception of their self-interests to better cultivate potential cooperation. Further, Keohane and Nye argue that fulfilling obligations of these international organizations can limit the pursuits of national interest, thereby subverting the "meaning and appeal of state sovereignty" (as cited in Burchill, 2009).

The defenders of the liberal mindset are also met with challenges. Globalization offers a great example of such a challenge. Hobsbawm claims that three areas of state authority have been limited by globalization: state monopolies of coercion by force, loyalty to the state from its citizens and finally, government capacity to supply public services due to liberal market forces. Overall, Hobsbawm notes: "The state as an essential unit of liberal democracy is weakening while public antipathy to globalization grows" (as cited in Burchill, 2009).

Where does this leave the liberal perspective as it relates to cyberwar under the auspices of international law? Is the weakening of state interference in the face of market liberalization necessarily a good thing, as lobbied for by liberalism? Can the market be relied upon for solutions to international problems? One could argue that liberalism does not offer an effective alternative to realism, because state authority has been weakened through globalization. This weakness perpetuates challenges to state sovereignty, and thereby participation under an international law paradigm. Some may defend liberal internationalism in its advocacy for democracy, free trade and essential human rights.

Realists could counter the weakening of state sovereignty as argued by Keohane and Nye with the important observation that only states may act as agents which may influence international law. The state, as an agent under the scope of international law, is subjugated to a multiplicity of globalizing forces outside its control. Nevertheless, while these external forces threaten its sovereignty, the state still has not had any serious competitor to its status as the primary unit of analysis. International law is in place to afford states a framework for the stability of relations amongst one another. Cooperation, as a noted cornerstone to the liberalist mindset, undermines any need for such a framework to even exist. Therefore, this framework of stability indicates that cooperation is not enough to allow states to peacefully concur on issues of pivotal importance. Indeed, cooperative initiatives have been constructed, such as The Budapest Convention on Cybercrime among others. However, the central idea in this thesis calling for international law to bring consensus on the issue of cyber-warfare supports the notion that minimal efforts at cooperation and unregulated market liberalization alone do not offer sufficient solutions to this global phenomenon.

This chapter has briefly described both realist and liberal perspectives, and the polarized nature of their positions as two of the great creeds of International Relations scholarship. With the understanding noted earlier, the competing sides see international law with respect to states in a cyber-world in very different views. Realism does not sympathize with a system of normative rules and customs by which states are to be bound. The idea directly contrasts with the self-help system that realism extols. Liberalism takes the opposite approach, in that international institutions may offer an arrangement where international obligations offer great opportunity for cooperation, but at the cost of potentially subverting national sovereignty. Market liberalization could weaken the state's ability to act as an authority, particularly when market forces undermine state ability to provide services to citizens that may already have shaky loyalty. In a liberal world of blurring borders, power becomes less tangible, whereas realism has been much more assured in where power rests. It has also already been noted that institutions such as international law and the United Nations only recognize states as agents, thereby reasserting the importance of the state.

With these ideas in mind, another hybrid perspective is available which offers the understanding of an anarchical arrangement of states and power seen in realism, merged with a greater perceived propensity for normative behavior and cooperation among nations found in liberalism, without challenging state sovereignty. The expectation from an international community of states of its individual members allows for customs to emerge, which is a main facet to international law. International law creates an environment where states are expected to act in a manner consistent with rules agreed upon by its members. Such an international society made up of sovereign entities is the foundation for the English School theory of international relations.

The English School

The English School offers a perspective that may be seen as a "middle ground" to those competing ideals of the realist and liberal camps. The term *via media* is frequently utilized in English School theory, referring to this "middle ground." Indeed, one could see the English School as the proverbial synthesis to realism's thesis and liberalism's antithesis. Linklater summarizes the English School: "The foundational claim of the English School is that sovereign states form a society, but an anarchic one since they do not have to submit to a higher power…members of the English School are attracted by elements of realism and idealism, yet gravitate towards the middle ground, never wholly reconciling themselves to either point of view" (Linklater, 2009). The English School emphasizes the lack of an overarching government in the international society.

In essence, the English School argues that the international system is more civil than realists would care to admit.

Bull claims such sociability among nations exists, "through their sense of shared interests and values, through their obedience to rules of international law, and through their participation in international institutions to regulate the conduct of international actors" (as cited in Keene, 2009). By extension, they find the notion of perpetual peace utopian and naïve. Principally, the English School and its proponents look to better understand the, "processes that transform systems of states into societies of states and in the norms and institutions that prevent the collapse of civility and the emergence of unbridled power" (Linklater, 2009). Linklater's point with respect to "unbridled power" as it relates to the English School's attempts to mitigate it within a society of states is important. The English School challenges the tenet of power found in realism, such as Muir's previous assertion of unilateral action on the part of the United States to achieve what he believes an international convention cannot. However, it is also important to note that the state is still the primary actor in an international society of states, and therefore challenges the liberalist perspective.

Wight alludes to the "Grotian Tradition" (as cited in Linklater, 2009), where the English School can trace its beginnings. During a time of conflict between Catholics and Protestants, Hugo Grotius imagined an international society which would promote coexistence. In fact, Wight himself "lamented the way in which debates between realism and utopianism…had neglected the *via media* with its distinctive focus on international society" (Linklater, 2009). Bull concurs with respect to the importance of an international society, stating that it was up to, "intelligent and sensitive persons" to take visions of "a world society or community" seriously (as cited in Linklater, 2009). One of the visionaries of the English School, Hedley Bull has been a proponent of the international society found in an otherwise anarchical environment. After all, anarchy is, "what states make of it" (Wendt, 1992).

Wilson notes that, "One of the defining features of the English School is the emphasis it places on normative rules, and in particular the rules of international law" (Wilson, 2009). Wilson also cites James: "For members of the English School, international law 'stands at the very centre of the international society's normative framework'" (as cited in Wilson, 2009). The contrast to the realist perspective is distinguished: "…it should be seen as a body of rules, deemed by those to whom it applies as binding, the purpose of which is to facilitate regular, continuous, and generally orderly international relationships" (Wilson, 2009). Wilson is explaining the emphasis placed on an international society by English School scholars, and that normative rules govern behavior of states. Inferred is the need for these rules to govern behaviors of otherwise competitive states in an anarchical arrangement. The English School understands the anarchical arrangement and attempts to create an environment where states are recognized as individuals with notable positions on issues. By granting a voice to each member of the community, and with each voice equal in weight, states may better understand what is acceptable versus not acceptable. States are also made aware of possible responses to activities based on customary practices. Adding such expectations to the proceedings, "helps reduce the degree of unpredictability in international affairs…Sense can thus only be made of international law by making sense of international society" (Wilson, 2009). Mayall agrees regarding international law, noting it is "the bedrock institution on which the idea of international society stands or fall" (Mayall, 2000).

English School scholars are at odds with realists and neo-realists with respect to the question of legitimacy. This is due to realism's lack of emphasis on the difficulties of legitimacy internal to the state as well as the international legitimacy among nations. Bull argued that safeguarding national sovereignty would allow nations comfort in the notion that they may promote whichever internal policies they wish, while still being recognized as legitimate in the eyes of other states (Linklater, 2009). On the other hand, the question of order versus justice is of high concern in the English School, and it leaves the theory with a quandary. The international order of things is agreeable among nations, as the question of sovereignty has been effectively assuaged, but the sense of justice is in the eyes of the beholder.

This wavering idea of justice can be explained by the example of human rights, and its somewhat metamorphic definition which is dependent upon whom you ask. Bull argues that, "the long-term trend over recent decades has favoured the introduction of solidarist measures to promote the international protection of human rights (as cited in Linklater, 2009). When Bull refers to "solidarist" measures, he denotes the rights of the individual and calling for greater cooperation and consensus of a greater range of issues among states more consistent with the liberal perspective. In contrast and sympathetic to realism, pluralism refers to the above discussed question of sovereignty and the lack of intervention and cooperation on the part of the international society members. This does not necessarily lessen the importance of sovereignty however, though members are to mutually recognize each other as equals: a precondition for international law. In the case of human rights, the solidarist perspective, as argued by Vincent can qualify the basic fundamental human right to be free from starvation. While extreme differences over negative versus positive human rights claims may exist, almost all can agree that global attention to malnutrition can lead to action among all of humanity (as cited in Linklater, 2009). The question of order (most often a Western ideal) and justice (non-Western in general) can become moot, as solidarity on issues such as Human Rights becomes the norm. By extension, international law can be the vehicle used to create consensus on such important matters, as exhibited by the International Declaration of Human Rights.

As discussed above, the English School offers a perspective that harnesses the ideals of an international society of states, including a perpetuation of international law which governs state behavior. An order emerges, and norms are found to mitigate international capriciousness. While such fickle behavior among states is simply lessened and not entirely eliminated, international law serves to enhance the order among states and to an extent, impart a sense of justice among members. International law brings legitimacy to nations who contribute to order amongst the anarchy. Against the backdrop of international cooperation with the question of state interests included amongst the dynamic world of international relations, international law indeed offers consensus as to how states ought to behave. It is in this environment, where international consensus on important matters has been observed. Examples such as the International Declaration of Human Rights and the Convention on the Prevention and Punishment of the Crime of Genocide, among others are noted in this regard. With this foundation for international law in place, the question of cyber-warfare can be better evaluated as to whether it is even reasonable to consider the issue relevant to international relations and international law.

Chapter Three:

Classifying Cyber-Attacks

Shifting in direction from the theoretical line of inquiry, it is now important to describe cyber-attacks. Later in this work, I will show what a cyber-attack is capable of in recent case studies. The present question is how can such activity accomplish such grand ends? What kinds of cyber-attack exist today, and what do they look to achieve? While entire volumes of intellectual findings are available on this topic alone, I look to very briefly explain cyber-attack methods used today in order to garner a general level of understanding. This helps the reader to better grasp the threats involved in this area as well as create a foundation for inquiry.

Defining Cyberwar

Some confusion exists in defining cyberwar. Azarov and Dodonov state that, "…in spite of the fact that terms information war, netwar, and cyberwar have distinctions in problem areas, all of them are frequently used in parallel with the purpose of adaptation in mass consciousness of various social layers – from government officials to the general public" (Azarov and Dodonov, 2006). In short, the interchanging usage of these terms exists so that general audiences may garner a familiarity with the issues inherent to the discussion. As mentioned previously, for the purposes of this thesis, former Special Advisor on Cyber-security under President G.W. Bush, Richard A. Clarke defines cyberwar as, "…actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke and Knake, 2010). The method of the attack, an example of which is the Distributed Denial of Service (DDoS) designed to disrupt operations on a grand scale, is simply the means of the attack. To clarify types of cyber-attack, it is important to understand the scale of these attacks, and what objective is to be attained.

Arquilla and Ronfeldt mention, "…when we think about 'cyber', we need to reflect on the Greek root – 'kybernan', which means to control or to govern" (Arquilla and Ronfeldt, 1997). Therefore, a cyber-attack is an attack meant to control or govern. This surmises that the end result is not necessarily to destroy. Azarov and Dodonov agree: "…the purpose of cyberwar is not destruction but control interception of information resources, systems and channels, which can be formally expressed as a process of changing of adversary control vectors according to the attacker's reference vectors…the modern information systems in cyberspace will be attacked with purposes not only for the destruction of information in the adversary information infrastructure but also for the control interception" (Azarov and Dodonov, 2006).

For further description, Azarov and Dodonov note that the Department of Defense has defined an information system as, "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information." More recently, Joint Publication 1-02 defines this term as 'the organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual" (Azarov and Dodonov, 2006).

To summarize the initial description of a cyber-attack in more conventional terms, a cyber-attack is an attempt to acquire control or govern information systems. These information systems act upon information in such a manner as to make it accessible, such as with power grids and other end products of that information. To control or govern the information not only affects the security of the information, but what can be accomplished with that information. Systems that could come under cyber-attack include electrical and telecommunications infrastructure or automatons, traffic and air control systems, nuclear power, defense systems, private information systems, and so on.

Cyber-attacks are capable of a wide range of ends. At times, the endeavor is simply espionage, such as the Flame cyber-attack discovered in 2012 in Iran, to be discussed later in Chapter Four. At other times the goal is governing the accessibility to that information or controlling or disrupting entire systems as in Estonia in 2007 and Georgia in 2008. Other invasions may look to undermine information in an effort to sabotage or even to perhaps destroy not only information, but the application of information manifested in physical, "real-world" systems. The Stuxnet infiltration in 2010 was an example of a cyber-attack that destroyed physical assets in Iran used to enrich Uranium, tied directly to the nuclear facility at Natanz. This example will also be analyzed in Chapter Four.

Types of Cyber-Attack

Many types of cyber-attack are at the disposal of the cyber-warrior. Therefore, a valuable effort in the analysis of cyberwar should include a general account of the options available in their arsenal. A brief description of notable forms of cyber-attack follows to grant the reader a foundation for further exploration of the matter.

Botnets. The botnet form of cyber-attack comes from the comingling of the term, "robot network". A botnet is defined as, "[a] network of Internet-connected end-user computing devices infected with bot malware, which are remotely controlled by third parties for nefarious purposes. A botnet is under the control of a given "botherder" or "botmaster." A botnet might have just a handful of botted hosts, or millions" (U.S. Federal Communications Commission, 2012). Botnets can be used in a large-scale operation in the sense that an attacking entity can conscript a multitude of computers without the typical user having any knowledge of their computer's supplementary cause or even of its subversion. Botnets can use their unwitting mediums to supervise the dissemination of Distributed Denial of Service attacks (DDoS), which I will cover shortly, acquire sensitive information from those participating computers as well as multiply itself amongst other unprotected computers. During the cyber-attack that afflicted the nation of Georgia in 2008 (described in the next chapter), botnets were used to bolster the scope of the Distributed Denial of Service attacks which crippled government websites and other information outlets.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Denial of Service (DoS) attacks refer to, "[t]he prevention of authorized access to resources or the delaying of time-critical operations" (U.S. Department of Commerce, National Institute of Standards and Technology, 2004). By using up all the resources available for the network, system or applications in question, the attacker can limit or even prohibit the usage of the above, effectively bringing operations to a standstill until resolved. Distributed Denial of Service (DDoS) attacks are simply DoS attacks, but on a grand scale with the usage of botnets or worms (which will also be discussed shortly). DDoS is the preferred vehicle among attackers because of its sheer scope which allows for the opportunity to bring down an entire network or website by flooding the target system with an overwhelming amount of incoming network traffic (IT Law Wiki, 2012).

In addition, although the attack can be traced to a multitude of sources across many countries, most are unwitting agents who are unaware that they are involved. This allows for plausible deniability. An applicable example of use of DoS or DDoS is the Denial of Service attack brought down Kyrgyzstan's main internet servers and email capability on January 18, 2009. Coincidentally, this occurred the same day as Russian public pressure on Kyrgyzstan to stop U.S. use of an airbase, located at Bishkek (Ashmore, 2009). The DDoS was traced back to Russia, but this does not necessarily mean that this is Russian interference.

Logic Bombs. Logic Bombs are, "…in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs…" (U.S. General Accounting Office, 2004). If an event occurs which prompts the malicious computer code to commence, the immediate results are realized in the form of data being compromised. Usually, a Logic Bomb is used to destroy data or at least render the data meaningless or unusable. An attacker wanting to "cover his tracks' could use a Logic Bomb to undermine the implicating data elements through this scrambling or destruction of the evidence. Logic Bombs can sometimes even be used to render hardware inoperable thereby compromising the attached elements of a system. On a small scale, this type of attack could be used by a disgruntled employee to erase data used on company servers. In a more relevant example, China could implant Logic Bombs on the military informational infrastructure used by the United States, which would cripple American capabilities militarily during a conflict (Clarke and Knake, 2010).

Trojan Horses. A relative of the Logic Bomb, the Trojan horse cyber-attack is a, "computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute" (U.S. General Accounting Office, 2004). Once the Trojan has been executed, its ulterior motive is revealed, which was built by the attacker. Indeed, in the realm of cyber-attack it is equivalent to self-sabotage. Many times, Trojan horses are opportunities for attackers to gain "back door" access not previously available to a system via an authorized user.

Using the previous example of Chinese asymmetrical warfare using cyber-attacks can explain the use of a Trojan. Modernizing a network with greater safeguards, such as the use of a more robust Intrusion Detection and Protection System (IDPS) is common for security experts to block incoming attacks. However, if a Trojan were to get onto the system prior to the installation of an IPS, it may appear as an authorized entry. Thus, a back door has been planted; an access point where infiltrators may plant such things as Logic Bombs, circumventing the protections is now in place.

Viruses. Viruses are similar to Trojan horses in their malicious intent, but are actually applications themselves. In addition, viruses can propagate with inadvertent (or advertent) human action, such as opening emails that include the virus or sharing infected files. To elaborate, a virus is "a program that 'infects' computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the 'infected' file is loaded into memory, allowing the virus to infect other files" (U.S. General Accounting Office, 2004).

The application of viruses can range anywhere from simple day-to-day computer operations (the ILOVEYOU virus in 2000), to the use on nation-states.

They can also range in their intentions from destruction to espionage. The “Flame” virus that will be analyzed later was used as an espionage tool in Iran. Inadvertent usage of infected files allowed the virus to spread, allowing for the designers of the virus access to information located on Iranian networks as well as the networks themselves.

Worms. Worms denote an, “independent computer program that reproduces by copying itself from one system to another across a network” (U.S. General Accounting Office, 2004). The main difference between worms and viruses are worms’ capability to self-propagate. Generally, worms are used to drain resources on network systems, create “back door” accessibility, perform DDoS attacks, and other various aims. While the self-propagation capability sounds ominous, this is indeed limited to network connectivity. Therefore, localization through disconnection from any network concentrates the worm to a location, unable to spread.

Containment is attainable, but if a worm is not known to exist, it is free to propagate at will. The example of “Stuxnet” (noted later) is a very appropriate explanation of what a worm is capable of. The use of Stuxnet spread beyond its intended scope by its designers. However, its initial use was to establish control within a system, allowing a different set of parameters to be followed based on what the worm designers had established. Once the worm had spread beyond its initial scope, the requirements imbedded in the worm code were not met, and therefore, the control interception beyond the initial scope was rendered largely harmless.

Examples of Cyber-Attack Usage

Cyber-attacks made up of the preceding methods are capable of a wide-range of control. Clarke and Knake utilize clever anecdotes to grant the reader an example of what such control can achieve. Details are sketchy on exactly what kinds of cyber-attacks were used and when these events occurred, but that does not lessen their practical importance, particularly given that the examples come from the former Special Advisor on Cyber-security under President George W. Bush (Clarke and Knake, 2010).

Looking back at the Second War in Iraq, Clarke and Knake describe the situation in Iraq prior to the conventional attack, where the United States had infiltrated the supposedly "closed-loop" military network. A "closed loop" network refers to a network that operates disconnected from outside influences could invade the information system.

Many Iraqi military officers had received emails of the sort that advised them of a course of action (most notably, do not participate and you will be reconstituted once the regime has been replaced). The emails intimated that these actions that would supposedly save them from the impending American onslaught (Clarke and Knake, 2010). The authors can speculate on what was actually in the emails, but the tool of information in the cyber-warrior's hands and the opportunity to disseminate that information as one chooses can be a powerful combination to face.

Another example Clarke and Knake cite is the event where Israel had "owned" the air-defense network of Syria, and attacked one of their nuclear facilities. In essence, the Israelis utilized a pseudo-cloaking device, replacing the air defense signals that Syria should have noticed (incoming Israeli planes), with a signal of silence (meant to signify peaceful skies to the observers) (Clarke and Knake, 2010). Through the undermining of the air defense information system Syria could have used to monitor their airspace and protect their closely guarded nuclear facility, Israel was able to violate Syrian airspace, and knock out what Israel perceived to be a potential threat.

A military incursion of another nation's air space could be construed as a violation of the sovereignty of that state, and a pretext to war. However, without evidence to support the assertion of an invasion on the part of Israel, save for perhaps obvious motives, denial on the part of Israel is all that would be needed to avert a local or regional crisis. After all, the intrusion was not even caught by Syria's first-alert air defense systems, and could have been interpreted as an accident at the site itself. Other reasons for Syria's silence on the matter may also exist, but without evidence, confirmation of the identity of Israeli military craft in Syrian airspace was unavailable.

These scenarios are not the product of an overactive imagination. These are real-world applications of where the commandeering of a nation's information system, in these cases military and defense related, and the scope of such intrusion is not left to simply military application. Civilian entities are also potential targets of cyber-attack, such as the informational or resource infrastructure within a state. Infiltration of a networked power grid could cripple a state financially and logistically if sabotage of the system were to be controlled, or worse, brought down. Schmitt states, "…because of the potentially grave impact of CNA on a state's infrastructure, it can prove a high gain, low risk option for a state outclassed militarily or economically (Schmitt, 1999).   It is therefore important to analyze historical examples of such cyber-attacks on nations.

Chapter Four:

Case Studies

With the relative youth of the practice of cyberwar, case studies are difficult to establish. The lack of concrete examples in which nations have participated in cyber-attacks on another nation exacerbates this task. This difficulty is augmented by the challenge of attributing cyber-attacks to a particular state. Inevitably, hacking agents and "cyber-warriors" utilize various tools to mask their identities as well as insulate themselves from their sponsors. Attempts to link the origination of cyber-attacks to the main force behind the attack are sometimes an almost insurmountable job. However, some incidents have been noted that have directly affected state operations. With a basic understanding of what cyber-attacks are available in the cyber-warrior's arsenal, we can examine cases that better help us understand what occurred.

These case studies are described in order to better equip the reader with a sense of the practical importance of cyberwar against states. I analyze recent cyber-attacks on states, all within the last five years. In these cases, I look for suspicion of state involvement in the attack, and if that suspicion became more substantial based on findings. In essence, these examples were chosen for analysis because of their potential for implicating nation-states. I also look to understand the intended effects of the cyber-attack, and who or what those effects were meant to target.

As mentioned previously, the following case studies will be covered briefly: the Estonian Cyber-Attack of 2007 and the Georgian Cyber-Attack of 2008 during their conflict with Russia. Also, the Stuxnet worm of 2009 and the Flame virus that was uncovered in 2012 involving Iran and its nuclear centrifuges at the Natanz complex will merit attention.

Estonian Cyber-Attack of 2007

The cyber-attack that afflicted the tiny nation of Estonia in 2007 is widely regarded as the world's first cyber-attack that left the national security of a state in the balance (Beidleman, 2011). According to Beidleman, "botnets…seized more than a million computers from 75 countries and directed them to barrage targets in Estonia" (Beidleman, 2011). The botnets utilized distributed denial of service attacks to flood information requests onto websites associated with the government, the banking sector and other important essentials of Estonian life. Such devastating information overload delivered by the distributed denial of service attacks crippled all Estonian informational infrastructure elements that were associated with everyday use of internet. Automated Teller Machines (ATMs) no longer dispensed currency. Vandalism of websites also occurred. The news media was incapable of offering citizens any updates.

Ashmore notes that the Estonians were able to respond effectively, limiting the effects to short-term outages. Further, there were no permanent damages inflicted to the informational infrastructure (Ashmore, 2009). Estonia successfully employed its Computer Emergency Response Team (CERT) and comingled efforts between government and civilian experts mitigated the potential for disaster. Alexander Ntok, head of Corporate Strategy at the International Telecommunication Union (ITU) lauds the Estonian responses and recovery efforts: "it was imaginative responses that allowed Estonia to emerge from the spring cyber-attack relatively unscathed" (as cited in Ashmore, 2009). In fact, Ashmore finds Estonia in a leadership role as it pertains to NATO Information Technology structural defense. Estonia has also provided expert personnel to staff the NATO Cyber Defence Centre in Tallinn upon its opening in May 2008 (as cited in Ashmore, 2009).

Estonia also has looked to bolster the international legal agenda to enhance laws to protect Information Technology infrastructures. According to the Estonian Ministry of Defense, Estonia has worked to increase international cooperation to protect global systems (as cited in Ashmore, 2009). In addition, during Estonia's response to the attack, the CERT for Estonia issued an international appeal for assistance among specialists and firms from around the world (Jenik, 2009).

While Estonia's response to an otherwise ground-breaking problem in state security has been extoled, the questions arise: why was the response necessary and who was answerable to the breach?

Many have speculated that because of the identification of Russian internet protocol (IP) addresses used in the attack, the culpability lies with Russia. Further, tensions at that time between ethnic Russians living in Estonia and the nation itself were peaking due to Estonian aims to move a statue in place to celebrate Soviet casualties during World War II. Russians have celebrated victory in World War II on May 9, and according to the Permanent Under-Secretary of State for the Estonian Ministry of Defence, Lauri Almann, "The idea was to have a huge gathering on 9 May that was combined with a huge cyber-attack" (Mansfield-Devine, 2012). Paramilitary groups, such as the Russian Business Network have been found to be involved in the cyber-attack (as well as in the Georgian cyber-attack in 2008). Gervais finds that, "the relationship between the Russian Business Network and the Russian State should be sufficient to impute state responsibility" (Gervais, 2012). In addition, the Russian government offered no cooperation in tracking down the botnets and their origination and Estonian requests for bilateral investigation under the Mutual Legal Assistance Treaty (MLAT) were denied by Russia (Shackelford, 2009).

Even with the smoking gun and a potential motive available, the extent of Russian guilt in this instance has not been ascertained. However, other cyber-attacks in former Soviet satellites have occurred in Lithuania, Kyrgyzstan and Georgia (to be discussed shortly). In these cases, allegations of Russian involvement have been voluble (Ashmore, 2009).

Georgian Cyber-Attack of 2008

Georgia was also a nation subjected to the aims of a cyber-attack. However, different from the Estonian example, this attack coincided with the Russian invasion of South Ossetia in August of 2008. According to Milikishvili, this was the first time that a cyber-attack accompanied armed conflict (as cited in Ashmore, 2009). A denial of service attack claimed the website of the Georgian president as well as other government sites (Ashmore, 2009). Defacement of websites (including adding images of Adolf Hitler to web pages associated with the Georgian president Mikheil Saakashvili) also occurred (as cited in Ashmore, 2009).

In the case of Georgia's informational infrastructure, its international connectivity was far more limited than Estonia's. Also, most international connectivity that was available was through Russian territory (Stapleton-Gray and Woodcock, 2011). Therefore, attempts to block outgoing messages including media reports were easier. Compared to Estonia's heavy reliance on Information Technology infrastructure and e-commerce, Georgia was not nearly as engaged.

Stapleton-Gray and Woodcock mention an interesting occurrence of outside entities "mirroring" Georgian web content in lieu of the cyber-attack. This mirroring is symbolic of external support from governments (Poland, e.g.) and corporations (Google, e.g.) sympathetic to the state's duress (Stapleton-Gray and Woodcock, 2011, Ashmore, 2009). Estonia sent Information Technology security specialists from its own CERT to assist in combating the cyber-attacks (Ashmore, 2009).

As with Estonia, there was no direct linkage between Russian government involvement and the cyber-attacks. However, the cyber-attacks in Georgia and Estonia, (as well as other attacks in Kyrgyzstan and Lithuania not analyzed here) were initiated in response to hostility with Russia (as cited in Ashmore, 2009). Whether there was some level of Russian involvement or not, Ashmore asserts, "opposition to the Russian government could result in a cyber-attack which could disrupt critical government infrastructure" (Ashmore, 2009). It is important to note Shackelford's assertion, "states remain the focus of containing IW (information warfare) as the Estonia incident and the Russian-Georgian armed conflict reveal more and more of a cyber dimension to international conflicts (Shackelford, 2009). If this trend continues, as many believe it will, the implications of cyber-attacks among states will require closer examination.

Stuxnet

Shifting geographically from Eastern Europe to the Middle East we find more evidence of cyber-warfare among states, although the evidence was not nearly as clear initially. A worm, popularly known as "Stuxnet," had infiltrated the Iranian nuclear facility at Natanz. Stuxnet has been found to have infected over 60,000 computers, half of which were located in the Iranian state (Farwell and Rohozinski, 2011). While that leaves other infections outside Iran, including

India, China, the United States and Australia among others, Ralph Langner calls Stuxnet, "an all-out cyber strike against the Iranian nuclear program" (Langner, 2010).

Stuxnet was a worm designed to infiltrate and establish control, as well as change instructions in remote systems (Farwell and Rohozinski, 2011). A "zero-day attack," Stuxnet used a penetration technique never before seen, aiming to exploit a previously unknown weakness in software (Clarke and Knake, 2010). In fact, the authors Clarke and Knake claim that the cyber-attack was made up of four zero-day attack techniques, ostensibly in the event that a technique was ineffective, it could try the next.

The challenge for the Stuxnet worm was that according to Farwell and Rohozinski, the worm's target was actually not connected to any public infrastructure. Therefore, the infection would require the use of an external device, such as a USB memory stick. Upon infection, Stuxnet used Siemens' default passwords to find and acquire access to particular programs, called Programmable Logic Controllers (PLC) (McMillan, 2010). The PLCs at Natanz were made by an Iranian company called Fararo Paya (Clarke and Knake, 2010). This fact has important ramifications to be discussed later.

Also important are SCADA (Supervisory Control and Data Acquisition) systems. They are used to control large-scale industrial systems in factories, power plants, military installations and others (McMillan, 2010). To simplify, the SCADA system tells the machinery what to do and monitors its work. Stuxnet not only gained access, but it reprogrammed the SCADA systems. It then began to manipulate the cycle drive speeds within gas centrifuges at Natanz, resulting in rotor damage and in effect rendering the centrifuge useless (Langner, 2010). Clarke and Knake claim that almost 1,000 centrifuges at the Natanz site were removed as a result of the sabotage.

As mentioned earlier, the worm had spread beyond Iran, into other nations. This was not by design. The worm was designed to search for Siemens software running Fararo Paya PLCs (Clarke and Knake, 2010). However, the worm continued to look outside of this scope, for the Siemens software. If it did not locate the software and PLC recipe, it continued on, infecting other networks but remaining dormant. As a result, the worm was now out in the open, available for cyber-warriors and hackers around the world to analyze and break down its complex code. Since it was never meant to get into the open, it truly highlights the dangers of cyber operations.

Who would be potentially responsible for this cyber-attack? Clarke and Knake note, "In June 2009, four Iranian organizations were infected. None of the four were publicly known to be connected to Natanz, but the CIA or Mossad knew they were" (Clarke and Knake, 2010). This infers American and Israeli coordination, if not direct action. Kaspersky Lab researcher Roel Schouwenberg agrees that this cyber-attack was most likely the work of a nation-state (McMillan, 2010). Sanger claims that President Barack Obama looked to accelerate former President G.W. Bush's aims to expand the United States' use of cyber-weapons (Sanger, 2012). Sanger reports that interviews with current and former American, European and Israeli officials involved confirmed American and Israeli involvement. Allegations of American involvement in another cyber-attack in the Middle East will be covered in the next section on "Flame". Langner notes that the attack was very sophisticated, requiring perhaps several years of preparation. This level of complexity was not believed possible at the time, indicating professional handling. Considering the chilling alternative, Langner states, "let's just HOPE the US is the leading force behind Stuxnet" (Langner, 2010). What Langner implies, is that if this level of complexity was not generated by the United States, the alternative could be another nation-state, or possibly a private hacking entity.

Flame

The previous case studies have alluded to cyber-attack potential for control, disruption and destruction. However, these need not be the only capabilities for hacking into state resources. It might befit a nation-state to utilize cyber resources in ways that human intelligence may be unrealistic or unprofitable. A great example of this scenario would be the computer virus now known as "Flame."

Flame was not designed to be destructive. Rather, its primary function was espionage. Also known as Flamer and Skywiper, the primary infection was deemed to be in Iran, though other Middle East nations reported infection. Later, infections spread among other nations. Experts believe the possibility exists that travelers may have taken laptops abroad with the infection (Constantin, 2012). The computers affected belonged to individuals, as well as educational institutions and state-related organizations (Nakashima, 2012).

Compared to Stuxnet, researchers have deemed Flame to be related, though approximately twenty times the size of Stuxnet (Nakashima, 2012) and much more complex (Constantin, 2012). Written in a computer language called LUA due to its stability (which is uncommon for most malware attacks), Flame was designed to be hard to detect (Tsukayama, 2012). This insinuates that the designers wished it to remain in an espionage capacity. Indeed, the infection was only found two years after initial activation, after Iran's Oil Ministry discovered disruptions and investigated (Nakashima, Miller and Tate, 2012).

Schouwenberg notes that this is the first virus capable of using, "Bluetooth wireless technology to send and receive commands and data" (as cited in Nakashima, 2012). However, the primary method of infection was copying itself to portable USB devices and through printer vulnerabilities (Constantin, 2012). CrySys, a cryptography and security lab, claims that Flame was capable of, "logging keystrokes, activating microphones to record conversations and taking screenshots" (Nakashima, 2012). Alexander Gostev says, "Flame can easily be described as one of the most complex threats ever discovered" (Gostev, 2012).

Researchers later found that Flame had also exploited Microsoft Windows

Update on machines with Windows Operating Systems. The writers of Flame had somehow stolen digital signatures of code which allowed the malicious code to masquerade as code "approved by Microsoft." This means that the fully-patched machines were infected by supposedly legitimate code. This prompted Microsoft to issue an immediate fix just days after the initial reports of the cyber-attack, rather than wait for the designated patch date (Keizer, 2012).

Initially, attribution was again challenging. Gostev offers the following analysis: "there are three known classes of players who develop malware and spyware: hacktivists, cybercriminals and nation-states" (Gostev, 2012). Given the complexity, hacktivism is not the likely source. Further, the intention of Flame was not to steal money from bank accounts, mitigating the possibility of cybercriminal activity (Gostev, 2012). Finally, this complexity in addition to the geographic focus of the attack (Iran, but also including Palestinian areas of Israel, Sudan, Syria, among others) leaves the ostensible conclusion that Flame was a tool used by nation-state(s) (Gostev, 2012).

Indeed, Kaspersky labs later surmised that specific computer code was used in both Flame as well as the aforementioned Stuxnet. Gostev claims, "…conclusions point to the existence of two independent developer teams…" though, "part of the code from the Flame platform was used in Stuxnet" (Gostev, 2012). The findings indicate that while two teams may have been independent, some collaboration existed.

The Washington Post confirmed that the United States and Israel,

"…jointly developed a sophisticated computer virus nicknamed Flame" (Nakashima, Miller and Tate, 2012). Further, "the massive piece of malware secretly mapped and monitored Iran's computer networks, sending back a steady stream of intelligence to prepare for a cyber-warfare campaign" (Nakashima, Miller and Tate, 2012). Based on this finding, it is reasonable to assume that Flame actually predated Stuxnet. According to Schouwenberg, Flame allowed for Stuxnet to sabotage Natanz based on Flame's findings regarding networks associated with the nuclear facilities (Nakashima, Miller and Tate, 2012). What began as an espionage operation led to an intricate first-strike on Iranian nuclear capability.

Evaluation of Cases

The cases highlight some basic aims of cyber-attacks: control, disruption, destruction and espionage. All of the cases implicated nation-states, but it is important to note that none of the cases were definitive in attributing the cyber-attack to the suspected nation-state. Both the Estonian and Georgian cases include suspected Russian involvement or at least Russian support. In both cases where Iran was the target of cyber-attacks, suspicion falls on the United States and Israel, with some media "insiders" alleging confirmation of the states' involvement. While some government officials and media point fingers, the instigators of the cyber-attacks remain unidentified. This finding has repercussions for the question of attribution of cyber-attacks to be analyzed later in Chapter Five.

The other important issue evaluated in these cases was the question of intended effects, as well as which entity or entities were to be affected. In both the Estonian and Georgian cases, informational infrastructure was targeted. This left not only government but civilian entities in a debilitated state for long periods of time. In addition, the Georgian cyber-attack was accompanied by a military incursion into Georgian territory, raising suspicions that the two operations were related. The Iranian cyber-attacks were both directed towards facilities suspected of uranium enrichment; the end result of which may or may not have been for military purposes. The issues surrounding these cases raise questions of targeting combatants vs. non-combatants as well as directing attacks against dual-use entities, which I also assess in Chapter Five.

Chapter Five:

International Law and Its Applications to Cyberwar upon Nation-states

The dangers of cyberwar among states go beyond the daily inconvenience that the common individual experiences every day. Viruses, worms and the like have become so commonplace among computer users that most of the population is aware of the dangers. Most individuals have taken reasonable measures to defend their property and capital from outside attack. Informed users know that malware protection is available, and it is up to them to keep their protection updated to keep up with the latest infections. Malware protection software companies are also hard at work to keep up with the constant barrage of new malware as best as they can. Even with such effort, there are challenges. The common individual does not have much of a say in the national defenses of states. States must continue to protect their infrastructures as well as communicate with fellow states within the international community. Otherwise, domestic safeguards noted above are largely inadequate. States have a duty to protect and assist not only their own citizens but civilians everywhere. International norms and agreements must exist that unequivocally define cyber-attacks, related terms and the behaviors among states that are to become customary in a cyber world. I argue these norms should go beyond the current application of *jus in bello* and include international law governing cyberwar.

Comparison to Nuclear Weapons

Authors Damrosh, Henkin, Murphy and Smit describe international law as, "concerned with law that principally operates among sovereign countries (or 'states'), arising from sources such as treaties and the customary practice of states" (Damrosch, Henkin, Murphy and Smit, 2009). The authors note that, "traditionally, international law was seen as the law of the international community of states, the basic units in the world political system from the Peace of Westphalia (1648) forward" (Ibid, 2009). However, an important change occurred following the First World War. Malanczuk calls this "modern" international law, concerning itself with an, "attempt to organize the international community and to ban the use of force" (Malanczuk, 1997).

This ban on the use of force is found in Article 2(4) of the United Nations Charter. As a caveat, Article 51 provides for the right of states to collective and individual self-defense against armed attacks (United Nations, 1945). The UN Charter does not offer any guidance on the topic of cyberwar, however. This makes sense, since the original UN Charter was created in 1945, well before this issue came about. Swanson definitively declares, "Currently, there is no provision in international humanitarian law (IHL) or customary international law (CIL) that explicitly outlaws cyber-warfare or computer network attacks, either carried out independently or during times of war (Swanson, 2010). However, Swanson finds that international law has been capable of addressing warfare and its changing dynamics and capabilities. "The Geneva Conventions, as well as the international humanitarian law principles of proportionality and unnecessary suffering, all provide a legal framework for addressing cyber-warfare issues (Swanson, 2010).

It could be argued that cyber-weapons are similar to nuclear weapons. Their unique capabilities and characteristics call for unique laws (Swanson, 2010). Shackelford points out that the cyber-attacks on Estonia, "like nuclear warfare, do not discriminate between combatants and non-combatants, nor do they pass the test of proportionality" (Shackelford, 2009). The International Court of Justice (ICJ) ruled the threat or use of nuclear weapons, "would generally be contrary to the rules of international law applicable in armed conflict, and in particular the principles and rules of humanitarian law" (I.C.J., 1996). The potential for disastrous consequences in a nuclear attack can be matched in the case of an all-out attack using cyber-warfare. The example of a cyber-attack where critical infrastructures are destroyed or otherwise rendered useless can leave a state in a helpless position, causing unnecessary suffering to its citizens. If nuclear weapon use is subject to the rules of international humanitarian law, so too should cyber-attacks (Shackelford, 2009).

Nuclear capability among major powers redefined the context of warfare during the twentieth century. Once the world observed what nuclear weapons were capable of, it became evident that this technology was not to be taken lightly. I would argue the same could be said for the use of cyberwar continuing in the twenty-first century. Except in this case, nuclear weapons are not as readily available to the general population, whereas hacking capabilities can be learned by anyone with the desire and talent. Furthermore, the world has not yet seen the overwhelming potential of cyberwar on a grand scale, and therefore this may not be taken as seriously unless a catastrophic cyberwar-like event were to occur.

Shortcomings of Conventional *Jus In Bello* Application to Cyberwar

The Geneva Conventions place limits on conduct among war participants. *Jus in bello,* the law of war, stipulate restraints placed on the extent of harm to non-combatants. Non-combatants have not forfeited the same rights that soldiers have by entering military service. Distinction between civilians (and civilian entities) and combatants (and their entities) must exist. Therefore, military objectives should be the primary targets for an attack (U.N.T.S. Protocol additional to the Geneva Conventions of 12 August 1949, Additional Protocol I, 2009).

Protections afforded to civilians also encompass any objects that are indispensable to the civilian population. However, Hollis explains a challenge inherent within cyberwar: "The irony of information operations (IO) is that the less likely it is that a particular IO functions as an attack, the more likely it is that its use against civilians and their objects is permissible. In other words, IO's development may actually result in warfare having more impact on civilians by expanding militaries' ability to target (but not attack) them" (Hollis, 2007). During conflict, any force must be met with a proportionate response. For example, an attack by Nation A at a military base in Nation B does not in and of itself grant license to Nation B to use a cyber-attack to shut down an entire portion of the national electrical infrastructure in Nation A. Such an escalated response would inevitably affect multiple sectors, public and private, reliant on electrical systems, including economic sectors, health sectors and public safety. That violates not only the proportional aspect of current *jus in bello,* as well as the non-combatant protections afforded by the Geneva Conventions.

Indeed, another aspect of the law of war allows for the military targeting of "dual-use" entities. For example, civilians working at a military munitions factory are seen to be in a "dual-use" capacity. As such, this facility would qualify for military targeting. This possibility exists for virtually all computer networks. Hollis notes that as of 2000, 95% of U.S. military traffic went through civilian telecommunication and computer systems (Hollis, 2007). Under the "dual-use" rule, any adversary could potentially attack any communication system (if they are to be treated as military objectives), and they may be targeted either using cyber-warfare OR conventional means. Attempts to interfere with military or government communications via the informational infrastructure would also interfere with civilian use of the same infrastructure.

Indeed, Schaap argues, "Cyber-warfare operations…create more opportunities for targeting dual-use objects" (Schaap, 2009).

While the attempts to endorse a law of war have thus far been well-intended, it is clear that the usage of *jus in bello* to adequately cover the complex intricacies of cyberwar is simplistic and naïve. Complications arise from cyberwar and its humanitarian effects on the non-combatants of the targeted state. This issue raises difficult questions, and does not even begin to satisfy concerns regarding asymmetric uses of cyberwar between state and non-state actors or including non-international areas and territories. In short, current international law is insufficient to address all complexities and circumstances through which cyberwar may occur (Hollis, 2007).

The Challenge of Attribution

Shackelford claims that attribution of a cyber-attack to a state is the key element in building a functioning international regime (Shackelford, 2010). While some instances of government sponsored cyber-attack using transnational networks can be traced to a nation-state, more typically these attacks are not from official state action.

Two international standards exist that could offer guidance on the issue of attribution. First, the doctrine of effective control establishes the understanding of a state's control over paramilitary groups and other non-state actors if the actors act in "complete dependence" on that state (as cited in Shackelford, 2010). Conversely, the operational control doctrine, found that where the state has a role in coordinating on behalf of a particular group and offering support, there is enough overall control to attribute a group's actions to the supporting state (as cited in Shackelford, 2010).

While the International Court of Justice has more often utilized the first and more constricting interpretation, the doctrine of effective control, this may not be feasible in the present context of cyber-attack. Nations may easily hide behind the doctrine of effective control because of the challenges of attributing cyber-attacks to any nation-state. Complete government control will be difficult to establish in many cases. However, if the second, more liberal doctrine of operational control is used as the interpretation of cyber-attacks and their attribution, any nation that simply coordinated and supported an attack would be attributed. Using the Estonian case noted previously, the doctrine of operational control interpretation would surely find Russian involvement to be adequate to grant Estonia reparations (Shackelford, 2010).

The need for clarity on the question of attribution is of great importance, as it may take many years of practice for customary international law to become crystalized. However, even with a firmer establishment of attributive law, this does not rectify the overall issue. Today's sophisticated techniques allow for the hacker to remain anonymous if they have the skillset. Worse, they may implicate an otherwise innocent entity or nation-state. "If a cyber-attack disabled critical infrastructure, or killed enough people, the United States could treat it as an act of war—and respond with force by invoking the right of self-defense—without knowing for sure who launched the attack" (Hollis, 2011). Therefore, the most hardened of efforts to attribute cyber-attacks to any one perpetrator or perpetrators may end without success, or worse the false-positivity of success.

Future of Cyberwar Under Norms of Potential International Agreement

A future framework of norms that govern cyberwar must offer adequate guidance to what is arguably one of the most complex, misunderstood and potentially devastating issues the world faces today. This challenge to international security and peace is occurring at the present, and unfortunately the international community is just starting to grasp what the issue entails. In the fast-paced cyber-world, being reactive leaves one behind and vulnerable. A proactive approach is needed on cyberwar to allow nation-states and their domestic and international entities the opportunity to mitigate the potential threats that are intrinsic within the growing cyber-world. Clear delineations of norms must come to fruition, or risk confusion and potential chaos among states in responses to cyber-attack.

The complexities and pitfalls of cyberwar call for new international agreements on the matter. The current regimes that govern warfare will not suffice. The law of war was put in place to add a humanitarian element to warfare, but in cyberwar, the distinction between combatants and non-combatants is not as discernible. Non-combatants and the infrastructures that they use on a daily basis must be protected to avoid modern catastrophe.

Regional cooperatives have been created, such as the NATO Cyber Defence Centre in Tallinn. The, "NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) was formally established on the 14th of May, 2008, in order to enhance NATO's cyber defence capability. Located in Tallinn, Estonia, the Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Poland, Slovakia, Spain, the Netherlands and USA as Sponsoring Nations" (CCD DOE, 2012). Their mission is, "to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation" (CCD DOE, 2012). The centre, located in Estonia, where the cyber-attacks of 2007 occurred, is a reminder of what can be accomplished as lessons are learned from difficult circumstances. Unfortunately, it was these difficult circumstances that brought the issue to light. The international society of states must come to consensus on this matter, before such disruption occurs. After all, it may not be a nation behind such attacks. States wishing to protect themselves beyond their own cyber-protections domestically should also come together diplomatically on this critical issue. Perhaps an international regime similar to regional cooperatives such as the NATO Cooperative Cyber Defense Centre may be in order. "The fight against cyber-terrorism, computer hacking and economic cyber deception has to be rated as a common strategy for any national government in the Information Age and requires consecutive coordinated interaction between groups of national governments" (Azarov and Dodonov, 2006).

Actions on the part of the international community during the Georgian conflict as well as during the Estonian cyber-attack seem to indicate that sympathetic nations are willing to help in times of crisis. As noted previously, during the Estonian affair, a call for help from the Estonian CERT went out around the world. During the Georgian crisis, sympathetic nations and corporations came to Georgian aid, placing important information onto the internet in lieu of the fact that Georgia was unable to do so. In addition, during the cyber-attacks, Estonia had sent IT security specialists to aid in bringing Georgia back online. While customary international law may take time to develop, there has been a historical basis for assisting ailing units during times of dire need. In fact, there is international law already in place that requires assistance, if it has been reasonably requested by the party under duress and the ability to help exists. The United Nations Convention on the Law of the Sea may hold some analogous application to cyberwar.

Duty To Assist. Hollis points out the similarities between an SOS at sea and the characteristics of cyber-attacks: "Strikingly, the three elements giving rise to the SOS at sea – incapacity, severity and urgency – characterize cyberthreats as well" (Hollis, 2011). Challenging cyber-attacks can, "overwhelm the most sophisticated individuals, groups and even states" (Hollis, 2011). As seen in Estonia and Georgia, the state became incapacitated under duress until the situation came under control, and outside assistance surely had a hand in bringing the crises to their conclusion.

In terms of severity, Hollis argues that cyber-attacks have the potential for systemic concerns, rather than simply localized consequences. While economic effects may occur, the entire system may become erratic due to the inherent entwined nature of many systems. Aggregated effects are felt throughout the system, its users and potentially an entire nation. Indeed, infrastructures that affect resource distribution, such as water and power systems can have real consequences for life, beyond merely systems and economic factors.

The question of urgency should be addressed without doubt. Cyber threats can and do arise immediately. Sometimes, dormant threats exist, such as logic bombs infused within informational infrastructures. These potential crises are waiting for the "go ahead," and therefore can become urgent issues.

A duty to assist (DTA) paradigm should be incorporated into any international regime governing the use of cyber-attacks. The previous question of attribution becomes less prevalent under an international system where professionals come to the aid of those under duress. If norms existed that elevated the need to mitigate harm, rather than attribute blame through a collectively agreed upon duty to assist, attackers may be deterred from attempting attacks in the first place. This is particularly true if requests for assistance come to a state that must aid against their own attack. The cyber-attack on Estonia led them to request assistance from the Russian government to cut off DDoS attacks coming from its territory. In the case of the actual account, Russia said it was not responsible and remained unhelpful. However, under the DTA norm, Russia may not have the option of doing nothing, and might be obligated by the international norm to assist. Of course, states must agree which threats are to be covered, who can legally request assistance and expect it, who must provide the assistance and finally, what assistance must be granted (Hollis, 2011).

The agreement must include clearly defined protocols on this matter, but under the circumstances, nation-states have many reasons to agree on such an idea. Hollis argues that the Internet has become indispensable. A shared and vested interest in the Internet is realized, when one understands that everyone is at risk, but at the same time, everyone can help (Hollis, 2011). Individuals, who learn that they are part of a botnet without realizing it, can disconnect from it. In the cyber-world of extreme interconnectivity, every little effort helps, and many times with instant results. Individual states can rely on their fellow states to assist, as in the future, the reverse may be true and the latter may need assistance from the former.

This whole area raises a pivotal question: Should cyber-attacks be outlawed in all situations? This universal ideal may be misguided, as states will want to continue their tactics of cyber-espionage, and perhaps even cyber-warfare on military targets. However, any international norms governing cyber-attack must be clear in what cyber-attacks are allowed under some sort of cyber-

jus in bello standard that can be negotiated by states. Cyber threats that cause unnecessary human suffering must continue to be outlawed as seen from the perspective of international law.

While the international community may continue to operate under auspices of shared interests in many cases, there still is the understanding that international anarchy is still in place. States are individuals in an international society with equal stature and equal resonance of opinion but there still is the expectation that states may indeed flout decrees if they see it in their best interest. However, under a set of international norms that governs cyberwar, a nation that does not follow these norms would be a member that cannot be trusted, and may find themselves isolated. Even so, I assert states will, in many cases identify common ground and should come to agreement on this international space known as the Internet, if it is in their best interest. With most states using the same informational, interconnected infrastructure their best interests lie in perpetuating its safety, until something else comes along to replace the Internet. Until then, everyone is in the same vulnerable situation.

Chapter Six:

Conclusion

Beidleman calls cyberspace, "the *world's* nervous system; the control system of modern society. Its protection is an international existential concern" (Beidleman, 2011). Such grand sentiment is echoed among users who have come to rely on cyberspace to function daily. Today's globalizing climate necessitates the use of cyberspace to communicate and grow. The issue of cyberwar challenges future state and international security. Cyberwar as we currently understand it has not had a very long existence, and yet its metamorphosis through technological advancement has brought remarkable strain to global proceedings.

After analyzing shortcomings of the realist and liberalist perspectives towards international norms concerning cyberwar, and looking at the issue through the lens of the English School perspective, I argue that this is not the time for unilateralism. Instead, I assert that international consensus on the question of cyberwar must come to fruition. The English School perspective offers an environment where an international society of states can perpetuate regional and international cooperation in the face of dangers not understood until recently. Customary international law may be too slow to respond to the fast-paced cyber-world. States must be proactive rather than reactive to the threats inherent in cyberspace. Those in the minority that believe that this issue does not command immediate attention need only speak with those who have experience in this arena. This is not meant to be a metaphorical "the sky is falling" attitude, but to continue the metaphor, an umbrella would be handy, and everyone should have access to one.

The case studies that are included have shown that states (as well as capable individuals and other actors) can create an environment that leaves those affected incapacitated and damaged. The potential for international consensus may be of comfort, but this consensus must be clear and address the multitude of complexities and dangers intrinsic to the issues of cyberwar. I recommend that newly formed norms perhaps codified in treaties might offer the international community some clarity and agreement among its members. Similar to the nuclear threat faced by those in the twentieth century, a new regime of international law needs to be sanctioned and enacted in order to begin to regulate cyberwar in the twenty-first century and beyond. To do less is to invite cyber-disaster.

List of References

Arquilla, John and David Ronfeldt. 1997. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation.

Ashmore, William C. 2009. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defense Review.* 11(1): 4-40.

Azarov, Serge S. and Alexander G. Dodonov. 2006. "Instrumental Corrections for a Definition of Cyberwar" In *Cyberwar-Netwar: Security in the Information Age Vol4,* Eds. Fernando Duarte Carvalho and Eduardo Mateus da Silva. Amsterdam: IOS Press.

Beidleman, Scott W. 2011. "Defining and Deterring Cyber War." Strategy Research Project, United States Army War College.

Beidleman, Scott W. 2011. "Defining and Deterring Cyber War." *Military Technology.* 35(11) 57-62.

Benatar, Marco. 2009. "The Use of Cyber Force: Need for Legal Justification?" *Goettingen Journal of Int Law* 1 No3 (2009) 375-396.

Brown, Davis. 2006. "A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict." *Harvard Int Law J* 47 no1 (Winter 2006): 179-221.

Bull, Hedley. 1977. *The Anarchical Society: A Study of Order in Politics.* London: Macmillan. Quoted in Edward Keene. 2009. *International Society as an Ideal Type.* New York: Palgrave-Macmillan, 113.

Bull, Hedley. 1977. *The Anarchical Society: A Study of Order in Politics.* London: Macmillan. Quoted in Andrew Linklater. 2009. *The English School.* Cambridge: Cambridge University Press, 96.

Bull, Hedley and University of Waterloo. 1984. "Justice in International Relations" In *The Hagey Lectures.* Waterloo: University of Waterloo. Quoted in Andrew Linklater. 2009. *The English School.* Cambridge: Cambridge University Press, 97.

Burchill, Scott. 2009. "Liberalism" In *Theories of International Relations 4th Ed.,* eds. Andrew Linklater and Scott Burchill. New York: Palgrave-Macmillan.

Carr, Edward H. 1946. *The Twenty Years' Crisis: 1919-1939: An Introduction to the Study of International Relations.* London: Macmillan. Quoted in Jack Donnelly. 2009*. Realism and International Relations.* Cambridge: Cambridge University Press, 53.

Center for Strategic and International Studies. 2012. "NATO and Cyber Defense: A Brief Overview and Recent Events." http://csis .org/blog/nato-and-cyber-defense-brief-overview-and-recent-events (March 5, 2012)

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins.

Collier, Mike. 2007. "Estonia: Cyber Superpower. Business Week, December 17. http://www.businessweek.com/globalbiz/content/ dec2007/gb20071217_535635. htm; (accessed August 7, 2008). Quoted in Ashmore, William C. 2009. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defense Review.* 11(1): 4-40.

Computer Language Company. 2012. "Definition of PLC." *PC Magazine.* http://www.pcmag.com/ encyclopedia_term/0,2542,t=PLC&i=49375,00.asp (October 18, 2012).

Constantin, Lucian. 2012. "Researchers identify Stuxnet-like malware called 'Flame.' *Computerworld.* May 28, 2012.

Damrosch, Lori F., Louis Henkin, Sean D. Murphy and Hans Smit. 2009. *International Law: Cases and Materials, 5th Ed.* St. Paul: West.

Donnelly, Jack. 2009. "Realism" In *Theories of International Relations 4th Ed.,* eds. Andrew Linklater and Scott Burchill. New York: Palgrave-Macmillan.

Estonian Ministry of Defence, 2008. *Cyber Security Strategy*. Tallinn. Quoted in Ashmore, William C. 2009. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defense Review.* 11(1): 4-40.

Farnsworth, Timothy. 2011. "UK Calls for International Cyber Conference." *Arms Control Today* Vol42 Issue 1 (March, 2011): p7.

Farwell, James P. and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival,* 53(1) 23-40.

Fukuyama, Francis. 1992. *The End of History and the Last Man.* London: Harper Perennial

Gervais, Michael. 2012. “Cyber Attacks and the Laws of War.” *Berkeley Journal Of International Law,* 30(2), 525-579.

Gostev, Alexander, 2012. “The Flame: Questions and Answers.” http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers. May 28, 2012.

Gostev, Alexander, 2012. “Back to Stuxnet: the missing link.” http://www.securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link. June 11, 2012.

Griffiths, Martin, Steven C. Roach and M. Scott Solomon. 2009. *Fifty Key Thinkers in International Relations 2nd Ed*. London: Routledge.

Grove, Gregory, Seymour E. Goodman and Stephen J. Lukasik. 2000. “Cyber-attacks and International Law.” *Survival: Global Politics and Strategy* Vol42 Issue 3: 89-104.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. 2012. “The Law of Cyber-Attack.” *California Law Review* 100(4), 817-885.

Herz, John H. 1976. *The Nation-State and the Crisis of World Politics: Essays on International Politics in the Twentieth Century.* New York: D. McKay. Quoted in Jack Donnelly. 2009*. Realism and International Relations.* Cambridge: Cambridge University Press, 54.

Hobsbawm, Eric. 2007. *Globalisation, Democracy and Terrorism.* London: Little & Brown*.* Quoted in Scott Burchill. 2009*. Liberalism.* Cambridge: Cambridge University Press, 81.

Hoisington, Matthew. 2009. “Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense.” *Boston Coll Int Comp Law Rev* 32 no2 (Spring 2009): 439-454.

Hollis, Duncan B. 2007. “Why States Need an International Law for Information Operations.” *Lewis Clark Law Rev* 11 no4 (Winter 2007): 1023-1061.

Hollis, Duncan B. 2011. “An e-SOS for Cyberspace.” *Harvard Int Law J* 52 no2 (Summer 2011): 373-432.

Hughes, Rex B. 2009. “NATO and Cyber Defence: Mission Accomplished?” http://www.atlcom.nl/site/english/nieuws/wp-cont ent/Hughes.pdf (October 1, 2012).

IT Law Wiki, “Distributed denial-of-service attack”. 2012. http://itlaw.wikia.com/wiki/Distributed_denial_of_service (September 28, 2012).

James, Alan. 1973. “Law and Order in International Society” In *The Bases of International Order: Essays in Honour of C. A. W. Manning.* ed. Alan James. London: Oxford University Press.

Jenik, Aviram. 2009. “Cyberwar: Cyberwar in Estonia and the Middle East.” *Network Security* 2009(4): 4-6.

Johnson, Janet B., H.T. Reynolds and Jason D. Mycoff. 2008. *Political Science Research Methods* 6th Ed. Washington D.C.: CQ Press.

Kanuck, Sean. 2010. “Sovereign Discourse on Cyber Conflict Under International Law.” *Tex Law Rev* 88 no7 (June 2010): 1571-1597.

Keene, Edward. 2009. “International Society as an Ideal Type” In *Theorizing International Society: English School Methods*. ed. Cornelia Navari. New York: Palgrave-Macmillan.

Keohane, R. O. and Joseph Nye. 1977. *Power and Interdependence: World Politics in Transition.* Boston: Little. Quoted in Scott Burchill. 2009. *Liberalism.* Cambridge: Cambridge University Press, 66.

Langner, Ralph. 2010. “The Big Picture.” http://www.langner.com/en/2010/11/19/the-big-picture (October 9, 2012).

Linklater, Andrew. 2009. “The English School” In *Theories of International Relations 4th Ed.* eds. Andrew Linklater and Scott Burchill. New York: Palgrave-Macmillan.

Malanczuk, Peter. 1997. *Akehurst’s Modern Introduction to International Law, 7th Rev. Ed.* London: Routledge.

Mansfield-Devine, Steve. 2012. “Feature: Estonia: What Doesn’t Kill You Makes You Stronger.” *Network Security* 2012(7): 12-20.

Mayall, J. 2000. *World Politics: Progress and its Limits.* Cambridge: Polity Press.

McMillan, Robert. 2010. "Siemens: Stuxnet worm hit industrial systems." *Computerworld.* October 9, 2012.

Melikishvili, Alexander. 2008. "Recent Events Suggest Cyber Warfare Can Become New Threat." *WMD Insights.* http://www.wmdinsights.com/I29/I29_G3_RecentEvents.htm; (February 19-20th, 2009). As quoted in Ashmore, William C. 2009. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defense Review.* 11(1): 4-40.

Military and Paramilitary Activities (Nicaragua v. U.S.). 1986. I.C.J. Rep. 14, 62 110 (June 27). Quoted in Shackelford, Scott J. 2009. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal Of International Law* 27(1), 192-251.

Montalbano, Elizabeth. 2011. "Federal Cyber Attacks Rose 39% in 2010." *Information Week.* March 23, 2011.

Morgenthau, Hans. 1948. *Politics Among Nations: The Struggle for Power and Peace 7th Ed.* New York: McGraw-Hill. Quoted in Jack Donnelly. 2009*. Realism and International Relations.* Cambridge: Cambridge University Press, 53.

Morgenthau, Hans. 1970. *Truth and Power: Essays of a Decade, 1960-1970.* New York: Praeger.

Muir, Lawrence L. 2011. "The Case Against an International Cyber Warfare Convention." *Wake Forest L. Rev. Online 5.*

Nakashima, Ellen. 2012. "Newly identified computer virus, used for spying, is 20 times size of Stuxnet." *The Washington Post.* May 28. http://www.washingtonpost.com/world/national-security/newly-identified-computer-virus-used-for-spying-is-20-times-size-of-stuxnet/2012/05/28/gJQAWa3VxU_story.html. May 28, 2012.

Nakashima, Ellen, Greg Miller and Julie Tate, 2012. "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say." *The Washington Post.* June 19. http://www.washingtonpost .com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials say/2012/06/19/gJQA6xBPoV _story.html June 19, 2012.

NATO CCD DOE, 2012. http://www.ccdcoe.org/. (October 21, 2012).

Prosecutor v. Tadic, Case No. IT-94-1-I ICTY (Oct 2, 1995). As quoted in Shackelford, Scott J. 2009. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal Of International Law* 27(1), 192-

251.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *The Journal of Strategic Studies* Vol 35 No1 5-32.

Russell, Greg. 1990. *Hans J. Morgenthau and the Ethics of American Statecraft.* Baton Rouge: Louisiana State University Press*.* Quoted in Jack Donnelly. 2009*. Realism and International Relations.* Cambridge: Cambridge University Press, 52.

Sanger, David E. 2012. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times.* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 (October 9, 2012).

Schaap, Arie J. 2009. "Cyber Warfare Operations: Development and Use under International Law." *Air Force Law Review* 64: 121-173.

Schmitt, Michael N. 1999. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*." Columbia Journal of Transnational Law* 37 no3 885-937.

Schwarzenberger, Georg. 1951. *Power Politics: A Study of International Society, 2nd Edition.* London: Stevens*.* Quoted in Jack Donnelly. 2009*. Realism and International Relations.* Cambridge: Cambridge University Press, 28.

Shackelford, Scott J. 2009. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal Of International Law* 27(1), 192-251.

Shackelford, Scott J. 2010. "Estonia Three Years Later: A Progress Report on Combating Cyber Attacks." *Journal of International Law* 13(8), 22-29.

Socor, Vladimir. 2008. "NATO Creates Cyber Defence Centre In Estonia." Eurasia Daily Monitor. http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=33636; (accessed December 18, 2008). Quoted in Ashmore, William C. 2009. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defense Review.* 11(1): 4-40.

Sofaer, Abraham D. and Seymour E. Goodman. 2001. "Cyber Crime and Security: The Transnational Dimension" In *The Transnational Dimension of Cyber Crime and Terrorism,* eds. Abraham D. Sofaer and Seymour E. Goodman. Stanford: Hoover Press.

Stapleton-Gray, Ross and William Woodcock. 2011. "National Internet Defense—Small States on the Skirmish Line." *Communications Of The ACM,* 54(3), 50-55.

Swanson, Lesley. "The era of cyber warfare: applying international humanitarian law to the 2008 Russian-Georgian cyber conflict." *Loyola Los Angeles Int Comp Law Rev* 32 no2 (Spring 2010): 303-333.

Symantec. 2012. "Malware." http://us.norton.com/security_ response /malware.jsp (October 17, 2012).

Talbot, David. 2010. "Moore's Outlaws" *Technology Review.* http://www.technologyreview.com/featured-story/419452/moores-outlaws/? Mod=related. (October 18, 2012).

Tsukayama, Hayley. 2012. "Flame cyberweapon written using gamer code, report says." *The Washington Post.* May 31. http://www.washingtonpost.com/business/technology/flame-cyberwea pon-written-using-gamer-code-report-says/2012/05/31/ gJQAkIB 83U _story.html. May 31, 2012.

United Nations. 1945. *Charter of the United Nations.* http://www.un.org/en/documents/charter/index.shtml. October 18, 2012.

U.N.T.S Protocol additional to the Geneva Conventions of 12 August 1949. 2009. Volume 1125. https://ehis-ebscohost-com.ezproxy.lib.usf.edu/eds/detail?vid=3&hid=102&sid=beec906d-fc3f-4a11-a12cbb0733708558@sessionmgr115&bdata=JnNpdGU9ZWRzLWxpdmU=#db=aph&AN=21212890. (October 20, 2012).

United States Army. 2010. *Cyberspace Operations Concept Capability Plan 2016-2028*. TRADOC Pamphlet 525-7-8. http://www.fas.org/irp/doddir/army/pam525-7-8.pdf (October 17, 2012).

U.S. Department of Commerce, National Institute of Standards and Technology. 2004. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security.* NIST Special Publication 800-27A. http://csrc.nist.gov/publications/nist pubs/800-27A/SP800-27-RevA.pdf (September 28, 2012).

U.S. Department of Commerce, National Institute of Standards and Technology. 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-94 http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (October 17, 2012).

U.S. Department of Defense, 2012. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02. http://www.dtic.mil/ doctrine /new_pubs/jp1_02.pdf. (October 17, 2012).

U.S. Federal Communications Commission, Communications Security, Reliability and Interoperability Council, Working Group 7, Botnet Remediation. 2012. *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs): Final Report.* http://www.maawg.org/system/files/20120322%20WG7%20Final%20Report%20for%20CSRIC%20III_3.pdf (September 28, 2012).

U.S. General Accounting Office. Report to Congressional Requestors. 2004. *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* U.S. GAO-04-354. http://www.gao.gov/new.items/d04354.pdf (September 28, 2012).

U.S. General Accounting Office. Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform. 2004. *Information Security: Agencies Face Challenges in Implementing Effective Software Patch Management Processes.* U.S. GAO-04-816T. http://www.gao.gov/new.items/d04816t.pdf (September 28, 2012).

Vincent, R. J. 1986. *Human Rights and International Relations.* Cambridge: Cambridge University Press. Quoted in Andrew Linklater. 2009. *The English School.* Cambridge: Cambridge University Press, 97.

Waltz, Kenneth. 1979. *Theory of International Politics*. Reading: McGraw-Hill.

Wendt, Alexander. 1992. "Anarchy is what states make of it: The social construction of power politics." *International Organization* 46 (spring): 391-425.

Wight, Martin and Gabriele Wight. 1992. *International Theory: The Three Traditions.* London: Holmes & Meier for the Royal Institute of International Affairs.

Wilson, Peter. 2009. "The English School's Approach to International Law" In *Theorizing International Society: English School Methods.* ed. Cornelia Navari. New York: Palgrave-Macmillan.

Appendices

Appendix A: Glossary of Acronyms and Terms

Botnet: A network of Internet-connected end-user computing devices infected with bot malware, which are remotely controlled by third parties for nefarious purposes. A botnet is under the control of a given "botherder" or "botmaster." A botnet might have just a handful of botted hosts, or millions (U.S. Federal Communications Commission, 2012).

Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (Department of Defense Joint Publication 1-02, 2012).

Cyber-attack (CyA): CyA actions combine Computer Network Attack (CNA) with other enabling capabilities (such as, EA, physical attack and others) to deny or manipulate information and/or infrastructure (U.S. Army TRADOC Pam 525-7-8, 2010).

Cyber-terrorism: Premeditated, politically motivated attack against information, computer systems, computer programmes, and data, which result in violence against noncombatant targets (Azarov and Dodonov, 2006).

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Department of Defense Joint Publication 1-02, 2012).

Cyberwar: Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption (Clarke and Knake, 2010).

Defense Information Infrastructure (DII): The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information (Department of Defense Joint Publication 1-02, 2012).

Denial of Service Attack (DoS): The prevention of authorized access to resources or the delaying of time-critical operations (U.S. Department of Commerce, National Institute of Standards and Technology, 2004).

Distributed Denial of Service Attack (DDoS): Same as Denial of Service attacks, but on a grand scale using Botnets or Worms to spread the attack.

Global Information Infrastructure (GII): The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure (Department of Defense Joint Publication 1-02, 2012).

Information Operations (IO): The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decision-making of adversaries and potential adversaries while protecting our own (Department of Defense Joint Publication 1-02, 2012).

Information Security (INFOSEC): The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users (Department of Defense Joint Publication 1-02, 2012).

Information System (IS): The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information (Department of Defense Joint Publication 1-02, 2012).

Intrusion Detection System (IDS): Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized (U.S. Department of Commerce, National Institute of Standards and Technology, 2007).

Intrusion Detection and Protection System (IDPS): An intrusion detection system (IDS) is software that automates the intrusion detection process (U.S. Department of Commerce, National Institute of Standards and Technology, 2007).

Intrusion Prevention System (IPS): An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents (U.S. Department of Commerce, National Institute of Standards and Technology, 2007).

Logic Bombs: In programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs. (U.S. General Accounting Office, 2004).

Malware: Malware is a category of malicious code that includes viruses, worms, and Trojan horses (Symantec, 2012).

National Information Infrastructure (NII): The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure (Department of Defense Joint Publication 1-02, 2012).

Programmable Logic Controller (PLC): A programmable microprocessor-based device that is used in discrete manufacturing to control assembly lines and machinery on the shop floor as well as many other types of mechanical, electrical and electronic equipment in a plant (The Computer Language Company, 2012).

Supervisory Control and Data Acquisition System (SCADA): Software for networks of devices that control the operation of a system of machines such as valves, pumps, generators, transformers and robotic arms. SCADA software collects information about the condition of and activities on a system. SCADA software sends unencrypted instructions to devices, often to do physical movements. Instructions sent to devices on SCADA networks are sometimes sent over the Internet or broadcast via radio waves (Clarke and Knake, 2010).

Transmission Control Protocol/Internet Protocol (TCP/IP): The format used to divide information such as emails into digital "packets" each with its own to and from data so that the packet can be routed on the internet (Clarke and Knake, 2010).

Trojan Horse: Computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute (U.S. General Accounting Office, 2004).

Virus: A program that 'infects' computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the 'infected' file is loaded into memory, allowing the virus to infect other files (U.S. General Accounting Office, 2004).

Worm: Independent computer program that reproduces by copying itself from one system to another across a network (U.S. General Accounting Office, 2004).

Zero-Day Vulnerability: Zero-day vulnerabilities are vulnerabilities against which no vendor has released a patch. The absence of a patch for a zero-day vulnerability presents a threat to organizations and consumers alike, because in many cases these threats can evade purely signature-based detection until a patch is released. The unexpected nature of zero-day threats is a serious concern, especially because they may be used in targeted attacks and in the propagation of malicious code (Symantec, 2012).