REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-04-2011	Master of Military Studies Research Paper	September 2010 - April 2011

4. TITLE AND SUBTITLE
International Acceptance of Kinetic Operations in Response to a Cyber Attack

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Major Andrew Rundle, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
The examination of recent cyber attack cases has illustrated the difficulties of dealing with warfare that originates from the domain of cyberspace. Proportionality, preemption, and attribution are three issues that are difficult to address when talking about cyber warfare and cyber attacks. An isolated incident of a cyber attack, if it can be attributed to an attacker, poses the idea of a responsive attack by the victim. If it is justified, then the next question is regarding the amount of force that would be seen as internationally legitimate. The question of preemption with regard to a cyber attack is more likely to be seen as legitimate when the cyber attack is initiated as the first of other kinetic operations at the beginning of a state of war. Currently, a kinetic response to a cyber attack as a means of self defense from follow-on kinetic attacks would be viewed as illegal preemption and/or an escalation of force. These scenarios present interesting considerations with regard to international law, just war, and legitimacy.

15. SUBJECT TERMS
Cyberwarfare, Cyber attacks.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps University / Command and Staff College
Unclass	Unclass	Unclass	UU	32	19b. TELEPONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

International Acceptance of Kinetic Operations in Response to a Cyber Attack

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Andrew A. Rundle, USMC

AY 10-11

Mentor and Oral Defense Committee Member: _____
Approved: Adam Cobb
Date: 15 MAR 11

Oral Defense Committee Member: Richard L. DiNardo
Approved: _____
Date: 15 March 2011

Executive Summary

Title: International Acceptance of Kinetic Operations in Response to a Cyber Attack

Author: Major Andrew A. Rundle, United States Marine Corps

Thesis: The physical effects of a cyber attack can result in those equal to or greater than that of a conventional kinetic attack. In some cases, a cyber attack is the initial strike in the beginning of a conventional war. Kinetic response options to such cyber attacks should not be viewed internationally as illegitimate or illegal. Cyber warfare response options should not be limited to the domain of cyber space.

Discussion: The examination of recent cyber attack cases has illustrated the difficulties of dealing with warfare that originates from the domain of cyberspace. Proportionality, preemption, and attribution are three issues that are difficult to address when talking about cyber warfare and cyber attacks. An isolated incident of a cyber attack, if it can be attributed to an attacker, poses the idea of a responsive attack by the victim. If it is justified, then the next question is regarding the amount of force that would be seen as internationally legitimate. The question of preemption with regard to a cyber attack is more likely to be seen as legitimate when the cyber attack is initiated as the first of other kinetic operations at the beginning of a state of war. Currently, a kinetic response to a cyber attack as a means of self defense from follow-on kinetic attacks would be viewed as illegal preemption and/or an escalation of force. Both scenarios present interesting considerations with regard to international law, just war, and legitimacy. The idea of preemption as a means of self defense is sensitive when the perceived threat is on the magnitude of a rogue nation with a nuclear weapon. It gets even more sensitive if the subject is the cyber attack that is preparing a nation for a kinetic invasion or one that will result in damage to vital national interests. Knowing the difference between the lone and the combined arms cyber attacks exampled in the body of this paper is typically only recognized after the kinetic invasion has begun or if nothing succeeds the cyber attacks themselves.

Conclusion: Whether an attack is delivered through physical means or by way of cyberspace, the resultant tangible effects felt by the victim determine the proportionality of the response. Cyber attack can be considered a use of force that warrants a kinetic response or preemptive attack if the damage to vital national interests by the cyber attack is equal to or greater than that of a kinetic attack. Kinetic response or a preemptive attack should not be the only option, but it should not be excluded as an unviable option. International law needs revising in order to remain relevant in the current and future conflicts the United States and its allies will face. This update should include a provision for the effects of attacks delivered in cyberspace that cross a threshold that can have an internationally justified kinetic response or preemption option.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Page

Preface

The topic of cyber warfare has become one of increasing importance in today's world. The term "cyber" itself has become a buzz word that many use, but few I think can really appreciate how big of a deal it is with regards to our nation's interests and security. So much of the United States' economy, banking, government, communications infrastructure, and military rely on the cyber realm around the clock that a prolonged absence of them because of a cyber attack could send the nation into a state of confusion. A minor inconvenience of up to a few days would be annoying, but if the outages lasted on the order of magnitude of a natural disaster like Hurricane Katrina, then serious negative effects could result. In either case, I began to think about the effects of a cyber attack and its impact on traditional warfare. I have never used the term "cyber" more than I have this past year at the Command and Staff College (CSC) and I too knew very little about the subject, which is why I chose it as my Masters of Military Studies (MMS) thesis topic. I am an EA-6B Prowler Electronic Countermeasures Officer (ECMO) by trade and the subject of the future of Electronic Warfare in the Marine Corps had been addressed by previous CSC MMS theses. At the beginning of this process I knew very little about cyber and at this point I know probably just enough to be dangerous, but what I have become acutely aware of is the complexity of the topic of cyber security and cyber warfare. Our nation's leadership has identified the cyber realm as an area we need to safeguard and other theses have addressed potential ways of doing that. With some good answers proposed I began to think about what might cause the cyber battle to transcend into something involving kinetic military action or the use of force. My intent is to provide some interesting perspectives and generate discussion on the topic as there will eventually be conflict in the world that presents commanders with intermingled cyber and traditional warfare.

I. INTRODUCTION

Globalization and the proliferation of internet access have made the world a smaller and better connected place. This luxury of instantaneous information comes at a price to individuals and organizations in several forms of "digital aggression."[1] International connectivity has created a world where a single person, nation, or non-state actor with computer and internet access can effect world events and impact the day to day lives of millions of people. In recent years these cyber events have started to make more headlines and as a result have been getting more attention by national governments, private businesses, and even educational institutions. Many universities have developed collegiate level programs offering majors in the study of cyber security and most businesses with their own networks, if not all, employ those who specialize in cyber security. The network systems of the United States government and armed forces are no different. Thieves, terrorists, and various predators prowl the internet looking to hack into a system for any number of reasons, but whatever the reasons once they gain access they can do tremendous damage. Identity theft, planting a virus to accomplish various types of damage, and international or corporate espionage are only a few threats that accompany the connectivity the world enjoys. Part of the problem with cyber warfare is determining how the attacked party should respond and to whom they should direct their efforts when these digital actions result in physical, lethal, and even catastrophic consequences.

The United States government has established security protocols to dissuade and prevent such attacks on vital national cyber systems and there has been limited discussion regarding retaliation for or preemptive military action against an impending cyber attack. In traditional warfare a legitimate and proportional response to a threat or hostile act is much simpler than one that resides in cyberspace. Because cyberspace itself cannot be invaded in the traditional sense,

it poses a very difficult problem as to what are some internationally legitimate options regarding a United States response to a cyber attack or pending attack. The issues of international legitimacy and proportionality are questions that have yet to be answered when it comes to a kinetic military operation in response to or in preemption of a cyber attack.

In either case, whether the response is motivated by preemption to a real and viable threat or in response to an attack on United States' cyber interests the action must be proportional for it to be seen as internationally just. Proportionality in a medium that physically does not exist as it does in traditional warfare creates a difficult situation regarding options for U.S. attack or counter-attack. The degree of damage to a nation's interests or threat to those interests should have a threshold that if crossed by the attacker could result in an internationally legitimate kinetic or lethal response. If not, nations faced with a cyber attack preceding a conventional attack would be unable to legally defend themselves under current international law.

The rationale for the use of force in response to a cyber attack or in preemption to an imminent attack will be addressed within the framework of current international law regarding the right to use force. A similar discussion of cyber warfare by Michael N. Schmitt will be referenced with regard to use of force as it pertains to the cyber world. Specifically, Michael Schmitt's work addresses cyber attacks within the current United Nation's guidelines for the use of force with cyber as that force being used. Current examples of cyber attacks on significant national infrastructure that had resulted in physical damage as well as attacks resulting in non-physical damage will be discussed. These scenarios will be viewed with the idea that the nations that were attacked were not in a state of traditional war with their attackers. Hypothetical situations that end with some sort of destructive result because of a cyber attack will also be discussed in an attempt to justify the need for a hierarchy of kinetic military response options.

The response to or preemption of a cyber attack during a state of war will not be examined in detail as the potential for a kinetic response to a cyber attack in that environment is more easily justified as the nations are already at war. The difficulties that result from hostilities of non-state aggressors and difficulties that are a side effect of this type of battle space will not be examined in detail.

II. BACKGROUND

When the internet in its most basic form was invented in 1969 the world had no idea how much of an impact it would have on the entire planet. The genesis of the cyber age began when an idea to connect a few scientific computers met with Advanced Research Project Agency (ARPA) funding from the Pentagon.[2] The ARPANET was born and twenty years later it had grown into a network of servers that were named the World Wide Web (WWW).[3] By 1993 the internet was able to be accessed by millions of users because of the development of software like Mosaic and later Netscape Navigator.[4] Throughout the 1990's the internet continued to shrink the planet by bringing people closer together with the assistance of rapid advances in technology. This increased connectivity led to great conveniences and efficiencies in business, education, government, media, and overall day to day life.

The global proliferation of network connectivity and access to the internet has increased the criminal activities of computer hackers. The motivation of these individuals or groups varies from simply desiring access to a system to a variety of malicious intentions.[5] Once access is gained to the system, the malicious hackers may be looking to steal, control the system, deny a service, or destroy it.[6] The destruction can range from data loss to physical destruction of hardware or the hardware the system controls. In recent years individuals with these

technological skills have been recruited into adversarial organizations that systematically probe U.S. governmental and military systems. These organizations can be state or non-state actors whose intentions range from theft to destruction as the goals of the basic hackers. These attackers have a variety of software and codes that they can use in order to create their desired effect.[7] These intruders and our national reliance on the systems being manipulated have elevated the topic and security of cyberspace to specific attention in the President's 2010 National Security Strategy.[8] Internationally, organized units of cyber attackers like North Korea's Lab 110, the Korean People's Army Joint Chiefs Cyber Warfare Unit 121 and Israel's Unit 8200 have been increasing in many national militaries.[9] In response to these threats the Secretary of Defense directed the establishment of U.S. Cyber Command which became operational on 21 May 2010.[10] Whether recognized or not the age of cyber warfare had begun.

Prior to the recognized need for a military command devoted to the medium of cyberspace and the Secretary's articulation that cyber security is a vital national interest in the 2010 Quadrennial Defense Review, there have been many instances of cyber warfare between nations who are currently not in an active state of war.[11] Several of these cyber warfare cases will be exampled in this paper. For the subject of cyber warfare to be discussed a clear definition should be agreed upon. One definition of cyber warfare is defined as:

> ... the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls.[12]

For the following discussion about cyber warfare the above definition will be used with the following modification. The unauthorized user or penetrator of the system can be an

organization other than a government. An organization or group that conducts these acts without any government affiliation against a sovereign nation will also be engaging in cyber warfare.

The following examples of cyber warfare in recent history will be discussed for background information and later examined in the context of the right to use force in retaliation or preemption as the case applies: Iraq prior to the U.S. invasion in 2003, Estonia in April 2007, Syria in September 2007, Georgia in July 2008, the United States in July 2009, and Iran in September 2010.

In early 2003 as the U.S. was preparing to conduct Operation Iraqi Freedom, there was discussion about employing a new tactic against Saddam Hussein. The idea of cyber warfare was eventually employed in the form of a psychological operations campaign targeting the Iraqi military leadership to assist in the facilitation of their defeat, but a plan to conduct an arguably escalated cyber attack was forgone.[13] The psychological operations campaign in the form of an email being used in conjunction with conventional war is interesting, but not as interesting as the idea that the U.S. was contemplating a cyber attack to destroy financial assets of Saddam Hussein.[14] Because this was never done, there is no way to know how Iraq would have responded to the U.S. cyber attack on Saddam's finances or if they would have been able to determine the cause or even the culprit. By today's standards, if this type of attack were carried out against the United States Federal Reserve it would require a response. The question then leads to what the appropriate response might be and to whom should it be directed.

On April 27, 2007 there was a cyber attack on Estonia. At the time Estonia was not in a conventional war with anyone.[15] It is believed that tensions between Estonians and Russians living in Estonia caught the attention of patriotic Russians within Russia and it was this attention that was the catalyst for the cyber attacks on Estonia.[16] The Russian government denied its

involvement in the distributed denial of service (DDOS) attack, but it is believed that either the Komitet Gosudarstvennoy Bezopasnosti (KGB) replacement or organized crime was to blame for the attacks.[17] Whether the attack originated from a governmental agency like the former KGB, organized crime, or Russian hackers angry at Estonia, the fact is that a country was attacked in cyberspace with real life repercussions. In this instance the DDOS attack did not cause any major physical damage, but it did impact the national economy of Estonia until the attack was defeated.[18] The overall effect on the international community was heightened awareness of the cyber warfare phenomena and the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).[19] If the U.S. was to put itself in the place of Estonia in this example it would be faced with the dilemma of what would be an appropriate response to such attacks. The minor inconvenience of a few days of DDOS attacks would hardly resort to armed conflict if it were on the scale of the Estonian example, but if the attack had greater, more long lasting, and detrimental consequences, then the use of force might be warranted. Finding the line between tolerance and response is where the difficulty lies. Again, there also arises the problem of to whom is the response directed. In the Estonia case, there was no clear evidence that would prove who was behind the attacks.

In the previously discussed examples the effects were strictly within the systems themselves and were not accompanied by kinetic or lethal effects. The next two examples show the use of cyber attacks as a combined arms weapon and not one that has been considered a stand-alone that is somehow not used in conjunction with some other means of force. Both examples are not during times of war, but were followed by the use of traditional force. In the Georgian example, a state of traditional warfare succeeded the initial cyber attacks and cyber tactics were later used in conjunction with that traditional force.[20]

On September 6, 2007 aircraft from the Israeli Air Force bombed a complex in Syria believed to be linked to the development of weapons of mass destruction (WMD).[21] This arguably preemptive attack was later justified in 2008 when proof was released showing the facility was in fact related to WMD.[22] This is not a unique occurrence for the region as Israel has acted in the past when it has perceived a threat and, as will later be discussed, allegedly continues to do so. The unique aspect is that the aircraft were able to deliver their payloads without detection from the Syrian integrated air defense system (IADS). In this particular attack the Syrian forces were expecting something from the Israelis based on their positioning along the border, but there was no activity to respond to on the ground and nothing was seen in the air on radar.[23] When the later confirmed nuclear facility was destroyed Syria was alerted to the fact. that something was wrong with its IADS. Upon further investigation it was determined that the Israelis had coordinated a cyber attack on the IADS in order to shield their attack aircraft.[24] In *Cyber War: The next threat to National Security and what to do about it*, Richard Clarke and Robert Knake further explain possible methods of how this could have happened, but regardless of the means of cyber attack the Israelis managed to manipulate the Russian made Syrian systems using the domain of cyberspace. Regardless of the method, the Israelis cyber attack fulfilled the role of a suppression of enemy air defense (SEAD) operation against the Syrians. If the SEAD occurred by more traditional means it would have been interpreted as an attack on Syria. Because it was conducted in cyberspace should it be viewed differently?

In this case the cyber attack was used in conjunction with conventional, kinetic, and lethal force. This non-cyber force would surely justify a proportional response on the part of the Syrians if they chose to do so, but the cyber attack is another issue. The cyber attack itself damaged no infrastructure and had no kinetic or lethal effect on any Syrian, but its relationship

with the kinetic and lethal effects of the Israeli Air Force does raise questions about cyber attack responses. If the Syrians knew their IADS had been infiltrated by an Israeli spy or hacker, would that equate to an act of war allowing for a Syrian retaliatory attack before the kinetic Israeli attack began? Assuming the Syrians knew where the cyber attack came from would they be justified in responding to it with kinetic or lethal force before the Israeli attack aircraft appeared overhead? The problem with this is that it would either be viewed as an escalation of force or an illegal act of preemption under current international law. Responding to the cyber attack with traditional means of force before the Israeli aircraft bombed the WMD facility would surely be seen as an escalation of force on the part of the Syrians. If the Syrians responded with force to the cyber attack and the Israeli aircraft never launched the kinetic portion, then the Syrians would be seen as carrying out an illegal action of preemption. In either case, Syria's actions as the originally attacked nation would be seen as illegitimate. Preemption as a means of national defense is highly controversial because it is unlikely that an adversary will be able to know exactly what the alleged attacker is planning. The alleged attacker can always deny their intentions after an act of preemption defeats them when they play the role of the international victim. Cyber warfare because of its intrinsic intangibility raises new issues regarding international conflict. The question raised by this case receives further validation with the next example.

On August 8, 2008 Russia and Georgia were at war over two of Georgia's regions, Abkhazia and South Ossetia.[25] On the evening of 7 August the cyber attacks began with the intent to isolate Georgia from the outside world as conventional war began the following day with the invasion of Russian forces.[26] These well orchestrated attacks targeted the communications capabilities of the Georgian government, its ministries, and banks.[27] The

attacks were successful as the outgoing information from Georgia stopped as the war began.[28] In *Surviving Cyber War*, Richard Stiennon describes the specific attacks conducted in great detail, but as in the Syrian IADS case the manner in which the cyber domains were disabled seems of secondary importance to the fact they were disabled at all and that it was followed by a kinetic and lethal attack. In reality, the manner in which communications and air traffic radar were disabled is of great importance as it shows the emergence of cyber attacks as an initial strike tactic that does not fit the conventional definition of armed force. In this case, however, the conventional attacks were on a greater scale as it was an invasion and not a precision strike.

An interesting fact regarding the August 2008 cyber attacks on Georgia and the complimentary conventional invasion forces is that cyber attacks were seen almost three weeks prior to the various attacks on 7 August. On July 20, 2008 an independent research organization observed cyber botnet attacks on the Georgian president's websites that caused it to shut down for 24 hours.[29] This could have been a dress rehearsal for what was to come in the next few weeks. This intrusion and denial of the presidential website alone would not justify a kinetic or lethal response, but if it were known to be the precursor for follow-on conventional attacks as in the previous example a kinetic response might be justified by the Georgians. However, the same problem arises with the Georgians as would have with the Syrians responding with force to the cyber attack. At what point would the Georgians have been justified in kinetic and potentially lethal options as they were being shaped by the Russians for conventional operations?

In the next example there was no loss of life or related kinetic attack experienced by those who were attacked. At most there was a large amount of inconvenience and possibly embarrassment on the part of those whose servers were penetrated, but no real harm was done. On July 4, 2009 a DDOS attack was launched against a variety of U.S. governmental servers that

ultimately led to those servers being shut down at some point for a short period of time in order to clear the attack and limit the damage.[30] A botnet virus that allegedly originated from North Korea infected thousands of computers that in turn began a DDOS attack against several very important servers including: the White House, the Department of Treasury, the Secret Service, the New York Stock Exchange (NYSE), and the Federal Trade Commission.[31] These attacks caused no substantial damage and were hopefully a wake-up call to the respective systems' vulnerabilities. The same virus was redirected and attacked more vulnerable servers in South Korea before it was contained, defeated, and openly attributed to North Korea by the South Koreans.[32] Although the attack was eventually traced to a server in England where it appeared to originate from, truly determining who is responsible for such an attack further illustrates the difficulties of cyber conflict.[33]

The July 2009 cyber attacks on the U.S. and South Korea pose a serious problem to those responsible for national defense. If the attacks had damaged critical servers within White House what would have been the U.S. response? If the attacks for example crashed the NYSE and the Department of the Treasury systems, then the effects on the U.S. could have been potentially serious to investment and banking worldwide, depending on the duration and the extent of the damage. Thankfully, they did not, but it does stimulate thought on the subject of what the U.S. is willing to do to protect its critical infrastructure, to include that which resides digitally in cyberspace.

On November 29, 2010 the assassination of two Iranian nuclear scientists was complemented by a complex cyber attack designed to impede Iran's nuclear programs.[34] The attack of the Stuxnet virus caused the degradation of more than half the centrifuges at the Natanz enrichment facility.[35] The U.S. and Israel have been credited with the attacks, but no clear

evidence implicating either nation has been found.[36] One could argue that Israel is and has been at war with Iran for several years. However, we will consider them not to be in a state of war. As previously stated, an act of cyber aggression during conventional warfare where lethal means have been employed seems to be a clear case as to whether or not force is authorized to counter the cyber attack. In the Stuxnet example, if Israel and Iran were at war, then both countries would be justified in the use of force to retaliate against the cyber attack. That is not the situation though. In this case Iran knows that two of its nuclear scientists were attacked and it knows that more than half their centrifuge computers were rendered useless by a virus.[37] They do not know who is responsible for either, nor do they have any solid evidence. This is the type of situation that puts a nation in a predicament regarding its defense, what constitutes an act of force, and what response options are internationally just if the culprit can be found.

III. JUST WAR, RESPONSE OPTIONS, AND CYBERSPACE

Just war deals with the right to wage war, jus ad bellum, and the conduct within that war, jus in bello, as two factors for defining a nation's validity for explaining its warfare activities as "just." This discussion of just war and cyberspace will deal with the right of a nation to wage war, jus ad bellum, as a result of impending or received cyber attack. Because the U.S. is a permanent member of the U.N. Security Council, the law governing the right of a nation to wage war will be evaluated based on the U.N. Charter. A closely related evaluation has been done by Michael Schmitt and he makes a case that cyber attack can be considered as force against a nation as there is no clear definition of "force" in the U.N. Charter as it relates to cyber. In his paper, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Schmitt discusses two scenarios regarding computer network attacks

(CNA) with different intents before reaching the conclusion that there needs to be a newly established framework for analyzing cyber attacks.[38] The first deals with a CNA or cyber attack that is intended to shape the enemy for follow on conventional operations.[39] The examples of the U.S. invasion of Iraq in 2003, Israel's attack on Syria in September 2007, and the Russian invasion of Georgia in July 2008 would fall in this category. The other cyber attack is one that is meant to be an isolated event with no follow on plans by the cyber attacker.[40] The examples of cyber attacks on Estonia in April 2007, the United States in July 2009, and Iran in September 2010 would fall into this category. This discussion will take his legal arguments further in order to render a conclusion as to whether kinetic and lethal force is internationally justified in response to or in preemption of an impending cyber attack.

The Shaping Attack

In the examples of cyber attack that were followed by kinetic and lethal military operations it is clear that those nations that were attacked would have been justified if they chose to respond to the kinetic operations they received and some did respond. Developing a judgment on whether or not the attacked nations would have been justified in responding with kinetic force seems fairly clear in these examples because kinetic force was employed against them. The difficulty in passing judgment would be if Syria, for example, upon realizing their IADs was compromised by the Israelis decided to launch their own kinetic attack on Israel in order to defend itself from the impending airstrikes. In this case, the hypothetical "counter" strikes by the Syrians would most likely have been considered an illegal use of force by the international community. No doubt the Syrians would claim the strikes as a means of self defense and the Israelis would deny the plans to strike the facility as well as the cyber attack itself. One can see how a nation's inherent right to self defense as granted in the U.N. Charter's Article 51 is left up

to interpretation which can cause problems when it comes to the cyber domain as well as traditional kinetic conflict.

The other examples that fall in this category are no different if hypothetically the attacked nations were to recognize an impending kinetic operation against them following the cyber attack. If the attacked nation could recognize they were under cyber attack, somehow understand the enemies plan and how that cyber attack complimented impending kinetic operations, and could accurately attribute the cyber attack to the forthcoming attacker before the kinetic attack began, then they would be able to act kinetically and lethally in response to their cyber attack. This might be seen internationally as a case where one nation was conducting a just war in self defense under Article 51 as long as the cyber attack was labeled an illegal use of armed force. The problem is that it is very difficult, if not impossible, to answer all these questions in order to act legitimately and in a timely manner.

In contrast, the same U.N. Charter states what is considered not to be armed force in Article 41 stating, "measures not involving the use of armed force" include "complete or partial disruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication..."[41] Based on Article 41, even if the hypothetical conditions were met, the nations attacked kinetically following their cyber attacks would not be acting in accordance with the U.N. The examples of the U.S. invasion of Iraq in 2003, Israel's attack on Syria in September 2007, and the Russian invasion of Georgia in July 2008 all have cyber attacks that dealt specifically within the classification of the Article 41 definition of what is not considered armed force. The cyber attack on Iraq in 2003 may have at most caused a "disruption of...other means of communication" by hacking into the Iraqi military email system.[42] Even based on the interpretation of Article 41, the Bush administration may have been able to carry out the

proposed cyber attack on Saddam Hussein's finances without it being considered an act of armed force. It could have been seen as a "complete disruption of economic relations."[43] In the example of Israel's attack on Syria in September 2007, the cyber attack employed resulted in a "partial disruption of ... air" by the program which caused the radars to be inoperative.[44] Regarding the attack that preceded the Russian invasion of Georgia in July 2008, the cyber attack resulted in a "complete disruption of ... other means of communication" when the government websites went down.[45] The retaliation to the cyber attacks by the attacked nations in all hypothetical cases would have been seen as an unjust war based on Article 41.

The Isolated Attack

In the examples of the cyber attacks that were not followed by kinetic and lethal military operations it is unclear if those nations that were attacked would have been justified in responding to cyber attack with kinetic and lethal force. Developing a judgment on whether or not the attacked nations would have been justified in responding with kinetic force is very difficult in the cases listed within this category because of the uncertainty of attribution. The examples of cyber attacks on Estonia in April 2007, the United States in July 2009, and Iran in September 2010 have no clear aggressor as did the other examples. The cyber attacks on Estonia in 2007 were never evidentially attributed to the Russian government and there were some who believed it to be the work of former KGB, patriotic Russian hackers, or even organized crime.[46] Although the attacks crippled the communications and banking infrastructure of Estonia, those inconveniences would fall under the Article 41 category of not being considered as armed force. Again this would mean an Estonian response with kinetic or lethal force would be seen as unjust in the eyes of the U.N. and international law.

The cyber attacks on the United States in July 2009 and Iran in September 2010 also have no clear adversary who invaded their sovereign physical territory in conjunction with the cyber attacks. The enemy is hard to find and the attack's origin is even harder to prove. In these examples, as well as the Estonian example, there is no way to prove where the attack came from and who is ultimately responsible for it. In the cyber attack on the U.S. in 2009, a variety of U.S. government servers were made unavailable in order to defeat the cyber attack that was traced to a server in England.[47] This resulted in a "partial disruption of ... other means of communication" and was not considered armed force by U.N standards.

The case of the Stuxnet attack on the Iranian nuclear program centrifuges does pose a unique scenario. This cyber attack was carried out in conjunction with a kinetic and lethal operation that killed two Iranian nuclear scientists.[48] Like the cases exampled in this category, the culprits have not been identified as of yet, but like the exampled cases in the shaping section, cyber attacks were used in combination with the lethal force against the nuclear scientists. Because the Stuxnet case shares characteristics of both categories it falls into a gray area with regard to whether or not an armed force response can be justified. The degradation of the centrifuges and the nuclear program as a whole does not really fit into anything the U.N. Charter considers not to be armed force. It may actually fit more with those actions the U.N. considers to be armed attack just as a single precision airstrike would be considered armed attacked. However, as the single airstrike does not result in a legitimate full scale military retaliation, neither should an attack like the Stuxnet virus. Basically, this is a case where kinetic and lethal force was used to eliminate a human threat and a non-kinetic force was applied to reduce a capability arguably causing physical damage.

If the assassination attempt is omitted in the examination of this attack, the Stuxnet virus alone resulted in the physical damage of a sovereign nation's vital national interest. If the attacker could be identified as another nation, Iran might be able to justify a military response. However, a kinetic operation aimed at the launcher of the Stuxnet virus in response to the damage it caused would most likely be seen as an escalation of hostilities because of the moderate level of physical damage the virus caused. Although the Stuxnet virus did result in physical damage, the damage to the progress of the nuclear program was far greater than the monetary value of a computer system. Hypothetically, if the Iranian government could justifiably mount a kinetic response that would result in proportional damage to the attacking organization it would still have the very difficult problem of evidentially proving the alleged attacker was responsible for the virus.

IV. PREEMPTION AND INTERNATIONAL LAW

In 2003 the United States' invasion of Iraq to disarm Saddam Hussein of WMD was not carried out as a United Nations collective effort as Article 1(1) states. The Bush administration took criticism for its actions when no WMD were found. This act of preemption was eventually unsuccessful because it failed to meet at least one of the three tenets of a limited right to preemption, necessity, since there were no WMD found in Iraq.[49] With no evidence, this act of preemption was seen by some as an illegal preventive war. Following the unilateral, non-U.N. coalition, invasion of Iraq, Secretary-General Kofi Annan addressed the United Nations arguing against the use of preemptive force. He stated that, "if it were to be adopted, it could set precedents that resulted in a proliferation of the unilateral and lawless use of force, with or

without justification."[50] This debate over preemption continues today with the fear of WMD falling into the hands of terrorist groups.

The U.S. Constitution states that a ratified treaty is the law and that the U.S. government will uphold the terms of signed treaties, which the U.N. Charter is considered to be.[51] If this is true, then the United States is obligated to conduct itself in accordance with the U.N. Charter it signed in 1945.[52] The U.N. Charter states that nations have the inherent right to self defense and the only time that force is considered legitimate and legal is when exercising that right. The only mention in the U.N. Charter of anything remotely similar to preemption is the Security Council's ability to use "preventive or enforcement actions" referenced in Chapter I, Article 2(5) and later explained in Chapter VI.[53] These preventive actions are identified as a Security Council function and armed force is not identified as a means of conducting them. If any nation were to act unilaterally in a manner interpreted as preemption or a preventive use of armed force, then its actions would be considered internationally illegal and an illegitimate use of force. This is why it is important for a nation to distinguish its actions as being carried out in self defense if it is going to use armed force. Based on the current understanding of what constitutes an illegal use of armed force and how an act of self defense might be perceived in response to a cyber attack, the international community is in a difficult position with regard to its individual and collective response options. Currently a nation that receives an initial assault in cyberspace would not be able to carry out its right to self defense until a kinetic attack begins even if it knows the cyber attack is the precursor to that conventional armed attack.

V. ISSUES FOR FURTHER INVESTIGATION

Some have argued that the current U.N. Charter needs to be revised to address the issues of cyber warfare as a means of armed force in certain instances. Schmitt makes a compelling case that in certain and specific instances cyber warfare itself can be considered armed force.[54] It also must be revised to include what is considered to be preemption. Although one Secretary-General felt very strongly about the idea that preemption would create a "lawless use of force, with or without justification," how can it be considered lawless if the justification is validated as in the Israeli attack on Syria case? Revision of the U.N. Charter to include preemptive force in response to a cyber attack must be incorporated so when the need arises action can be taken. If the U.N. and the international community fail to agree with Schmitt's belief that the U.N. needs to modernize with a new framework, then a first strike in the form of a cyber attack will have to be disregarded for what it truly is because a retaliation for such an attack would currently be seen as an illegal use of force and not an act of self defense. New weapons and tactics will challenge the definition of conventional common sense terms used in the language of the U.N. Charter.

International investment in greater cyber security measures to prevent the need to retaliate and preemptively attack must also be continued. The cliche that "the best defense is a good offense" does not apply in cyberspace. In fact the opposite is true. This defense must include improved capability to attribute successful and attempted cyber attacks so the need for preemptive attacks, kinetic or non-kinetic, are not needed and non-violent means can be used to deal with the issue.

VI. CONCLUSION

The reality of cyber attacks and the increase in physical effects that they can have has raised the stature of cyber warfare from the idea of hackers meddling in a system for trivial ends to a threat to nation's interests. In reality, the effect of a cyber attack on a nation and its populace is the issue to debate and not the means of delivery of those effects. If a country is under attack by any means, kinetic or non-kinetic, then the nation is under attack. If the enemy can be identified, then the victim nation has the right to defend itself. The fact that the attack is in cyberspace is irrelevant from the perspective of whether or not a response is justified. The type of response, designed with proportionality in mind is the key to any response being seen as legitimate and internationally just.[55] It does not matter if the response is kinetic or not, if the cyber attack had physical or kinetic effects or even lethal effects, then the victim should be able to respond without fear of international condemnation as it is their inherent right to defend themselves. For example, if an attack results in damage and loss of life comparable to that of a major natural disaster, such as Hurricane Katrina in 2005, it should not matter the means of delivery of that attack. Essential services such as electricity, gas, hospitals, and food stores were "functioning at less than half of pre-Katrina capacity" one year after the hurricane struck New Orleans.[56] An estimate of peak restoration efforts following Katrina did not occur until approximately 24 weeks after the storm and even a year later the restoration still was not complete.[57] If the unknown number of dead, $40-50 Billion in damages, and hundreds of thousands of residents now living as refugees were the result of a cyber attack of some kind on a U.S. city, then that attack should be considered an illegal use of force and the U.S. should have the right to defend itself legitimately.[58]

The vague, ambiguous, and outdated wording of the U.N. Charter raises some very difficult questions with regard to international law and a nation's right to go to war. These questions will only get more difficult as conflicts continue to emerge that do not fit the current framework of the U.N. For example, in Article 2(7) the U.N. Charter references a nation's right to deal with "matters which are essentially within the domestic jurisdiction of any state" and states the U.N. has no authority to intervene.[59] This may have worked in 1945, but today there are significant domestic issues in sovereign nations caused by non-state actors residing in other sovereign nations. How does a country pursue a threat within the borders of a sovereign nation, especially if that threat is not from the government of that sovereign nation? The same difficulty resides in reference to cyber warfare. How does a nation pursue an attacker whose method of weapon delivery is data via the internet? This problem is further compounded by the difficulty of attribution for cyber attacks.

Regardless of the shape an attack takes, if that attack causes damage to vital national interests, then a nation has the right to defend itself. Since the events in cyberspace can cause real physical damage, national governments should be able to do what is necessary to protect its and international interests to include the option of a use of kinetic and lethal force in response to cyber attacks that are known to be the initial stage of a conventional attack.

Because the international community is highly interconnected in this age of globalization, a cyber attack that damages one nation's vital national cyber interests, such as banking, could surely damage many others as in the Estonia example. It is for this reason, as in most cases, that diplomacy should take a larger role so a collective effort can bring the issue to a resolution. The cases exampled dealt with one nation and global effects were not felt. The United Nations needs to take that lead and as Schmitt has proposed there needs to be a development of "an alternative

normative framework based on scrutiny of the consequences caused by such operations."[60] Schmitt proposed the following three factors that would warrant a "forceful" response to a cyber attack: "the CNA is part of an overall operation culminating in armed attack; the CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and the defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack."[61] These are a good set of guidelines that a nation can use with regard to warfare in general regardless of whether the attack is a cyber attack or a conventional one, including his explanation of preemptive force in the third factor.

Until the U.N. Charter is modified and updated to incorporate new domains, ideas of what sovereignty really is, and what constitutes force in the 21st century member nations faced with tough situations exampled earlier may be forced to justify and legitimize their actions when it comes to dealing with cyberspace or cyber initiated warfare.

---

[1] Julie E.Mehan. *Cyberwar, Cyberterror, Cybercrime: a Guide to the Role of Standards in an Environment of Change and Danger.* (Ely, U.K.: IT Governance Publishing, 2008) 83.

[2] Jean Guisnel. *Cyberwars: Espionage on the Internet*, trans. Gui Masai (New York: Plenum Press, 1997) 13.

[3] Ibid., 17.

[4] Ibid., 18.

[5] Julie E.Mehan. *Cyberwar, Cyberterror, Cybercrime: a Guide to the Role of Standards in an Environment of Change and Danger.* (Ely, U.K.: IT Governance Publishing, 2008), 52.

[6] Ibid., 53.

[7] Ibid., 53-62.

[8] The White House, *2010 National Security Strategy,* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (Jan. 10, 2011) 27.

[9] Richard A. Clarke and Robert K. Knake. *Cyber War: The next threat to National Security and what to do about it.* (New York: Ecco HarperCollins 2010) 26-27.

Christopher Dickey, R. M. Schneiderman, and Babak Dehghanpisheh. "The Shadow War; Someone is Killing Iran's Nuclear Scientists. But a Computer Worm May be the Scarier Threat." Newsweek. New York. Dec. 20, 2010. Vol. 156, Iss. 25.

[10] United States Strategic Command, *U.S. Cyber Command Fact Sheet*, http://www.stratcom.mil/factsheets/cc/ (Jan. 6, 2011).

[11] United States Department of Defense, *2010 Quadrennial Defense Review*, http://www.defense.gov/qdr/QDR%20as%20of%2026JAN10%200700.pdf (Jan. 6, 2011) 37-39.

[12] Richard A. Clarke and Robert K. Knake. *Cyber War: The next threat to National Security and what to do about it.* (New York: Ecco HarperCollins 2010), 228.

[13] Ibid., 9-11.

[14] Ibid., 10.

[15] Ibid., 13.

[16] Ibid., 12-16.

[17] Ibid., 15-16.

[18] Ibid., 15.

[19] Richard Stiennon. *Surviving Cyber War.* (Plymouth, U.K.: Government Institutes 2010), 90.

[20] Ibid., 96.

[21] Richard A. Clarke and Robert K. Knake. *Cyber War: The next threat to National Security and what to do about it.* (New York: Ecco HarperCollins 2010), 2.

[22] Ibid., 3-4.

[23] Ibid., 5.

[24] Ibid., 6-8.

[25] Richard Stiennon. *Surviving Cyber War.* (Plymouth, U.K.: Government Institutes 2010), 96.

[26] Ibid., 97.

[27] Ibid., 97.

[28] Ibid., 97.

[29] Ibid., 96-97.

[30] Richard A. Clarke and Robert K. Knake. *Cyber War: The next threat to National Security and what to do about it.* (New York: Ecco HarperCollins 2010), 23-24.

[31] Ibid., 24.

[32] Ibid., 24-26.

[33] Ibid., 23-24.

[34] Christopher Dickey, R. M. Schneiderman, and Babak Dehghanpisheh. "The Shadow War; Someone is Killing Iran's Nuclear Scientists. But a Computer Worm May be the Scarier Threat." Newsweek. New York. Dec. 20, 2010. Vol. 156, Iss. 25.

[35] Ibid.

[36] Julian Borger and Saeed Kamali Dehghan, "Attack on Iranian nuclear scientists prompts hit squad claims," *Guardian* [U.K.], November 29, 2010 (http://www.guardian.co.uk/world/2010/nov/29/iranian-nuclear-scientists-attack-claims).

[37] Christopher Dickey, R. M. Schneiderman, and Babak Dehghanpisheh. "The Shadow War; Someone is Killing Iran's Nuclear Scientists. But a Computer Worm May be the Scarier Threat." Newsweek. New York. Dec. 20, 2010. Vol. 156, Iss. 25.

[38] Michael N. Schmitt. *Computer Network Attack and the use of force in international law: thoughts on a normative framework*. Institute for Information Technology Applications, June 1999. 29.

[39] Ibid., 11.

[40] Ibid.,11.

[41] United Nations Charter, Chapter 7. http://www.un.org/en/documents/charter/chapter7.shtml (January 18, 2011).

[42] Richard A. Clarke and Robert K. Knake. *Cyber War: The next threat to National Security and what to do about it.* (New York: Ecco HarperCollins 2010), 9-11.

[43] United Nations Charter, Chapter 7. http://www.un.org/en/documents/charter/chapter7.shtml (January 18, 2011).

[44] Richard A. Clarke and Robert K. Knake. *Cyber War: The next threat to National Security and what to do about it.* (New York: Ecco HarperCollins 2010), 5.

[45] Richard Stiennon. *Surviving Cyber War.* (Plymouth, U.K.: Government Institutes 2010), 97.

[46] Richard A. Clarke and Robert K. Knake. *Cyber War: The next threat to National Security and what to do about it.* (New York: Ecco HarperCollins 2010), 12-16.

[47] Ibid., 23-24.

[48] Christopher Dickey, R. M. Schneiderman, and Babak Dehghanpisheh. "The Shadow War; Someone is Killing Iran's Nuclear Scientists. But a Computer Worm May be the Scarier Threat." Newsweek. New York. Dec. 20, 2010. Vol. 156, Iss. 25.

[49] Alex J. Bellamy. *Just Wars: From Cicero to Iraq*. (Cambridge, U.K.: Polity Press 2006) 162-163.

[50] Kofi Annan, United Nations Press Release SG/SM/8891 GA/10157. 23 September 2003, http://www.un.org/News/Press/docs/2003/sgsm8891.doc.htm (January 18, 2011).

[51] Richard J. Regan. *Just War: Principles and Cases.* (Washington, D.C.: The Catholic University of America Press 1996) 23-25.

[52] Ibid., 24.

[53] United Nations Charter, Chapter 1. http://www.un.org/en/documents/charter/chapter1.shtml (January 18, 2011).

United Nations Charter, Chapter 6. http://www.un.org/en/documents/charter/chapter1.shtml (March 8, 2011).

[54] Michael N. Schmitt. *Computer Network Attack and the use of force in international law: thoughts on a normative framework.* Institute for Information Technology Applications, June 1999.

[55] Alex J. Bellamy. *Just Wars: From Cicero to Iraq*. (Cambridge, U.K.: Polity Press 2006), 123.

[56] R.W. Kates, C.E. Colton, S. Laska, and S.P. Leatherman. October 3, 2006. "Reconstruction of New Orleans after Hurricane Katrina: A research perspective." *Proceedings of the National Academy of Sciences of the United States of America,* vol. 103, no. 40. http://belfercenter.hsg.harvard.edu/files/xstandard/hates_pnas_katrina_2006.pdf (February 28, 2011), 14656.

[57] Ibid., 14655.

[58] Ibid., 14655.

[59] United Nations Charter, Chapter 1. http://www.un.org/en/documents/charter/chapter1.shtml (January 18, 2011).

[60] Michael N. Schmitt. *Computer Network Attack and the use of force in international law: thoughts on a normative framework.* Institute for Information Technology Applications, June 1999, 3.

[61] Ibid., 28.

References

INTERNATIONAL: Cyber attacks signal new warfare era. 2009. *OxResearch Daily Brief Service* (Aug 27): 1, http://proquest.umi.com/pqdweb?did=1847243871&Fmt=7&clientId=32176&RQT=309&VName=PQD.

NSA, DoD Review Options for Cyber Attack Policy. 2000. *C4I News* 15, (9) (May 31): 1, http://proquest.umi.com/pqdweb?did=54480753&Fmt=7&clientId=32176&RQT=309&VName=PQD.

The United Nations Charter. http://www.un.org/en/documents/charter/chapter7.shtml (January 18, 2011).

The Virtual Battlefield: Perspectives on cyber warfare 2009. Cryptology and information security series / ciss. Vol. 3. Washington, DC: IOS Press.

The White House, *2010 National Security Strategy*, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (Jan. 10, 2011).

United States Department of Defense, *2010 Quadrennial Defense Review*, http://www.defense.gov/qdr/QDR%20as%20of%2026JAN10%200700.pdf (Jan. 6, 2011).

United States Strategic Command, *U.S. Cyber Command Fact Sheet*, http://www.stratcom.mil/factsheets/cc/ (Jan. 6, 2011).

Annan, Kofi, United Nations Press Release SG/SM/8891 GA/10157. 23 September 2003, http://www.un.org/News/Press/docs/2003/sgsm8891.doc.htm (January 18, 2011).

Bellamy, Alex J. *Just Wars: From Cicero to Iraq*. (Cambridge, U.K.: Polity Press 2006).

Blair, Dennis C. February 2010. *Annual threat assessment of the U.S. intelligence community for the House Permanent Select Committee on Intelligence.* Office of the Director of National Intelligence.

Borger, Julian and Saeed Kamali Dehghan, "Attack on Iranian nuclear scientists prompts hit squad claims," *Guardian* [U.K.], November 29, 2010 (http://www.guardian.co.uk/world/2010/nov/29/iranian-nuclear-scientists-attack-claims).

Carr, Jeffrey and Lewis Shepherd. 2010. *Inside cyber warfare*. 1st ed. Sebastopol, Calif.: O'Reilly Media, Inc.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber war : The next threat to national security and what to do about it.* 1st ed. New York: Ecco.

Cordesman, Anthony H.; Justin G. Cordesman; and Center for Strategic and International Studies. 2002. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.* Westport, Conn.: Praeger.

De Borchgrave, Arnaud, and CSIS Homeland Defense Project. 2001. *Cyber threats and information security : meeting the 21st century challenge.* CSIS report. Washington, D.C.: CSIS Press.

Dickey, Christopher; R. M. Schneiderman; and Babak Dehghanpisheh. Newsweek. New York. Dec. 20, 2010. Vol. 156, Iss. 25.

Fulghum, D. 2009. Cyber Attacks At U.S. Agencies Seen As Having Minor Impact, Major Implications. *Aviation Daily* 377, (6) (Jul 9): 1, http://proquest.umi.com/pqdweb?did=1796529921&Fmt=7&clientId=32176&RQT=309&VName=PQD.

Gallaher, Michael P., Albert N. Link, and Brent Rowe. 2008. *Cyber security : Economic strategies and public policy alternatives.* Cheltenham, UK ; Northampton, MA: Edward Elgar, http://www.loc.gov/catdir/toc/ecip081/2007039429.html.

Guisnel, Jean. *Cyberwars: Espionage on the Internet*, trans. Gui Masai (New York: Plenum Press, 1997).

Janczewski, Lech, and Andrew M. Colarik. 2008. *Cyber warfare and cyber terrorism.* Hershey: Information Science Reference, http://www.loc.gov/catdir/toc/ecip077/2006102336.html.

Jenik, A. 2009. Cyberwar in Estonia and the Middle East. *Network Security* 2009, (4) (Apr): 4, http://proquest.umi.com/pqdweb?did=1700191181&Fmt=7&clientId=32176&RQT=309&VName=PQD.

Kates, R.W., C.E. Colton, S. Laska, and S.P. Leatherman. October 3, 2006. "Reconstruction of New Orleans after Hurricane Katrina: A research perspective." *Proceedings of the National Academy of Sciences of the United States of America,* vol. 103, no. 40. http://belfercenter.hsg.harvard.edu/files/xstandard/hates_pnas_katrina_2006.pdf (February 28, 2011)

Knake, Robert K. September 2010. *Internet governance in an age of cyber insecurity.* Council on Foreign Relations, 56.

Mehan, Julie E. *Cyberwar, Cyberterror, Cybercrime: a Guide to the Role of Standards in an Environment of Change and Danger.* (Ely, U.K.: IT Governance Publishing, 2008).

Perlmutter, David D. 1999. *Visions of war: picturing warfare from the Stone Age to the Cyber Age.* 1st ed. New York: St. Martin's Press, http://www.loc.gov/catdir/bios/hol054/00502072.html; http://www.loc.gov/catdir/description/hol042/00502072.html.

Regan, Richard J. *Just War: Principles and Cases.* (Washington, D.C.: The Catholic University of America Press 1996).

Schaap, A., MAJOR. 2009. Cyber Warfare Operations: Development and use Under International Law. *The Air Force Law Review* 64, : 121, http://proquest.umi.com/pqdweb?did=1889115881&Fmt=7&clientId=32176&RQT=309&VName=PQD.

Schmitt, Michael N. *Computer Network Attack and the use of force in international law: thoughts on a normative framework.* Institute for Information Technology Applications, June 1999.

Shachtman, Noah. January 2010. Spooks in the machine: how the government should fight cyber spies. , http://www.progressivefix.com/wp-content/uploads/2010/01/Spooks-in-the-Machine_Jan2010.pdf (accessed 27 October 2010).

Stiennon, Richard. *Surviving Cyber War.* (Plymouth, U.K.: Government Institutes 2010).

Ware, Willis H., United States. Office of Science and Technology Policy, and Critical Technologies Institute. 1998. *The cyber-posture of the national information infrastructure.* Santa Monica, CA: Rand, http://www.rand.org/publications/MR/MR976/.

Wilshusen, Gregory C. and Davi M. D'Agostino. March 2010. *Cybersecurity: progress made but challenges remain in defining and coordinating the Comprehensive National Initiative.* United States Government Accountability Office, GAO-10-338.

Yonah, Alexander and Michael S. Swetnam. 1999. *Cyber terrorism and information warfare.* Terrorism. Vol. 2nd ser., 5th-8th v. Dobbs Ferry, N.Y.: Oceana Publications.