Strategy Research Project

CYBER ATTACK! CRIME OR ACT OF WAR?

BY

LIEUTENANT COLONEL DAVID M. KEELY
United States Air Force

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-04-2011	Strategy Research Project	13 April 2011 – 13 April 2011

4. TITLE AND SUBTITLE

Cyber Attack! Crime or Act of War?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel David M. Keely

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

COL Thomas Reilly
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

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

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In order to determine between crimes and acts of war for certain activities in cyberspace, the United States government must use national and international law, expert opinion, and logic. Since there are few existing rules or norms for cyber warfare, existing laws and norms must be examined and interpreted to develop guidance for responses to cyber attacks. A possible decision model incorporating this guidance is Schmitt's Analysis which should be adopted by the United States government to ensure that advice to the President regarding cyber attacks is consistent with international law.

15. SUBJECT TERMS

Cyberspace, Schmitt's Analysis, International Law, United Nations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	36	

USAWC STRATEGY RESEARCH PROJECT

CYBER ATTACK! CRIME OR ACT OF WAR?

by

Lieutenant Colonel David M. Keely
United States Air Force

Colonel Thomas Reilly
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel David M. Keely

TITLE: Cyber Attack! Crime or Act of War?

FORMAT: Strategy Research Project

DATE: 13 April 2011 WORD COUNT: 7,417 PAGES: 36

KEY TERMS: Cyberspace, Schmitt's Analysis, International Law, United Nations

CLASSIFICATION: Unclassified

In order to determine between crimes and acts of war for certain activities in cyberspace, the United States government must use national and international law, expert opinion, and logic. Since there are few existing rules or norms for cyber warfare, existing laws and norms must be examined and interpreted to develop guidance for responses to cyber attacks. A possible decision model incorporating this guidance is Schmitt's Analysis which should be adopted by the United States government to ensure that advice to the President regarding cyber attacks is consistent with international law.

CYBER ATTACK! CRIME OR ACT OF WAR?

How do we discern a cyber attack that is a crime from one that is an act of terrorism, espionage or war? It is the goal of this paper to help readers make that determination. We will define terms and use national and international law, expert opinion and logic to discern the difference between crime, espionage, and acts of war in the cyber domain. We will look at examples and comparative analysis with non-cyber events to illustrate the arguments. While exploring a group of factors known as Schmitt's Analysis to further clarify how to respond appropriately to cyber incidents, we will use a brief case study of Estonia to test them. Finally, a short set of recommendations are made to help the U.S. Government institutionalize an approach for making the determination between crimes and acts of war.

Why is this question important? It may seem like technocrats trying to count the number of electrons dancing on the head of a pin. But the definition of what is an act of war and what is not carries a great deal of importance in the United States. The Constitution very carefully divides powers between the Federal government and the states as well as internally among the executive, legislative, and judicial branches. While the executive contains the powers of the —Commander in Chief" and grants the President war powers, many facets of cyber security (defense against cyber-attacks) lie outside of the traditional definitions of war. War powers likely do not permit daily control of the nation's networks as they lay mostly in the hands of corporations and other private sector entities. Therefore, if the President, and by extension the federal government, is to defend the nation from cyber intrusions or attacks, there must be a

defined boundary of what falls under his authority as Commander in Chief and what does not.[1]

Before we explore national and international law on cyber attacks, we need to define what that and some related terms mean.

Defining the Terms

Since Congress has created statutes to govern computer and network crime (Title 18 of the United States Code, Section 1030), we are given legally enforceable definitions of what activities currently compose —cyber-crimes" within the jurisdiction of the United States. These currently cover areas such as computer fraud and abuse, identity theft, wire fraud, sexual exploitation of children, unlawful acts affecting commerce, fraud in connection with identification documents, authentication features, and information and fraud associated with access devices.[2]

Cyber attack and cyber war, however, are not so neatly defined in U.S. statutes. In fact, the terms of —Cyber war" and —Cyber attack" are often used interchangeably or are used to describe various computer crimes to include espionage. Place either of the terms in an internet search engine and the results will cover a broad spectrum from defacing social or corporate web pages to thievery to the clandestine collection of national security data. A good definition of cyber attack can be found in discussions of the Critical Infrastructures Protection Act (CIPA) of 2001: —All intentional attacks on a computer or computer network involving actions that are meant to disrupt, destroy, or deny information."[3] While this succinctly tells us the —What" of an attack, it cannot tell us the —Why"; it does not categorize the attack. How do we discern a cyber attack that is a crime from one that is an act of terrorism, or an act of war? The key factors are the

motivation and identity of the attacker and, to a lesser extent, the impact or result of the attack.

If the motivation of the attacker is monetary gain, destruction of property, or espionage, then a crime has been committed.[4] If the desired result is —to cause death or seriously bodily harm to civilians or non-combatants, with the purpose of intimidating a population or compelling a Government or an international organization to do or abstain from doing any act"[5] then an act of terrorism has occurred. If the motivation is to wage or to assist in waging an —armed hostile conflict between States or nations"[6], then an act of war has occurred.

We should note that a definition of —cyber attack" is not a matter of consensus. A RAND Project AIR FORCE study by Martin Libicki, for example, defines it as —The deliberate disruption or corruption by one state of a system of interest to another state".[7] This definition restricts cyber attacks to the realm of nation-states and would presumably use different terms to describe the same behavior and effects created by non-government activities. The RAND study's approach is that only actions that are possibly acts of war fall under this term and even excludes acts of espionage by nation-states from the term as —spying" does not fall under the usually accepted norms for causes of war.[8] This is too narrow of a definition for the purposes of this paper to use.

Furthermore, the CIPA definition does not include attacks where the goal is not to disrupt, destroy, or deny use of the information but to steal it (crime or espionage) or otherwise use it in an unlawful way. It is important to define —cyber attack" as a general concept that encompasses all of the activities listed above because the targeted organization of the attack often has no idea for some time what the purpose of the

attack is. It can take hours, days, weeks, or longer to determine the goal of the attacker. It can take even longer, if ever, to determine the attacker's identity.[9] Without knowing the purpose and identity, we cannot meet the RAND study or the CIPA definition and therefore could not use the term "cyber attack" to describe a cyber event.

Moreover, the word "attack" is used in non-cyber ways to include many non-military meanings. The commonly accepted usage of the word attack includes criminal, espionage, and terrorist activities in addition to military ones. People and Automated Teller Machines, for example, are attacked by criminals every day. Our nation's secrets are under attack by foreign intelligence services, and terrorists have attacked our embassies overseas and buildings within the U.S. Therefore, we will use the CIPA definition with a few additional words that will include acts of espionage and crime: "All intentional attacks on a computer or computer network involving actions that are meant to disrupt, destroy, deny, or unlawfully use information."

This broader definition will allow the full complexity of the prime question we are attempting to answer – namely how to discern whether a cyber attack is an act of war or not. Otherwise, the definition of the very word would always lead one to conclude "yes" since the definition also meets the parameters of an act of war – nation state involvement with the goal of destroying something of value.

Cyber war is defined by the RAND study as "A campaign of cyber attacks launched by one entity against a State and its society, primarily but not exclusively for the purpose of affecting the target State's behavior."[10] This definition allows for the attacker to be anyone, not just a nation-state. The target, however, is limited to nations. Since this paper is to assist U.S. Government policy makers, that definition will suffice.

It is important to note that cyber, like the other domains, may experience a war where most military actions are contained within the domain or it may contain a mere portion of the sum total of military actions. The closest analogy may be that of the air domain. Generally, airpower is used in support of land or sea domains but occasionally it is used almost exclusively in an air war, such as a no-fly zone.[11] Likewise, cyber war may be a component of an overall military effort or stand on its own.[12]

In either case, whether the act being evaluated is in a traditional domain or the cyber domain, the standard for determining if a *casus belli* exists should be the same. Nevertheless, a discussion regarding the characteristics of U.S. Cyberspace is important. A discussion of —US Cyberspace" should start with a definition of the Cyberspace Domain: —A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[13] U.S. Cyberspace can be then derived as that portion of the Cyberspace Domain that resides physically within US territory or under the ownership or authority of US government or citizens to include US organizations such as corporations or non-profits. This leads us to explore some of the characteristics of the cyber domain that make it operationally unique from the air, land, sea, and space domains.

Characteristics of the Cyber Domain

The National Military Strategy for Cyberspace Operations has an excellent discussion on features of the cyber domain.[14] We want to focus on just the factors in the cyber domain that make determinations regarding *casus belli* more difficult than in other domains. First, it is harder to maintain situational awareness in the cyber domain than in any other domain.[15] We generally have a good idea of what other States, and

many non-state actors, possess in terms of both offensive and defensive weapon systems in the space, air, sea, and land domains. Open source information such as Jane's (published by IHS, Inc.) document these capabilities for all but the most hidden of assets.[16] Not only are most current systems and their capabilities known, but so are many systems in development. Contrast that with the cyber domain. While categories of cyber weapons are generally known (see Table 1.),[17] the exact effect of each use of those weapons is unknown. It would be as if we knew about the submarines an opposing navy possessed but not the payloads of its torpedoes or missiles.

Type of Exploit	Description
Denial of service	A method of attack from a single source that denies system access to legitimate owners by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
Distributed denial of service	A variant of the denial of service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publically available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites – designed to look like those of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
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. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adapter that involves patrolling locations

	to gain unauthorized access
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no known fixes.

Table 1. Types of Cyber Weapons[18]

Second, a close watch is maintained on the intentions of the owners of those weapons in the other domains.[19] The U.S. maintains an extensive network of sensors in all domains to track deployment and employment of those weapons and the organizations that use and support them.[20] Both strategic and tactical surprises have occurred regarding intentions and uses but those are the exceptions rather than the rule.[21] Back to our analogy with the cyber domain, it would be as if we had some idea about the general (strategic) intentions of the owners of the submarines but little information on tactical intentions, and no idea of the submarine's specific locations to include their home ports. In short, determining a potential foe's intentions in the cyber domain is difficult.[22] Even after an attack is underway or completed, the intention of the attacker may not be known for hours or days or even longer.[23] The attack may have been an act of crime, espionage, terrorism or war.

Third, we have a fairly good idea of our shortcomings in our defenses in the other domains and try to compensate with a variety of tools to include alliances, adjusted techniques, tactics and procedures, or make plans accounting for the increased risk. We don't know what or where all of our vulnerabilities are in cyberspace.[24] Additionally, the vulnerabilities we are aware of often go unfixed and unmitigated for years. Adversaries intrude on our networks everyday using both known and unknown weaknesses.[25] The economic toll alone of these intrusions is significant. The estimated

loss to U.S. businesses due to cyber crime in 2008 was $42 billion.[26] According to DoD, —more than 100 foreign intelligence organizations are trying to break into U.S. networks."[27] Costs of repair due to military network intrusions attributed to China alone over a six month period exceed $100 million.[28]

Fourth is attribution of the attack. In the other four domains, either the direct observation of the attack or the analysis of physical evidence will usually determine who is responsible. Examples abound but the Chinese anti-satellite test in January 2007[29] and the North Korean sinking of the South Korean patrol boat Cheonan[30] both demonstrate the ability to accurately determine the method and source of attacks, even when the adversaries respectively initially remain silent or continuously deny culpability. This is much more difficult in the cyber domain. The Deputy Secretary of Defense, William Lynn, stated very succinctly —Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all."[31] Even when the attack can be tracked to a point of origin while the attack is taking place, often the computer or server being used is not in the same State as the attacker. A frequent tactic is to use Robot Networks or —botnets" – computer systems used for attacks unbeknown to their legitimate owners.[32] Due to a number of factors such as current technology, the way internet communicates, and the use of willing and unwilling third parties, attribution of an attack to a nation-state aggressor is extremely difficult.[33]

However, there is one more salient point regarding domain differences that must be made. Any State may attack any other State in space, air, land, or sea if it so chooses. If the State is willing to bear the cost of developing the force and using it, the

domain itself will usually permit it. This is not so with the cyber domain. Because of the low cost and current ease of attack in cyber, this statement may seem extremely odd. But attack in cyber is only possible because of vulnerabilities in the software code and the user's settings. Whoever gains illicit entry into a system only does so because a pathway exists. There is no such thing as a "forced entry" in cyberspace. A State and its inhabitants can only be attacked in the cyber domain if they allow it.[34] This fact is not lost on the Chinese who have undertaken an effort to secure their part of the internet with a unique operating system and designated choke points.[35] The U.S. Government also recognizes this which accounts for statements in the 2010 Quadrennial Defense Review like "DoD must actively defend its networks." Or "Joint Forces will secure the '.mil' domain" in the 2011 National Military Strategy. These observations lead us to explore the roles and responsibilities of defending U.S. Cyberspace.

Defending U.S. Cyberspace

The defense of the non .mil portion of U.S. Cyberspace is primarily the responsibility of civilian agencies and private entities. The Department of Homeland Security has the lead but is supported by the Department of Justice, the intelligence community, and others. Corporations are responsible for their own security but are encouraged to coordinate and cooperate with the government. It is worth noting the only entity that can take offensive actions (armed force) is the government. Private citizens, corporations, etc. are not authorized to stage cyber attacks of their own – not even in retaliation.[36]

A review of current United States Code gives a glimpse of the division of roles and legal responsibilities within the United States Cyberspace. (See Table 2.) This fractionalization of cyber defense creates a situation where no military service has

primary responsibility for the domain – unlike all of the other domains. A plans officer pointed out that if we used this scheme of defense in land warfare, an —invasion of New Jersey would have to be fought by U.S. citizens and commercial entities with whatever weapons they happened to possess. DoD would only defend Ft. Monmouth and Dix."[37]

US Code	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	Domestic Security	Homeland Security	Department of Homeland Security	Security of US Cyberspace
Title 10	Armed Forces	National Defense	DoD	Secure US Interests by Conducting Military Operations in cyberspace
Title 18	Crimes and Criminal Procedure	Law Enforcement	Department of Justice	Crime Prevention, Apprehension, and Prosecution of Cyberspace Criminals
Title 32	National Guard	First Line Defense of the United States	Army National Guard, Air National Guard	Support Defense of US Interests Through Critical Infrastructure Protection, Domestic Consequence Management and Other Homeland Defense-Related Activities
Title 40	Public Buildings, Property, and Works	Chief Information Officer roles and Responsibilities	All Federal Departments and Agencies	Establish and Enforce Standards for Acquisition and Security of Information Technologies
Title 50	War and National Defense	Foreign Intelligence and Counter-Intelligence Activities	Intelligence Community Aligned Under the Office of the Director of National Intelligence	Intelligence Gathering Through Cyberspace on Foreign Intentions, Operations, and Capabilities

Table 2. Cyber Roles[38]

The ability to respond to an act of war, however, resides exclusively with the government of the United States. To date, however, this has not been well defined for the cyber domain. The 2001 Authorization for Use of Military Force, passed by

Congress in the wake of the 9/11 attacks, does seem to grant the President some authority to conduct cyber defense efforts against cyber terrorism.[39] However, it contained little guidance regarding acts of war within the cyber domain. What can or cannot be done in the name of national defense by the executive branch then depends greatly upon this connection to the Presidents' war powers.[40] This is another reason why an understanding of what constitutes an act of war in and out of the cyber domain is important.

Of course, defining what the military is allowed to do in the construct of defending the cyber domain is greatly impacted by this understanding as well. A great deal of effort has gone into creating organizations, doctrine, and tools to defend military networks. When can the military use this expertise to help defend the nation's networks in general? During a war of course, but under what conditions is a cyber attack an act of war? As you can see, the answer to this question is no longer of interest to just legal philosophers or War College professors.

Secretary of Defense Robert Gates acknowledged that the nation's dependence on cyberspace represented a new element of risk to our national security. To address this risk and to synchronize "warfighting effects" in cyberspace, he created the U.S. Cyber Command under U.S. Strategic Command. Cyber Command is now responsible for U.S. military cyberspace operations and provides support to domestic civil authorities and international allies. [41]

The President's direction is found in the May 2010 NSS: "We will work with all the key players— including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and

unified response to future cyber incidents. Just as we do for natural disasters, we have to have plans and resources in place beforehand."[42] This is a tall order considering that no one is completely sure where the boundaries lie between all of the agencies and levels of government. How can they? The cyber domain is characterized by a lack of boundaries. A fictional but very realistic example: Data stored on servers in Holland is used by engineers in the United States to research where the next oil well should be drilled in waters off the Nigerian coast. This research is then hacked by someone using an IP address assigned to a university in Russia and later a Chinese joint venture bids on the Nigerian oil lease drilling project with what appears to be the U.S. engineer's estimates. Was this a crime, an act of espionage, a threat to national security or all three? Who has the authority to defend against the attack, investigate the theft of data, and determine the culpability of any alleged parties to the attack? How does any one agency determine these answers?

Work done by James Michael and George Mason University has resulted in the creation of a decision matrix that helps organizations respond to cyber-attacks in a legally appropriate way.[43] The model breaks all cyber intrusions into one of three legal paradigms or categories: Law Enforcement governed by the U.S. Constitution and Titles 18 and 15 of the USC, Intelligence Collection governed by Title 50 USC and Executive Order 12333, or Military Operations governed by Title 10 USC. While the matrix is extraordinarily useful as a tool for determining what the legal rules are before conducting a response to a cyber-attack, James Michael openly admits that the answers to the questions of who is conducting the attack and why are critical but are often unavailable, especially during and in the immediate aftermath of the attack.[44] This

leaves us with the practical problem of who has the responsibility to make the decision regarding who responds to the cyber-attack.

Who Determines Acts of War?

Declaring that an act of war has occurred is not the same as declaring that a crime has taken place. In the event of a serious crime in the United States, police officers collect the evidence which is then often evaluated by detectives and technical experts. Suspects are identified, pursued, and arrested. The results of the investigation are delivered to the prosecutor who, after review, may file charges in a court of law. A judge determines if there is sufficient evidence to warrant a trial. If so, a trial occurs with a presentation of evidence before a judge and a jury of citizens who determine if guilt has been established beyond a reasonable doubt.[45]

Declaring that an act of war has taken place contains few of these elements. Some acts of war are investigated such as the Gulf of Tonkin (1965) or the 9/11 attacks (2001). Most do not require it as the facts on the ground make the action obvious such as Iraq's invasion of Kuwait (1990), Japan's bombing of Pearl Harbor (1941), and the North Korean invasion of South Korea (1950). Regardless if there is a formal investigation or not, who are these facts delivered to? What court has the authority to authorize a war? What jury determines if the alleged act has actually taken place and the suspected party is guilty beyond a reasonable doubt? What judge determines the punishment of the guilty party and using what guidelines? Who is to carry out the sentence?

The answers are that no court system or international mechanism exists to fill these roles. While some may point to the United Nations General Assembly and Security Council as sources of authority to conduct a war, these are political bodies and

not judicial ones.[46] Facts are presented to the court of public opinion (national and international), and nations take it upon themselves to carry out whatever sentence they feel is appropriate and capable of carrying out.[47]

So we return to the critical question of how to determine if a cyber-attack is an act of war or not. No international court will make the determination for us and the costs of getting it wrong can be severe. The mistaken belief that the U.S. Navy had been deliberately attacked a second time in the Gulf of Tonkin in 1965 provided the spark for the U.S. Senate passing a resolution approving the use of force against North Vietnam. While not the only factor causing the war, it was the galvanizing moment that authorized the President to send hundreds of thousands of American serviceman into combat.[48] The outcome, eight years later, was the waste of over 58,000 U.S. lives and 150 billion dollars.[49]

Multiply the confusion of that night in the China Sea on 4 August 1965 by a magnitude of 10 and one begins to approximate the difficulty of making decisions regarding acts of war in the cyber domain. We must depend on international norms, conventions, and laws to assist us in that determination. Perhaps the most relevant document regarding acts of war with the widest acceptance among the nations of the world is the Charter of the United Nations.

International Law

It is essential to understand that the UN Charter does not prohibit the use of force. It does, however, prohibit the use of aggressive force.[50] There are four articles that bring light to this issue. The first, appropriately enough, is Article 1 as it enumerates the purposes of the United Nations (UN).

> To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;[51]

Even though this article does not mention war or even the use of force between nations, it has relevance. The member nations established the UN to maintain international peace. It makes the avoidance of, or failing that, resolution of breaches of the peace the primary purpose of the UN. If we construe cyber attacks as a breach of the peace, they then fall under the purview of the UN and its charter. Recalling from earlier the economic impact of cyber attacks on the U.S. alone, it is a fair assessment to state that peace has been breached.

The next Charter article of interest is Article 2(4). It states that –All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state . . .”[52] It is noteworthy that this article offers no mechanism of relief from an aggressor. It does not authorize defense, retaliation, or any other response to force against your State. It merely prohibits force against another State.[53]

So is a cyber attack considered a use of force? We need to be careful in our response as this is a double edged sword. If someone is attacking the U.S. the temptation is to swiftly answer –yes”. However, a finding that cyber attacks are indeed considered a use of force then the U.S. is forbidden from engaging in that activity itself under this article. To provide an answer to this question we must first understand what the UN Charter means by –force”. Is it any kind of force such as diplomatic, economic, and military or is it just military (armed) force?

Michael N. Schmitt, a professor of International Law and former Air Force Judge Advocate published a research paper on this issue for the United States Air Force Academy's Institute for Information Technology in 1999. His analysis of UN documents, including minutes of the original 1947 meetings, as well as follow-on General Assembly Resolutions, other international treaties, and customary international law, concluded the term "force" under current international law most closely means "armed force" and not diplomatic, informational, or economic.[54] Other legal scholars concur in this interpretation, one using the term "aggressive force" in lieu of "armed force" but with a similar conclusion to Schmitt's.[55]

So now we modify our question to this: Is a cyber attack considered a use of armed force? We turn to Article 41 of the Charter which delineates all of the actions member nations may take against an aggressor nation that do not involve armed force. These actions include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[56] This indicates that at least some forms of cyber attack do NOT fall into the description of armed force – particularly the denial of service attack. The ramification of this is the U.S. could employ this form of cyber attack to temporarily block access to a website that posed a threat to U.S. interests without crossing the Article 2(4) prohibition of the use of force. Of course, that enables others to do the same to the U.S.

We cannot, however, state unequivocally that all forms of cyber attack have been eliminated from the "armed force" category. For example, any cyber attack that aims to kill or injure people or cause damage to physical property clearly is a use of armed

force.[57] This is exactly what many experts and policy makers are concerned about when they discuss Critical Infrastructure Protection (CIP) and Supervisory Control and Data Acquisition (SCADA) systems. A well executed cyber attack that is able to gain control of the system or the data it uses to control critical infrastructure (such as an electrical power grid, locks or gates of a dam, water supply system, transportation system) could quite easily cause widespread destruction and human fatalities.[58]

This is not a theoretical discussion – an incident of computer warfare from the Cold War demonstrates what armed force looks like when executed against critical infrastructure via software code. A former director of the National Reconnaissance Office, Thomas Reed, recounts the following incident from 1981 in his memoirs. The Soviets were years behind the West in computer technology. They had a desperate need to obtain hardware and software that could regulate natural gas as it was shipped from the fields to storage to pipelines and into Eastern Europe. Because this was a significant source of income for the Soviets, the KGB was tasked to steal the relevant software from a Canadian company. Tipped off by the French, the U.S. and Canada modified the software before the KGB "acquired" it.

> Once in the Soviet Union, computers and software, working together, ran the pipeline beautifully – for a while. But that tranquility was deceptive. Buried in the stolen Canadian goods – the software operating this whole new pipeline system – was a Trojan Horse. (An expression describing a few lines of software, buried in the normal operating system, that will cause that system to go berserk at some future date or upon the receipt of some outside message.) In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space. At the White House, we received warning from our infrared satellites of some bizarre event out in

> the middle of Soviet nowhere. NORAD feared a missile liftoff from a place where no rockets were known to be based.[59]

This manipulation of the SCADA was not accomplished by means of a cyber attack but it clearly demonstrates the potential result from the insertion of malware via the internet. Had the trojan horse been delivered through a cyber attack, it clearly would have been an armed force and, possibly, a *casus belli*. In other instances of malware infecting a control system, the end result was not nearly so dramatic. So it is not the method of cyber attack that matters but rather the direct result of that attack.

We are beginning to develop some boundaries as to when a cyber attack meets the definition of armed force. Clearly some types of attack meet the definition while others do not. Before we further delineate which ones do, we need to examine one last article, Article 51: —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. . .”[60]

This article grants member nations the right to defend themselves using all means necessary – including armed force. Once the State is attacked, it may respond with its own attacks against the aggressor without violating the UN Charter. This raises the ante in defining cyber attacks as armed force as that will enable an armed force response. There is no restriction in Article 51 as the type of attacks undertaken in self-defense. While proportionality is generally expected, the response does not have to be symmetrical. Forces in any domain may be used separately or together – the defense is not limited to the cyber domain.

It is clear that a State or the UN Security Council should take great care in labeling a cyber attack as something that amounts to an armed force. The situation

could escalate to the level of an international crisis and possibly degenerate into armed conflict across the spectrum of domains. This is assuming that a clear and convincing case of attribution can even be made in the first place. As discussed earlier, finding the true culprit in a cyber attack is far more difficult than in the other domains. We should also note that espionage is considered a crime, not a use of armed force. Planting a trojan horse that extracts data is a cyber attack and punishable as a felony but it is not armed force or an act of war.[61]

In 1999, Schmitt made the observation that the UN Charter specifically forbids the use of armed force in most situations (permitted in self-defense and when the Security Council authorizes it to end a breach of the peace). But it intentionally excludes from this prohibition the use of coercive force types listed in Article 41. If economic and political coercion are not considered armed force then we have additional criteria to determine whether a cyber attack's effects cross the line of demarcation between a crime and armed force.[62]

Further refinement of that line requires additional criteria. It is time to introduce Dr. Schmitt's analysis and seven factors and then we will use them in a brief case study of events in Estonia in 2007.

Schmitt's Analysis

Schmitt's 1999 analysis was updated in 2010 and delineated seven factors that can guide a State to define whether or not a cyber attack meets definition of a use of force.[63] While there is a lack of consensus in this area,[64] his criteria provide an admittedly subjective framework to evaluate the cyber action as a potential *casus belli*. The factors are: Severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[65]

Severity is exactly what it sounds like – how significant were the effects of the attack? As discussed above, a denial of service attack is not going to meet the standard of armed force but a disaster like the Soviet gas pipeline explosion could. There must be harm to individuals and property. The degree to which the attack impacts the nation in terms of economic cost, societal cost, and length of time will affect the calculation of severity.[66]

Immediacy reflects the concern about the rapidity of consequences from the attack. An economic embargo, for example, has consequences that build slowly over time, allowing the affected State to make rational choices on how to avoid further harm. A cyber attack that has a similar effect would not qualify as an armed force. However, one that had immediate significant and severe effects could.[67]

Directness measures the connectivity between the initial act and the result. Again, to use the embargo as example, the eventual consequences of deprivation of a particular good are impacted by other market forces as well as innovation to replace the good. An armed attack, in contrast, results in direct harm to people and property.[68]

Invasiveness addresses the degree to which the aggressor has penetrated the State‘s sovereignty. The economic embargo entails no penetration, an air raid or land invasion involves the other extreme. The deeper the cyber attack resides within US Cyberspace, the greater the invasive aspect, the greater the violation of sovereignty.[69]

Measurability concerns how well and accurately the State can quantify the damage it has suffered as a result of the attack. If it is difficult to point out visible damage in terms of destruction and death, then the State will find proving the negative consequences to the world community be difficult.[70]

Presumptive Legitimacy reflects the state of international law regarding permissive actions by States. In short, if it is not prohibited, it is presumed to be legitimate. Since international law —does not prohibit propaganda, psychological warfare, or espionage" those activities in the cyber domain are presumed to be legitimate.[71]

Responsibility addresses the level to which the aggressor State was involved in the cyber attack. This is directly related to problem of attribution mentioned above. The closer the victim State can tie the attack to the aggressor State, the more likely the cyber attack will be recognized by the international community as a prohibited armed attack.[72]

Now that we have defined Schmitt's seven factors, let's apply them to a real world situation and make a decision as to whether it was an act of war or not.

Applying the Schmitt Analysis - Estonia

Examining a historical example of a cyber attack may be the best way to illustrate how these criteria can be used to make a determination as whether a *casus belli* exists or not. On April 26, 2007, the Estonian government moved a World War II Soviet Army memorial out of the center of Tallinn, the capital city. This move was seen as anti-Russian and was extremely unpopular with the Russian public and ethnic Russians living in Estonia. The cyber attacks began on April 27 and lasted for three weeks. The attacks were primarily distributed denial of service attacks and disrupted banking, government communications, and e-mail services. Estonian news media, universities, and other government agencies were all victims of the attacks. Web defacement also occurred on official government websites.[73]

Although the sources of most of the attacks were from Russia, the Russian government denied responsibility. Despite accusations from the Estonian government, intense post attack investigations have yet to demonstrate a connection with the Russian government. One individual was identified, charged and convicted under Estonian law but the many others involved have escaped retribution.[74] So was this attack a use of armed force? Did the cyber attacks cross the line and become an act of war?

Using the Schmitt analysis, this author unequivocally believes that the answer is no because of a lack physical damage or death. Ironically, Schmitt himself wrote in a 2010 article that he believes the answer could be yes for the reason that the attacks frustrated Estonian government and economic functions. [75] While it is slightly intimidating to disagree with a renowned expert on this subject, let's go through the factors:

Severity – while the 3 week length of time is considerable (especially for a cyber attack), there were no facilities destroyed or lives lost. Admittedly the annoyance factor was extremely high and many citizens' lives and businesses were significantly impacted but no permanent damage was done.[76] As Schmitt himself points out, this is the most significant of the seven factors and —consequences involving physical harm to individuals or property will alone amount to a use of force."[77] Since physical harm did not occur, ergo no use of force occurred and no *casus belli*.

Immediacy – the attacks occurred without warning and less than 24 hours after the protested action (removal of the statue) took place. The effects of the attacks occurred with great rapidity.[78]

Directness – it was quite clear that the negative effects of the attacks – loss of communications, etc. were directly caused by the cyber attacks and were not enhanced by indirect factors.

Invasiveness – the cyber attacks were definitely within Estonian Cyberspace. The attacks clearly originated outside of the State and were flowing through Estonian servers and communications circuits. Proof of this was provided when Estonia cut all international data circuits coming into the country and nearly all cyber attack activity immediately halted.[79]

Measurability – While economic harm can be somewhat quantified it is important to recall from our discussion above that economic coercion is not seen as a use of armed force by the UN. Schmitt himself agrees that this is the case —even though it (economic coercion) may cause significant suffering."[80]

Presumptive Legitimacy – Since propaganda, psychological warfare, and espionage are not considered prohibited forces under international law – we must examine the actual effects of the attacks upon Estonia. Web defacement is a form of propaganda; interruption of the mail and communications are not considered armed force by Article 41 of the UN Charter, and the continuous denial of access to these functions is a form of psychological warfare. While the conduct was criminal, it was not necessarily a use of armed force.[81]

Responsibility – While a connection to the Russian government has not been proven, even if it was, the cyber attacks simply do not rise to the definition of armed force. If this was a State sponsored action, it would have certainly brought the declaration of a breach of the peace, but without physical injury or destruction of

physical property, there is no armed force and thus no *casus belli*. It is also worth noting that although Estonia is a member of NATO, Article 5 of the North Atlantic Treaty (common defense of a member against an armed attack) was never invoked.[82]

We could repeat this exercise for any number of cyber incidents such as the Stuxnet Worm that damaged Iran's centrifuge machines that enrich uranium[83] or the cyber attacks that accompanied the very kinetic land/air attacks in Georgia in 2008.[84] In each case we would derive a valid, even if subjective, answer. The seven factors of Schmitt's analysis can provide an answer to that ever elusive question: When is a cyber attack an actual act of war? We now turn to what we should do with this information in the form of some recommendations to the U.S. Government and a conclusion.

Recommendations

Based on the preceding discussion and analysis, the United States Government should adopt the seven factors of Schmitt's Analysis to evaluate the impact of cyber attacks upon U.S. Cyberspace to determine if a *casus belli* exists. Furthermore, if an offensive cyber action is considered, Schmitt's analysis should also be conducted to determine if U.S. actions would constitute an armed attack under the UN Charter.

First, the Schmitt Analysis should be structured into a matrix with as many objective criteria inserted as possible to improve the rapidity and accuracy of decisions being made based on the seven factors. Each of the factors need to be refined with guidance and examples that narrow the level of interpretation required as to whether the cyber activity in question crosses or does not cross the line of armed force. While the analysis is ultimately subjective, the more objective it can be made, the higher the fidelity of advice based on the model will be.

Second, the analysis needs to be included or referenced in a number of documents to become the framework that all government agencies reference when making recommendations. The National Strategy to Secure Cyberspace and the Comprehensive National Cybersecurity Initiative both affect multiple agencies across the government and should be updated with the analysis. One of the primary Department of Defense documents that should also reflect this change is the National Military Strategy for Cyberspace Operations (NMS CO). Changes to derivative documents like the NMS CO implementation plan, the USSTRATCOM Campaign Plan and the USCYBERCOM OPORD will bring the analysis to the operational levels of DOD. Based on the guidance contained in these documents, the Judge Advocate General (JAG) Corp will need to recommend amendments to the Standing Rules of Engagement (SROE) and any specific ROE that are currently being used in support of cyber operations. The need for this was reflected in a statement to Congress by the USCYBERCOM Commander, General Keith Alexander, in November 2010. He confirmed that there are still ~~no~~ clear rules of engagement clarifying what cyber activity might trigger an armed cyber response from the U.S."[85]

Finally, all military and civilian agency leaders who are charged with taking actions in cyberspace or will be advising the President regarding acts of war in cyberspace must be made familiar with the Schmitt Analysis. Even though opinions will vary among government leaders, having a common set of criteria to work with will standardize the reference terms, concepts, and understanding of the issues involved and will aid in rapid decision making.

Conclusion

This paper addressed the need to determine if a cyber attack is a crime or act of war. It defined the terms of cyber attack and cyber war in such a way to support the idea that all attacks are not a *casus belli* but include a wide array of actions such as terrorism, espionage, and more mundane crimes such as fraud. Characteristics of the cyber domain make situational awareness and attribution of attacks difficult. Though we are aware of the standard tools of cyber attacks, we are still plagued with vulnerabilities in cyberspace that are taken advantage of by criminals and adversaries.

A review of the statutory guidance revealed that each type of cyber attack is dealt with by a different agency within the government, even though during the attack, no one may be aware of which type of event it is. Indeed, the initial detection and notification is likely to be by private entities such as corporations. Regardless of what damage has occurred to whom, only the President as Commander-in-Chief may authorize the use of force in retaliation. But he has to be advised as to what types of force in the cyber domain are considered —armed force".

A review of international law revealed that cyber attacks can rise to the level of an armed force and thus be a *casus belli*. The seven factors contained within Michael Schmitt's analysis are a viable framework for helping decision makers reach that determination.

The vast majority of cyber attacks occurring against and within U.S. Cyberspace are criminal acts or espionage. But for those few events, either current or in the future, that has the characteristics of an armed force, recommendations and courses of action will need to be provided to the President in his Commander-in-Chief role. The

foundation of those recommendations must be as firm as possible and the Schmitt Analysis provides a method to do that.

Endnotes

[1]John Rollins and Anna Henning, ―Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations" (Washington, DC: Congressional Research Service, March 10, 2009), 8-15.

[2] U.S. Government Accountability Office, *CYBERCRIME: Report to Congressional Requesters* (Washington, DC: U.S. Government Accountability Office, June 2007), 12.

[3] Jeffrey F. Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition* (Tucson, AZ: Lawyers and Judges Publishing Inc., 2009) 311.

[4] Ibid., 318

[5] Ibid. Addicott is quoting the United Nations Secretary General, Kofi Annan, in 2005 defining terrorism.

[6] Merriam Webster Dictionary

[7] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Arlington, VA: RAND Corporation, 2009), 23

[8] Ibid.

[9] Ibid., 43-46.

[10] Ibid., 117.

[11] U.S. Department of the Air Force, *Air Force Basic Doctrine*, Air Force Doctrine Document 1 (Washington, DC: U.S. Department of the Air Force, November 17, 2003), 36-37.

[12] Peter Pace, *The National Military Strategy for Cyberspace Operations (Redacted)* (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006), 3.

[13] Ibid., ix.

[14] Ibid., 3-5

[15] U.S. Department of the Air Force, *Cyberspace Operations*, Air Force Doctrine Document 3-12 (Washington, DC: U.S. Department of the Air Force, July 15, 2010), 7.

[16] IHS Jane's, ―Jane's Defense Equipment and Solutions," http://www.janes.com/products/janes/defence/index.aspx (accessed January 9. 2011)

[17] U.S. Government Accountability Office, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance* (Washington, DC: U.S. Government Accountability Office, July 2010), 5.

[18] Ibid.

[19] Richard B. Porterfield, "Naval Intelligence: Transforming to Meet the Threat," *United States Naval Institute Proceedings*, (September 1, 2005): 13-14

[20] U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01 (Washington, DC: U.S. Joint Chiefs of Staff, October 7, 2004), I3 - I7.

[21] Mark M. Lowenthal, *Intelligence: From Secrets to Policy,* 4th ed. (Washington, DC: CQ Press, 2009), 2-3.

[22] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in Proceedings of a Workshop on Deterring Cyberattacks (Washington, DC: The National Academies Press, 2010): 168.

[23] George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), viii.

[24] House Permanent Select Committee on Intelligence, *Cyber Security: Hearing on the Nation's Cyber Security Risks*, 110th Cong. (September 18, 2008) (Statement of Paul Kurtz, Former Senior Director, Critical Infrastructure Protection, White House Homeland Security Council).

[25] Senators Sheldon Whitehouse, Barbara Mikulski, and Olympia Snowe, "Cyber Self-Defense Can Help U.S. Security," September 3, 2010, http://www.cnn.com/2010/ OPINION/09/03/senators.cyber.security/index.html?hpt=C2 (accessed September 3, 2010). The senators are members of the Senate Intelligence Committee and were making comments on an unclassified key finding from a classified study on cybersecurity.

[26] Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence,* (Washington, DC: Director of National Intelligence, February 25, 2009).

[27] William Lynn, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September/October 2010): 99.

[28] "2009 Report to Congress of the US-China Economic and Security Review Commission," (Washington, DC: US Government Printing Office, November 2009), 167-180, quoted in U.S. Army War College, *Information Operations Primer,* FY11 ed. (Carlisle Barracks, PA: U.S. Army War College, November 2010), 21

[29] Shirley Kan, "China's Anti-Satellite Weapon Test," (Washington, DC: Congressional Research Service, April 23, 2007), 1-3.

[30] IHS Jane's, "Seoul Reacts to North Korean Cheonan Attack," http://www.janes.com/products/janes/defence-security-report.aspx?ID=1065927927 (accessed January 9, 2011)

[31] Lynn, "Defending a New Domain," 99.

[32] Whitehouse, "Cyber Self-Defense Can Help U.S. Security,"

[33] David M. Hollis, "USCYBERCOM, The Need for a Combatant Command versus a Subunified Command," *Joint Force Quarterly* 58 (3rd Quarter 2010): 50.

[34] Libecki, *Cyberdetterence and Cyberwar*, xiii

[35] Brian M. Mazanec, "The Art of (Cyber) War," *Journal of International Security Affairs* no. 16 (Spring 2009): 81-90

[36] Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 340.

[37] Hollis, "USCYBERCOM, The Need for a Combatant Command versus a Subunified Command, 50.

[38] Pace, *The National Military Strategy for Cyberspace Operations (Redacted)*, A1.

[39] Rollins and Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations", 12-13.

[40] Rollins and Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations", 11.

[41] U.S Secretary of Defense Robert Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," Memorandum for Secretaries of the Military Departments, Washington DC, June 23, 2009.

[42] Barrack Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27

[43] Leisheng Peng, University of Malaga, Spain, Duminda Wijesekera, University of Malaga, Spain, Thomas C. Wingfield, University of Malaga, Spain, and James B. Michael, University of Malaga, Spain. 2006. An ontology-based distributed whiteboard to determine legal responses to online cyber attacks. Internet Research 16, no. 5, (October 20): 475-490. http://www.proquest.com.ezproxy.usawcpubs.org/ (accessed December 8, 2010).

[44] Ibid.

[45] Oklahoma Assistant District Attorney Michelle Bodine-Keely, interview by author, Tulsa, OK, January 2, 2011.

[46] A. LeRoy Bennett, *International Organizations*, 2nd ed. (Englewood Cliffs, NJ: Prentice-Hall, 1980), 54-60

[47] Ibid., 5-9.

[48] George C. Herring, *America's Longest War*, 4th ed. (New York: McGraw-Hill, 2002), 142-145

[49] Ibid., xi

[50]Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 341.

[51] United Nations Charter, Article 1.

[52] United Nations Charter, Article 2(4).

[53] Michael N. Schmitt, ―Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *The Columbia Journal of Transnational Law* 37 (1999): 900.

[54] Schmitt, ―Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 900-908.

[55] Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 340-342.

[56] United Nations Charter, Article 41.

[57] Schmitt, ―Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 913.

[58] Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 312-314.

[59] Thomas C. Reed, *At the Abyss, An Insider's History of the Cold War*, (New York: Ballantine Books, 2004), 268.

[60] United Nations Charter, Article 51.

[61] Schmitt, ―Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156.

[62] Schmitt, ―Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 912-914.

[63] Schmitt, ―Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156-157.

[64] United States Army War College, *Information Operations Primer – AY 11 Edition*, (Carlisle Barracks, PA: U.S. Army War College, November, 2010), 24.

[65] Schmitt, ―Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156-157.

[66] Ibid.

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Ibid.

[73] Jason Richards, ―Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, April 4, 2009, http://www.iar-gwu.org/node/65 (accessed August 10, 2010), 1-5.

[74] Ibid.

[75] Schmitt, ―Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156-157.

[76] Ibid.

[77] Ibid.

[78] Richards, ―Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," 3.

[79] Ibid., 4.

[80] Schmitt, ―Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156

[81] Ibid.

[82] Kenneth Geers, *Cyberspace and the Changing Nature of Warfare*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2008), 7.

[83] Pascal Mallet, ―Emergence of Stuxnet Worm Highlights Cyber Warfare," *Defense News*, October 1, 2010, http://www.defensenews.com/story.php?i=4824625 (accessed October 20, 2010)

[84] Paul A. Matus, *Strategic Impact of Cyber Warfare Rules for the United States*, Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, 25 March 2010), 18-22.

[85] Joseph Menn, ―Rules of Engagement for Cyberwars See Slow Progress," *Financial Times*, December 29, 2010, http://ebird.osd.mil/ebfiles/e20101229797273.html (accessed December 29, 2010)