Strategy Research Project

DEFINING AND DETERRING CYBER WAR

BY

LIEUTENANT COLONEL SCOTT W. BEIDLEMAN
United States Air Force

USAWC CLASS OF 2009

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)*
06-01-2009	Strategy Research Project	

4. TITLE AND SUBTITLE

Defining and Deterring Cyber War

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Scott W. Beidleman

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Colonel Blane R. Clark
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

Since the advent of the Internet in the 1990s, not all users have acted in cyberspace for peaceful purposes. In fact, the threat and impact of attack in and through cyberspace has continuously grown to the extent that cyberspace has emerged as a setting for war on par with land, sea, air, and space, with increasing potential to damage the national security of states, as illustrated by attacks on Estonia and Georgia. Roughly a decade after the advent of the Internet, the international community still has no codified, sanctioned body of norms to govern state action in cyberspace. Such a body of norms, or regime, must be established to deter aggression in cyberspace. This project explores the potential for cyber attack to cause exceptionally grave damage to a state's national security, and examines cyber attack as an act of war. The paper examines efforts to apply existing international norms to cyberspace and also assesses how traditional concepts of deterrence apply in cyberspace. The project concludes that cyber attack, under certain conditions, must be treated as an act of war, that deterrence works to dissuade cyber aggression, and provides recommendations to protect American national interests.

15. SUBJECT TERMS

Cyber Attack, International Law, Deterrence

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Beidleman, Scott W.
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	36	717-249-1387

USAWC STRATEGY RESEARCH PROJECT

DEFINING AND DETERRING CYBER WAR

by

Lieutenant Colonel Scott W. Beidleman
United States Air Force

Colonel Blane R. Clark
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 Scott W. Beidleman

TITLE: Defining and Deterring Cyber War

FORMAT: Strategy Research Project

DATE: 06 January 2009 WORD COUNT: 6,746 PAGES: 36

KEY TERMS: Cyber Attack, International Law, Deterrence

CLASSIFICATION: Unclassified

Since the advent of the Internet in the 1990s, not all users have acted in cyberspace for peaceful purposes. In fact, the threat and impact of attack in and through cyberspace has continuously grown to the extent that cyberspace has emerged as a setting for war on par with land, sea, air, and space, with increasing potential to damage the national security of states, as illustrated by attacks on Estonia and Georgia. Roughly a decade after the advent of the Internet, the international community still has no codified, sanctioned body of norms to govern state action in cyberspace. Such a body of norms, or regime, must be established to deter aggression in cyberspace. This project explores the potential for cyber attack to cause exceptionally grave damage to a state's national security, and examines cyber attack as an act of war. The paper examines efforts to apply existing international norms to cyberspace and also assesses how traditional concepts of deterrence apply in cyberspace. The project concludes that cyber attack, under certain conditions, must be treated as an act of war, that deterrence works to dissuade cyber aggression, and provides recommendations to protect American national interests.

DEFINING AND DETERRING CYBER WAR

> Cyberspace is the nervous system—the control system of our country.
>
> —President George W. Bush [1]

What if one day the control systems of a major dam suddenly released torrents of water upon nearby communities, or safety systems of nuclear power plants malfunctioned, or air traffic control systems of major airports shut down, or financial transactions of major banks and stock exchanges stopped or disappeared? What if this happened simultaneously? Is this the plot of a Hollywood blockbuster, or the new reality of twenty-first century cyber war?

Since the public debut of the Internet in the early 1990s, not all users have acted in cyberspace for peaceful purposes. The magnitude and frequency of cyber attacks have continuously grown since the inception of the World Wide Web, from the nuisance of individual hackers in the early years to the recent potentially state-sponsored cyber aggression against Estonia and Georgia. Indeed, cyberspace has emerged as a setting for war on par with land, sea, air, and space. This is notably unsettling since the Internet and information and communications technologies (ICT) have become fully integrated into all aspects of human society. In fact, computers control much of America's critical infrastructure and essential processes in manufacturing, utilities, banking, and communications.[2] Even President Bush declared cyberspace as America's nervous system and the control system of the country.[3] Cyberspace is America's operating system, analogous to a national-level Windows XP™. A system crash would cause grave damage to the economy and national security; rebooting America might not be easy. Consequently, this paper asserts that cyber attacks can

cause potentially grave damage to the national security of the United States and must be treated as an act of war. As a first line of deterrence in this relatively new domain of war, the United States should lead efforts to establish an international regime of laws, norms, and definitions to deter aggression in cyberspace.

The question of cyber deterrence reveals several more fundamental questions, upon which the international community has not reached consensus. Does cyber attack constitute a use of force? Is it an act of war? Do the traditional concepts of deterrence prevail in cyberspace? These questions are difficult to answer because there are no common, codified, legal standards regarding cyber aggression. More than a decade after the advent of the Internet, the international community still has no sanctioned body of norms to constrain states' actions in cyberspace.

This paper begins by examining the increasing scope and destructiveness of cyber attacks and establishes cyber war as a threat to the national interests of the United States. Next, it defines cyber war and attempts to assess cyber attack as an act of war regarding current international law. Then the study applies the traditional concepts of deterrence to cyberspace and concludes with recommendations. The research concludes that deterrence can work in cyberspace, but the United States must pursue a comprehensive approach that combines the fielding of defensive and offensive cyber capabilities with a concerted effort to establish an international regime to constrain cyber aggression.

A Threat to National Security

Since its arrival as a public domain in the 1990s, the Internet and ICT have become fully integrated into all aspects of human society. Advances in ICT

continuously fuel globalization, which increases the interdependence of states' economies, politics, and security. Concurrently, it increases states' vulnerability to cyber attack. Like any other medium, cyberspace is an avenue to pursue peaceful ends as well as aggression.

One of the earliest attacks in cyberspace to gain notoriety occurred in 1994 at Rome Lab, a military research and development laboratory. Two hackers intruded into the lab's network 150 times but caused no damage.[4] One of the hackers from Israel was acquitted because no Israeli laws applied to the incident.[5] A few years later the Love Bug virus infected over 60 million computers worldwide and caused organizations as diverse as the British Parliament and the Ford Motor Company to shut down their servers.[6] Again, the Filipino perpetrator was not charged or punished because "creating computer viruses was not a crime under Philippine law."[7]

In 1997, the U.S. military conducted Eligible Receiver, the nation's first-ever information warfare exercise. This exercise tasked a group of highly trained, computer experts, known as a government red team, to independently examine plans and operations from the perspective of adversaries.[8] The red team "was able to infiltrate and take control of Pacific command center computers, as well as power grids and 911 systems in nine major U.S. cities."[9] These results suggested that America's critical military and civilian infrastructures were highly vulnerable. In fact, the very next year hackers confirmed the findings of Eligible Receiver when they attacked Department of Defense networks and compromised over 500 computers in the incident dubbed "Solar Sunrise."[10] This attack targeted logistics and accounting systems essential to managing and deploying U.S. military forces at a time when the U.S. was considering military

action against Iraq for failing to comply with UN resolutions.[11] These events served as signs of things to come as smaller-scale hacker-level assaults gave way to much more organized and destructive attacks, culminating in reputed state-level attacks on Estonia and Georgia.

Since Estonia declared independence from the Soviet Union in 1991, it has zealously embraced information and communications technology and has become one of the most wired nations in Europe. More than 65 percent of Estonians have access to the Internet and they conduct virtually all administrative functions of society online.[12] This includes 97 percent of all banking transactions, as well as voting and paying taxes online.[13] In fact, Estonia has embraced cyberspace to such a high degree that all of its citizens carry national identification cards embedded with electronic identity chips and the country's parliament declared Internet access a basic human right in 2000."[14] This high degree of reliance on ICT made Estonia extremely vulnerable to cyber attack.

For two weeks beginning in late April 2007 the eastern European nation endured the world's first cyber attack to threaten the national security of an entire state.[15] The persistent attacks involved computer robot networks, known as botnets, that seized more than a million computers from 75 countries and directed them to barrage targets in Estonia, eventually "bringing the functioning of government, banks, media and other institutions to a virtual standstill."[16] The majority of the attacks came in the form of distributed denial of service (DDOS) attacks that overwhelmed websites with a massive number of requests for information and crippled the underlying network of routers and servers.[17] Although Estonian officials said the sources of the attacks had possible ties to the Russian government, insufficient evidence existed to accuse Moscow. While the

investigation continues, so far only one person has been convicted and fined in the cyber attack against Estonia.[18]

A year after the Estonia attacks, Georgia suffered the world's first cyber attacks that coincided with conventional attacks.[19] The cyber attacks were staged to kick off shortly before the initial Russian airstrikes as part of the Russian invasion in August 2008.[20] The attacks focused on government websites, with media, communications, banking, and transportation companies also targeted.[21] These botnet-driven DDOS attacks were accompanied by a cyber blockade that rerouted all Georgian Internet traffic through Russia and blocked electronic traffic in and out of Georgia.[22] The impact of the cyber attacks on Georgia was significant, but less severe than the Estonia attacks since Georgia is a much less advanced Internet society. Nonetheless, the attacks severely limited Georgia's ability to communicate its message to the world and its own people, and to shape international perception while fighting a war in which "accusations of genocide have been levied."[23] Similar to the Estonian attacks, while evidence suggested Russian involvement, there was no smoking gun to substantiate its complicity. However, experts believe the cyber attacks bore "the markings of a trained and centrally coordinated cadre of professionals" and "were too successful to have materialized independent of one another."[24] As evidenced by the cyber attacks on the two former Soviet republics, greater dependence on cyberspace equates to greater vulnerability.

In the U.S., where Internet use has penetrated 73 percent of the American population, cyberspace plays a vital role in controlling American critical infrastructure and processes in manufacturing, utilities, banking, and communications, as well as

military systems.[25] Recognizing this vulnerability, President Bush declared that a healthy, functioning cyberspace was essential to U.S. national interests.[26] In fact, cyber aggression threatens three of the four core U.S. national interests as defined by the U.S. Army War College: security of the homeland, economic well-being, and a stable international order.[27]

The critical infrastructure of homeland security is extremely reliant on ICT, specifically the supervisory control and data acquisition (SCADA) systems. SCADA systems are the computer systems that autonomously monitor and adjust switching and other processes of critical infrastructures like power plants. These systems are frequently unmanned and are remotely accessed by engineers via telecommunications links.[28] The Chairman of the Joint Chiefs of Staff recognized the destructive potential of cyber attacks against critical infrastructures and compared cyber war with weapons of mass destruction when he stated,

> Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction or methods producing WMD-like effects. Such catastrophic effects are possible in cyberspace because of the existing linkage of cyberspace to critical infrastructure SCADA systems. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructures locally, nationally, or possibly globally.[29]

The corresponding vulnerabilities have not gone unnoticed. Al Qaeda computers seized in Afghanistan contained models of a dam complete with engineering software that "enabled the simulation of a catastrophic failure of dam controls," as well as "programming instructions for digital switches that run power, water, transport, and communications grids."[30] Additionally, in late 2001 the FBI uncovered multiple cases of electronic surveillance of "emergency telephone systems, electrical generation and

transmission equipment, water storage and distribution systems, nuclear power plants, and gas facilities across the U.S.," emanating from Saudi Arabia, Indonesia, and Pakistan.[31] Furthermore, hackers frequently employ malicious computer code known as worms, to identify and exploit vulnerabilities within a network.[32] In one such instance, the "Slammer" computer worm corrupted the safety monitoring systems of a nuclear power plant in Ohio for five hours in 2003 via a backdoor through the Internet.[33] Another worm known as MSBlast was reportedly linked to the major power outage that hit the northeast United States in August 2003, where it "crippled key detection systems and delayed response during a critical time."[34] And in 2007, researchers at the Idaho National Laboratory "launched an experimental cyber attack" causing a generator to self-destruct by changing the device's operating cycle.[35] Industry experts hypothesize that "cyber attacks on key electrical facilities could knock out power to large geographic areas for months, harming the nation's economy."[36]

Like homeland security, economic well being is another national interest that is seriously vulnerable to cyber attack. The whole economy is linked to U.S. and global financial systems controlled by computer networks. In fact, "finance, wholesale and retail trade, transportation, much of manufacturing, and many service industries would slow to a crawl without computers."[37] Estimated losses due to cyber attacks amounted to $226 billion worldwide in 2003.[38] The average corporation traded on the New York Stock Exchange suffered losses up to five percent in the days following an attack, which translated into shareholder losses up to $200 million.[39] In 2006, a jihadist web site promoted an aspirational threat to "carry out cyber attacks on the U.S. financial industry to retaliate for abuses at the Guantanamo Bay prison facility."[40] A year later, the

aforementioned cyber attack on Estonia forced two major banks to suspend operations, losing millions of dollars.[41] Similarly, the attacks on Georgia's banking system in August, 2008, shut down electronic financial transactions for 10 days.[42] Sensitive, global financial markets are volatile enough without the added disruption and uncertainty of cyber attacks. A successful major attack on a primary financial center like Wall Street or the Nikkei would damage economies worldwide, induce fiscal panic for Americans concerned about their pensions and life savings, and severely damage people's faith in their governments.

In addition to security and economic well being, cyber aggression can adversely affect a stable international order, as the cumulative damage from cyber attacks against critical infrastructure "…can ignite panic, cause a loss of confidence, create uncertainty, and destroy trust in modern society."[43] Sustained disruptions to basic services could lead to a mob mentality. "The fragility of social order was demonstrated in 2008 when fuel price increases led to widespread violent protests across the globe."[44]

In short, since the inception of the Internet, cyber attacks have grown in scope and destructiveness to where it now threatens America's core national interests of homeland security, the economy, and international stability. In fact, aggression in cyberspace has emerged as a threat to the national security of all sovereign states. However, "there is currently no international, legally binding instrument that would address cyber attacks as threats to national security."[45] Can cyber attack threaten national security and not be an act of war?

Cyber Attack as an Act of War

States exist in an anarchic world where security is a self-help system. States maintain order and security by exercising their monopoly on legitimate violence.[46] This legitimacy is derived and defined by the international regime of laws, norms, and definitions regarding war and aggression. Therefore, international stability is underpinned by a common understanding of this regime and ultimately frames how states behave in the anarchic system. Similarly, definitions of cyber war and related terms are critical because they will drive how the laws of war and international treaties will proscribe the scope and use of cyber capabilities for martial purposes.[47] In other words, norms and definitions guide how states will behave in cyberspace. The lack of a common understanding regarding cyber attack causes uncertainty that could unintentionally escalate conflicts if states have different interpretations of what is permissible in cyberspace.[48] A common understanding of cyber war will also guide how a state can deter cyber attacks. At any rate, a definition of cyber war must be preceded by a definition of cyberspace.

The expansive, global nature of cyberspace and the rapid rate of change of ICT make defining cyberspace a challenge. Dr. Dan Kuehl, an information operations expert at the National Defense University identified over a dozen definitions of cyberspace in circulation, ranging from Google's "the place between the phones" to several variations within the Department of Defense.[49]

The Department of Defense's definition has matured over time. Early joint doctrine limited cyberspace to "a notional environment in which digitized information is communicated over computer networks," implying cyberspace was simply a communications medium of a theoretical or imaginary nature.[50] In 2006, the Chairman

of the Joint Chiefs of Staff referred to cyberspace as 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," which recognized cyberspace as a domain that stretched beyond computers.[51] In the same year, the Air Force's Cyber Task Force more bluntly deemed cyberspace as an operational warfighting domain where the electromagnetic spectrum was the maneuver space.[52] Finally, the October 2008 update of Joint Publication (JP) 1-02, the official military dictionary, refined cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[53] This definition in JP 1-02 provides a solid basis for defining cyber war. In addition to recognizing the global, omnipresent nature of cyberspace, this definition references the information environment, inferring cyberspace pervades and links the *physical* world, where people and society's critical infrastructures reside, the *information* realm, where data is created and stored, and the *cognitive* realm where human perceptions and decisions are made.[54] These linkages make cyber warfare an attractive supplement or alternative to conventional war and tie cyberspace to national security.

President Bush underscored the national security implications of cyberspace when he characterized it as the nervous system of the nation's critical infrastructures, controlling public and private institutional assets in the "…agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and

hazardous materials, and postal and shipping" sectors.[55] The president specifically stated cyberspace "is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work."[56]

From this definition and its implications, one could deduce that cyber war is simply warfare in the cyberspace domain, but this simplification is insufficient for two reasons. First, 'warfare in cyberspace' is too broad a definition. Dropping a bomb on a telecommunications center is not cyber war. Moreover, cyber war is not synonymous with information operations (IO), but it could be a subset of IO. IO is comprised of psychological operations, military deception, operations security, electronic warfare, and computer network operations (CNO).[57] CNO involves actions through "…the use of computer networks…" to attack "…information resident in computers and computer networks, or the computers and networks themselves."[58] Cyber war uses cyberspace to attack personnel, facilities, or equipment *in addition* to information and computers.[59]

Second, defining cyber war as warfare in cyberspace ignores the complexity of applying the more fundamental legal aspects of war to cyberspace. What is war in cyberspace? The original drafters of international law did not envision cyber capabilities and the current regime of international law reflects this shortcoming. However, the United Nations (UN) Charter, Hague and Geneva Conventions, and related treaties are the only basis from which to assess acts of war.

International law does not define the term "act of war." In the sense that war is "the legal consequence of the use of force" between states, international law is organized on the concepts of "use of force" and aggression.[60] A state of war may exist

when a nation violates Article 2(4) of the UN Charter. Article 2(4) prohibits states from threatening or using force "…against the territorial integrity or political independence of any state."[61] However, not all force is prohibited. The UN Charter outlaws the use of *aggressive* force while recognizing the right of states to use force in self-defense as specified in Article 51.[62] The term *aggressive* generally refers to the actions of the first party resorting to force or the threat thereof.[63] Furthermore, the UN defines aggression in Article 1 of the UN General Assembly Resolution 3314 as "the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another state."[64] Thus the "…trigger for the inherent right of self-defense…" that defines a legal state of war "…is contingent on a use of force amounting to an armed attack."[65] So the key issue in understanding cyber war involves the concept of armed attack.

Unfortunately, the UN Charter does not provide a definition of armed attack to apply to cyberspace. However, the General Assembly's Resolution 3314 provides several examples of aggression that constitute armed attack.[66] Such actions include invasion or attack, bombardment, blockade of ports or coasts, and attacks on land, sea, or air forces of another state.[67] These examples manifest themselves in the physical world and fall within the traditional approach of kinetic means that produce physical effects on a state and its sovereignty. How does one translate these ideas into cyberspace where the concept of kinetic means does not easily apply?

In cyberspace, cyber attack is the mechanism that equates to the use of force. Cyber attack, although not defined officially, can be viewed as a subset of cyber operations employing the hostile use of computers and information technology infrastructure to achieve effects or objectives in or through cyberspace.[68] Cyber war

occurs when cyber attacks reach the threshold of hostilities commonly recognized as war by the international community and defined by international law. While cyber attacks are hostile acts in cyberspace, not all cyber attacks equate to armed attack. Defacing web sites hardly amounts to an act of war. Yet cyber attacks can range from the defacing of individual web sites to the organized shut down of electrical power grids. Correspondingly, the effects of cyber attack can range from mere annoyance to physical destruction and death. Cyber attacks can target individuals, objects, or entire societies.[69] Somewhere along this spectrum of conflict in cyberspace, cyber attack crosses the threshold and becomes an armed attack.

A logical discriminator to gauge a cyber attack is to judge the action by the effect or consequence it produces, rather than its means of delivery. "Armed attack should not be defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused."[70] This is supported by international law where it is recognized that the use of "unarmed, non-military physical force" can produce the same severe effects as an armed attack, so actions like the "spreading of fire across a frontier" or the "diversion of a river by an upstream state" would constitute armed attacks in terms of Article 2(4) of the UN Charter.[71] Cyber attacks may not exactly fit the unarmed, non-military physical force paradigm, but they can cause commensurate effects.

Following this logic, any cyber attack that causes the same level of damage as a traditional armed or kinetic attack, either through the destruction of physical property or loss of life, would be considered an armed attack. Whether a power plant is bombed by aircraft or its electrical grid destroyed by malicious code, a blackout is a blackout. Until

recently this quantitative approach towards assessing cyber attacks achieved consensus among legal scholars.[72] However, cyber attacks can cause damage to other aspects of society besides physical property and people. As seen in Estonia and Georgia, cyber attack can inflict economic and psychological damage as well. Also, scholars argue this exclusively effects-based approach to classifying armed attack is out of sync with the qualitative, instrument-based paradigm of the UN Charter that places greater restrictions on military activity versus non-military activity.[73] For instance, a long-term, devastating economic embargo that causes enormous suffering would not be considered an armed attack, but a minor, armed border incursion *would* equate to an armed attack.[74] One method that attempts to bridge this quantitative and qualitative gap and may provide a more comprehensive assessment of cyber attack is known as Schmitt Analysis.

In 1999, Professor Michael N. Schmitt created a framework that can be used to assess whether a cyber attack equates to a use force in terms the UN Charter. For a given attack scenario, the method evaluates seven qualitative factors and produces a cumulative score that "determines the overall level of forcefulness, which is either above or below the Article 2(4) threshold" of the UN Charter.[75] Some of the more pertinent factors include *severity*, which measures the level of physical injury or damage to property; *immediacy*, which evaluates how fast the effects are seen; *directness*, which measures to what extent the attack is the sole cause of the effect; and *invasiveness*, which assesses to what degree the attack crosses into the targeted state.[76]

In 2003, a team of researchers applied the Schmitt Analysis to a notional cyber attack scenario where terrorists remotely used malicious code to strike the software-

intensive control systems of the Washington D.C. subway.[77] The simulated attack caused several train collisions, killing 30 people and causing extensive property damage. The analysis concluded that an armed attack occurred. It is clear that any cyber attack that produces effects tantamount to traditional armed force will score above the threshold of an armed attack. What is not clear is the case of cyber attacks that cause extreme economic damage. The severity factor of the Schmitt Analysis is designed to weigh physical destruction heavier than economic impact. Also, since most cyber attacks would emanate from outside the targeted state, cyber attacks earn lower invasiveness scores than traditional armed attacks, as was the case in the subway scenario.[78] The economic impact of the Estonian and Georgian cyber attacks was considerable and illustrates the potential for future, more devastating attacks on economies. As this potential develops, the Schmitt criteria applied to cyber attack will need to adjust.

International law is also unclear regarding acts of economic coercion. The prevailing view among scholars interpreting Article 2(4) of the UN Charter is that the charter only prohibits armed force and would not proscribe acts of economic coercion. [79] Alternatively, some scholars suggest economic coercion becomes economic aggression if the action jeopardizes a state's security.[80] A cyber attack of this consequence would meet the Article 2(4) threshold for a use of force, but probably not the armed attack threshold for self defense in Article 51.

Given its potential to cause grave damage to national security, cyber attack must be treated as an act of war, or in terms of international law, as a "use of force" and an armed attack. However, assessing whether a cyber attack is an act of war is a

complicated effort. Each case must be examined in its own context against international laws and circumstances because no single rule set exists that defines what constitutes a use of force or armed attack under all circumstances.[81] Furthermore, the current regime of international laws, norms, and definitions were designed a half century before the advent of cyber capabilities and are ill-suited for cyberspace. Existing international law impedes the development of a common understanding of cyber aggression and hinders a state's ability to deter cyber attacks against them.

Deterring Cyber War

In general, deterrence is a state of mind. It is the concept of one state influencing another state to choose *not* to do something that would conflict with the interests of the influencing state. Similarly, the central idea of deterrence from the perspective of the Department of Defense is "to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against U.S. vital interests."[82] Deterred states decide not to take certain actions because they perceive or fear that such actions would produce intolerable consequences.[83] The idea of influencing states' decisions assumes that states are rational actors "willing to weigh the perceived costs of an action against the perceived benefits, and to choose a course of action" logically based on "some reasonable cost-benefit ratio."[84]

Thus the efficacy of cyber deterrence relies on the ability to impose or raise costs and to deny or lower benefits related to cyber attack in a state's decision-making calculus. Credible cyber deterrence is also dependent on a state's willingness to use these abilities and a potential aggressor's awareness that these abilities, and the will to use them, exist. While a state's ability to deter cyber attacks is a subset of its

overarching defense strategy comprised of all instruments of national power, this paper focuses on states' actions to deter cyber attack within the cyberspace domain. Effective cyber deterrence in cyberspace will employ a comprehensive scheme of offensive and defensive cyber capabilities supported by a robust international legal framework.

Offensive capabilities are the primary tools used to impose or raise costs in deterrence. Offensive cyber capabilities and operations provide a state the means and ways for retaliation and enhance the perceived probability that aggressors will pay severely for their actions. A more robust capability translates to a more credible imposition of costs. Until recently, U.S. efforts to develop offensive cyber capabilities have lagged efforts on the defensive side. The daily onslaught of attacks on U.S. networks, coupled with the likelihood that potential U.S. adversaries will be less dependent on electronic networks than the U.S., has prioritized intelligence gathering and defending U.S. capabilities over disrupting enemy capabilities.[85] However, the United States has recently gained momentum in the development of offensive cyber capabilities.

In 2006, the U.S. published the National Military Strategy for Cyber Operations with the expressed intent to achieve "military strategic superiority in cyberspace."[86] One of its main goals is to ensure "adversaries are deterred from establishing or employing offensive capabilities against U.S. interests in cyberspace."[87] Unlike the air, land, and sea domains, the U.S. currently lacks dominance in cyberspace.[88] In fact, without a significant effort, the U.S. will lose its current technological advantages and "risks parity with adversaries" in cyberspace.[89] To this end, the U.S. has taken measures in support of offensive cyber operations. While each military service has some form of cyber

footprint, the U.S. Air Force has incorporated operating in cyberspace as part of its core mission on par with flying and space operations. For instance, the commander of the Air Force's provisional cyber operations command envisions initial offensive cyber operations as subduing or killing data packets that threaten U.S. systems, with the potential to expand in the future to missions normally executed by conventional forces in the past.[90] The U.S. continues to modernize its cyber forces, create new hacker units, and conduct cyberwar exercises,[91] with the intent to "penetrate and disrupt foreign computer systems."[92] However, the U.S. is not alone in pursuing cyber attack. Over 120 countries already have or are developing computer attack capabilities, reinforcing the need for a strong defense.[93]

In addition to offensive means, defensive capabilities play a critical role in deterring cyber attack. Defensive cyber capabilities not only ensure essential services and functions of society continue unabated, they also deny or lower the benefits an aggressor might obtain via cyber attack. Defensive cyber capabilities increase a state's resistance to attacks and reduce the consequences of attacks. They enable the state to strengthen the security of potential targets and correspondingly limit or eliminate an aggressor's ability to threaten the state through cyberspace. Ultimately they reduce the probability of success that an aggressor will achieve its goals.

The U.S. historically has primarily employed a defensive cyber policy as outlined in the National Strategy to Secure Cyberspace. This strategy focuses on preventing cyber attacks against America's critical infrastructures, reducing national vulnerability to cyber attacks, and minimizing damage and recovery time from attacks that do occur.[94] It recognizes the need to unite all levels and facets of government with private industry

and individual Internet users to synergize defensive efforts, and outlines broad, robust defensive measures and capabilities to deter cyber attack. For instance, the U.S. continues to invest defensively in cyberspace infrastructure by "…diversifying and limiting the number of access points that could be used for an attack."[95] Also, the Department of Homeland Security (DHS) is leading integrated efforts between the public and private sectors, like the U.S. Computer Emergency Readiness Team designed to analyze threats and coordinate responses to cyber attacks.[96]

However, the current U.S. approach focuses on deterring attacks in *American* cyberspace, as if cyberspace recognizes state borders. Cyber attacks against the infrastructure or economies of other states can have severe, cascading effects on the U.S. The globalized interdependence of cyberspace underscores the adage 'a risk accepted by one is a risk assumed by all,' implying that cyber aggression requires a cosmopolitan solution. Unfortunately, the U.S. deterrent strategies do little to foster the crafting of international standards of state behavior in cyberspace. In contrast, Estonia, a veteran of the largest cyber attack in history, promotes a defensive strategy to secure cyberspace with a broader perspective. Like the U.S., Estonia seeks to protect its critical infrastructure, to prevent cyber attacks, and to ensure a swift recovery of systems should an attack occur.[97] However, Estonia also champions the development of international norms to regulate cyber attacks.[98]

Over and above offensive and defensive cyber capabilities, a robust, international legal framework that addresses cyber aggression is the most critical component of a comprehensive approach to deter cyber attack. International law and norms are fundamental to deterrence because states "share an interest in adopting or

codifying common standards for the conduct of international transactions…or in promoting or banning specific kinds of behavior by" states.[99] Multilateral agreements provide the most efficient way of realizing these shared interests.[100] The common acceptance of norms moderates state interaction and makes state behavior more predictable, which leads states to "combine to insist on respect for specific norms of…conduct by those who violate their consensus."[101] In this way, international law builds the framework that guides how and when states employ offensive and defensive cyber capabilities and forms the foundation of cyber deterrence. International law adds certainty to punitive actions and amplifies the costs of cyber attack by engendering a negative response from the international community, not just from the attacked state. Moreover, it adds credibility to the threat of reprisal by providing legitimacy to retaliatory actions and by increasing the potential to isolate the aggressive state. Also, international law provides a measure of protection to states that lack robust defensive and offensive cyber capabilities and serves as their first and possibly only line of deterrence.

However, as outlined previously, there is currently "no binding international law on cyber security" that "expresses the common will of countries."[102] In fact, the lack of international norms, laws, and definitions to govern state actions in cyberspace has led to a gray area that can be exploited by aggressive states as long as their actions skirt the imprecise thresholds contained in the UN charter.[103] For example, in response to accusations of state-sponsored cyber war against Estonia, "the head of the Russian Military Forecasting Centre stated that the attacks against Estonia had not violated any international agreements because no such agreements exist," suggesting that even if

Russia's complicity could be proved, Estonia's options for reprisal were limited.[104] Such an environment thwarts deterrence because it lowers the probability "of reprisal even if the attacker's identity is suspected" and reduces an attacker's potential costs of pursuing cyber attack.[105] Oddly, this void in international law is unique to cyberspace.

Each time warfare was introduced to a new domain, international law reacted by developing domain-specific guidance in some form of treaty or convention. For example, the rules governing actions on the seas have existed as customary law for centuries, based on the Grotian doctrine of 'freedom of the seas' dating back to the early 1600s.[106] This customary law now exists as the United Nations Convention on Law of the Seas. Also, five years after World War I, the war in which the airplane made its debut as a weapon, the international community drafted the 1923 Hague Rules of Aerial Warfare. Although not ratified, these rules have endured to "form the basis of all current regulation of air warfare."[107] Moreover, ten years after the launch of Sputnik, the international community agreed to the principles of the Outer Space Treaty in 1967. Despite these precedents, roughly 16 years after the World Wide Web burst onto the public scene, no international regime exists to govern state actions in cyberspace.[108]

In addition to a non-existent regulatory framework, ineffective attribution of cyber attacks further undermines deterrence in cyberspace and widens the exploitable gray area. The threat of offensive cyber capabilities will not deter aggression if the attacked state cannot identify its attacker. Likewise, deterrence falters if the UN cannot identify whom to target with sanctions. In the aftermath of the Estonian attacks, "neither NATO nor European Commission experts were able to find any proof of official Russian government participation."[109] This would reduce the probability of reprisal to zero and

nearly eliminate the costs of pursuing cyber attack. Reversing this recurring theme in cyber attack investigations requires significant international investment.

In summary, the concept of deterrence is applicable to cyberspace since it focuses on the decision calculus of a state, not the domain in which it is employed. While offensive and defensive cyber capabilities are critical to deterring aggression, employing these capabilities depends on robust international norms for state behavior in cyberspace. International law is the first line of deterrence in cyberspace.

Conclusions and Recommendations

Since the launch of the information superhighway in the 1990s, the destructiveness of cyber attack has consistently grown in magnitude to the extent that it can now threaten the critical infrastructure that forms the basis of modern society. In short, cyber attack can cause grave damage to national security. In fact, it can prevent a state from functioning.[110] Rational, commonsensical thought realizes cyber attack can be an act of war, but common sense and the rule of law conflict in cyberspace. The current regime of international laws, norms, and definitions not only insufficiently addresses cyber aggression, it actually intensifies the dangers of cyber attack by creating a gray area or loophole that can be exploited by cyber aggressors. This loophole, coupled with insufficient techniques to identify assailants, undermines a state's ability to deter cyber attack. To reverse this trend, the U.S. must pursue a policy of regime change, where regime in this case refers to the "complex of norms, treaties, international organizations, and transnational activity that orders" cyberspace.[111]

The U.S. should lead a multilateral effort in conjunction with the UN to adapt the existing international regime of laws and norms governing warfare to address

aggression in cyberspace, or build a new regime for the new warfighting domain. Only the UN has the "membership and capability to address these issues in a meaningful way that will have a global impact" to this global problem.[112] Regulation within individual countries alone will prove ineffective.[113] Already the world has seen "Internet activities considered to be legitimate in one country violate the laws in another."[114] Additionally, the U.S. should lead a United Nations effort to establish an institution to "…serve as a clearinghouse and coordination center…" to pool international cyber security initiatives and maintain standards.[115] The regime and institution would define international relations within cyberspace and provide a mechanism for the international community to initiate sanctions or punitive actions for noncompliance. The knowledge that a cyber attack is an act of war provoking a severe, costly reprisal from the global community would serve as a strong deterrent to would-be cyber aggressors. This regime change proposal fully supports the U.S. National Security Strategy, in which the President urges, "where existing institutions and regimes can be reformed to meet new challenges, we…must reform them. Where appropriate institutions do not exist, we…must create them."[116]

The Council of Europe's (CoE) Convention on Cybercrime provides the U.S. a solid basis on which to build a new international regime. The CoE recognized that addressing the transnational character of cybercrime required a global effort.[117] The treaty fosters international cooperation to fight crime in cyberspace and defines various offenses as cybercrimes with the intent to "establish a common criminal policy," improve deterrence, and "reduce the number of countries in which criminals can avoid prosecution."[118] However, this convention cannot be extended to cyber war as it treats

cyber attacks as crimes against private and public property and makes no distinction between the scope and impact of the attack, "thereby disregarding the national security dimension of the threat."[119] Despite these shortcomings, the convention still serves as a model for international cooperation and the development of a larger-scale regime.

The U.S. is uniquely suited to lead this effort. "The United States…acts as an architect of global and regional security affairs for the purpose of containing new-era dangers."[120] More importantly, this effort allows the U.S. to shape international norms for states' behavior in cyberspace in accordance with American national interests; otherwise the U.S. risks forfeiting this advantage to other nations. For example, China is engaged "in the debate of defining cyber warfare, in part through the Shanghai Cooperation Organization, in order to have a hand in the shaping of a legal framework and rules of engagement related to this new warfare."[121]

To strengthen the new regime's ability to deter cyber attack, the U.S. should also lead research and development efforts to improve attribution techniques. This includes accelerating ventures like the multilateral effort within the UN to trace original sources of Internet communications and reduce the anonymity of cyberspace; creating an "International Caller-ID capability" of sorts for the Internet.[122] Such an effort "requires multilateral actions that transcend jurisdictions and national boundaries."[123] Ultimately, an acknowledged ability to track aggression is essential to deter future attacks by increasing the probability of reprisal and elevating the costs of resorting to cyber attack.[124]

In closing, cyber attack can cause grave damage to national security and must be treated as an act of war. A robust international regime of laws, norms, and

definitions provides the basis for deterrence in cyberspace. Moreover, the U.S. is uniquely suited to lead efforts to constrain state behavior in this new global, warfighting domain. The Internet is an "interconnected global network of 600 million users served by 15 million hosts connecting nearly 200 countries."[125] Consequently, cyberspace is the *world's* nervous system; the control system of modern society. Its protection is an international existential concern.

Endnotes

[1] George W. Bush, *National Strategy to Secure Cyberspace*, (Washington DC: The White House, February 2003), 5

[2] Ibid.

[3] Ibid.

[4] Steven A. Hildreth, "Cyberwarfare," Congressional Research Service policy paper, June 19, 2001

[5] Ibid.

[6] Margaret Kane, "I Love You Email Worm Invades PCs," *ZDNet News*, May 4, 2000, http://news.zdnet.com/2100-9595_22-107318.html?legacy=zdnn, (accessed December 1, 2008).

[7] Lincoln P. Bloomfield, Jr., "Cybersecurity: Ensuring the Safety and Security of Networked Information Systems," remarks at the Southeastern European Cybersecurity Conference, Sophia, Bulgaria, September 8, 2003, U.S. Department of State, http://www.state.gov/t/pm/rls/rm/23874.htm, (access October 30, 2008).

[8] Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," (Washington DC: Dept. of Defense, April 12, 2001, amended through October 17, 2008), 459, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf, (accessed November 23, 2008).

[9] *Frontline: Cyberwar!*, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, (accessed November 30, 2008).

[10] Ibid.

[11] Bloomfield.

[12] Christopher Rhoads, “Politics & Economics: Estonia Gauges Best Response to Cyber Attack,” *The Wall Street Journal*, May 18, 2007.

[13] “Cyberwar is genuine Threat,” *RSA Conference Daily*, October 23, 2007, http://newsweaver.co.uk/rsaconference/e_article000935998.cfm?x=bbs1LTr,b8gpBBSr,w, (accessed October 28, 2008).

[14] “Cyberwarfare 101: Case Study of a Textbook Attack,” *Stratfor*, April 18, 2008, http://www.stratfor.com/analysis/cyberwarfare_101_case_study_textbook_attack, (accessed November 5, 2008).

[15] Joshua Davis, “Hackers Take Down the Most Wired Country in Europe,” Wired Magazine, Iss. 15.09, August 21, 2007, http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia, (accessed October 16, 2008)

[16] “Cyberwarfare 101: Case Study of a Textbook Attack,” *Stratfor*, April 18, 2008, http://www.stratfor.com/analysis/cyberwarfare_101_case_study_textbook_attack, (accessed November 5, 2008).

[17] Adam Smith, “Under Attack, Over the Net,” *Time International*, June 11, 2007, 50.

[18] Clay Wilson, “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,” Congressional Research Service Report for Congress, RL32114, January 29, 2008, 8.

[19] John Markoff, “Before the Gunfire, Cyberattacks,” *New York Times*, August 13, 2008.

[20] Ibid.

[21] Ibid.

[22] “Russian Invasion of Georgia, Russian Cyberwar on Georgia,” *Georgia Update*, http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf, (accessed November 14, 2008).

[23] “Cyberwarfare 101: Georgia, Russia: The Cyberwarfare Angle,” Stratfor.com, August 12, 2008, http://www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle, (accessed November 5, 2008).

[24] Travis Wentworth, “Russian Nationalists Waged a Cyber War against Georgia. Fighting Back is Virtually Impossible,” *Newsweek*, September 1, 2008.

[25] Internet World Stats, http://www.internetworldstats.com/top20.htm (accessed November 11, 2008).

[26] George W. Bush, *National Strategy to Secure Cyberspace*, vii.

[27] US Army War College, “National Security Policy and Strategy Course Directive,” Appendix I, 124 (Carlisle Barracks, PA: US Army War College, 2008).

[28] Wilson, 22.

[29] General Peter Pace, Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, (Washington DC: Dept. of Defense, December 2006), C-1, http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf, (accessed November 30, 2008).

[30] World Federation of Scientists, "Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar," report and recommendations of the Permanent Monitoring Panel on Information Security, November 19, 2003, 10.

[31] World Federation of Scientists, 10.

[32] Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala*, Vol. 8, No. 1, October 2008, 51.

[33] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Nework," *Security Focus*, August 19, 2003, http://www.securityfocus.com/news/6767 (accessed November 14, 2008).

[34] Robert Lemos, "MSBlast and the Northeast Power Outage," *CNet News*, February 16, 2005, http://news.cnet.com/8301-10784_3-5579309-7.html (accessed December 1, 2008).

[35] Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," http://www.cnn.com/2007/US/09/26/power.at.risk/index.html, (accessed October 28, 2008)

[36] Ibid.

[37] Brian Cashell, William D. Jackson, Mark Jicklin,et al., "The Economic Impact of Cyber Attacks, CRS Report for Congress RL 32331, April 1, 2004, CRS-1, http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf, (accessed December 1, 2008).

[38] Cashell, et al., summary page.

[39] Ibid.

[40]"US Warns of Possible Financial Cyber Attack," *NBC News and News Services*, November 30, 2006, http://www.msnbc.msn.com/id/15975889/, (accessed December 1, 2008).

[41] Stratfor online, "Cyberwarfare 101: Case Study of a Textbook Attack," http://www.stratfor.com/analysis/cyberwarfare_101_case_study_textbook_attack, (accessed November 8, 2008).

[42] Eneken Tikk, Kadri Kaska, Kristel Runnimeri, et al, "Georgian Cyber Attacks: Legal Lessons Identified," (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008), 7.

[43] World Federation of Scientists, 9.

[44] Fritz, 66.

[45] Eneken Tikk, et al, 13.

[46] Max Weber, *The Theory of Social and Economic Organization*, (New York: Collier-MacMillan, 1964), 154.

[47] Richard W. Aldrich, "The International Legal Implications of Information Warfare," Airpower Journal, Fall 1996, 100, http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf, (accessed November 3, 2008).

[48] Duncan B. Hollis, "Rules of Cyberwar?" *Los Angeles Times*, October 8, 2007, A15.

[49] Dr. Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," http://www.maxwell.af.mil/au/awc/cyberspace/documents/Cyber%20Chapter%20Kuehl%20Final.doc, (accessed November 3, 2008).

[50] Kuehl, 2.

[51] Pace, 3.

[52] Dr. Lani Kass, "A Warfighting Domain," AF Cyberspace Task Force briefing, September 26, 2006, 14, http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf (accessed November 3, 2008).

[53] JP 1-02, 141.

[54] Joint Publication 3-13, "Information Operations," (Washington DC: February 13, 2006), I-1 – I-2.

[55] Bush, 1.

[56] Ibid.

[57] JP 3-13, II-1.

[58] Ibid., II-5.

[59] Keith B. Alexander, "Warfighting in Cyberspace," Joint Force Quarterly, issue 46,3d Quarter 2007, 60, http://www.carlisle.army.mil/DIME/documents/Alexander.pdf, (accessed November, 23, 2008).

[60] Walter G. Sharp, Jr., Cyberspace and the Use of Force, (Falls Church, VA: Aegis Research, 1999), 28.

[61] *United Nations Charter*, Article 2(4), http://www.un.org/aboutun/charter/. (accessed November 4, 2008).

[62] Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, (Falls Church, VA: Aegis Research, 2000), 37.

[63] Ibid.

[64] United Nations, Resolution 3314, "Definition of Aggression," December 14, 1974, http://www.un-documents.net/a29r3314.htm, (accessed November 3, 2008).

[65] Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, 81.

[66] Bruno Simma, *The Charter of the United Nations: A Commentary*, (Oxford, UKI: Oxford University Press, 1994), 670.

[67] United Nations, Resolution 3314.

[68] JP 1-02, 141.

[69] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," (Colorado Springs, CO: Institute for Information Technology, 1999), 17, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993&Location=U2&doc=GetTRDoc.pdf (accessed November 3, 2008).

[70] Schmitt, 17.

[71] Sharp, 101.

[72] Thomas Wingfield and James B. Michael, "An Introduction to Legal Aspects of Operations in Cyberspace," report, (Monterrey, CA: Naval Postgraduate School, April 28, 2004), 10.

[73] Ibid.

[74] Michael N. Schmitt, quoted in Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, 116.

[75] Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, 122.

[76] Schmitt, 18 – 19.

[77] Thomas Wingfield, James B. Michael, Duminda Wijesekera, "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," November 2003, http://www.au.af.mil/au/awc/awcgate/nps/ws09-with-pub-info.pdf (accessed November 10, 2008).

[78] Ibid.

[79] Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace. 87-89.*

[80] Ibid, 90.

[81] Ibid, 56.

[82] Department of Defense, *Deterrence Operations Joint Operating Concept*, (Washington DC: Department of Defense, December 2006), 5.

[83] Colin S. Gray, "Deterrence and the Nature of Strategy," in *Deterrence in the 21st Century*, ed. Max G. Manwaring, (London: Frank Cass, 2001), 18.

[84] Robert H. Dorff and Joseph R. Cerami, “Deterrence and Competitive Strategies: A New Look at an Old Concept,” in *Deterrence in the 21st Century*, ed. Max G. Manwaring, (London: Frank Cass, 2001), 111.

[85] Julian E. Barnes, “Hacking Could Become Weapon in US Arsenal,” *Los Angeles Times*, September 28, 2008, http://www.latimes.com/news/nationworld/nation/la-na-cyber8-2008sep08,0,5570856,print.story, (accessed November 4, 2008).

[86] Pace, ix..

[87] Ibid., 13.

[88] General James Cartwright, quoted by David Blake, “Fighting in Cyberspace,” *Military Periscope,* April 25, 2007, http://www.militaryperiscope.com/special/special-200704251756.shtml, (accessed September 3, 2008).

[89] Pace, 10.

[90] “Military Ponders Cyber War Rules,” *Los Angeles Times*, April 7, 2008.

[91] Fritz, 42.

[92] Bradley Graham, “Bush Orders Guidelines for Cyber-Warfare,” *The Washington Post*, February 7, 2003, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38110-2003Feb6&notFound=true, (accessed November 14, 2008).

[93] General Accounting Office, “Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,” http://www.fas.org/irp/gao/aim96084.htm, (accessed November 4, 2008).

[94] Bush, viii.

[95] Fritz, 42

[96] United States Computer Emergency Response Team, http://www.us-cert.gov/aboutus.html (accessed November 12, 2008).

[97] Ministry of Defence, Estonia, *Cyber Security Strategy*, (Tallinn, Estonia: Ministry of Defence, 2008), 7.

[98] Ibid., 4-5.

[99] Charles W. Freeman, Jr., *Diplomatic Strategy and Tactics*, (Washington DC: US Institute of Peace, 1997), 84.

[100] Ibid.

[101] Charles W. Freeman, Jr., *Arts of Power: Statecraft and Diplomacy*, (Washington DC: US Institute of Peace, 1997), 38.

[102] Ministry of Defence, Estonia, *Cyber Security Strategy*, 17.

[103] Tikk, et al., 22.

[104] Fritz, 61.

[105] Tikk, et al., 22.

[106] James B. Morell, *The Law of the Sea: The 1982 Treaty and Its Rejection by the United States*, (London, UK: McFarland, 1992), 2.

[107] Richard H. Wyman, "The First Rules of Air Warfare," Air University Review, March-April 1984, (Maxwell AFB, AL: Air University Press, 1984), http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/mar-apr/wyman.html, (accessed December 1, 2008).

[108] "A History of the Internet 1962-1992," *Computer History Museum*, http://www.computerhistory.org/internet_history/internet_history_90s.shtml (accessed December 1, 2008).

[109] Fritz, 58.

[110] Ministry of Defence, Estonia, *Cyber Security Strategy*, 21.

[111] John T. Rourke and Mark A. Boyer, *International Politics on the World Stage*, glossary, http://highered.mcgraw-hill.com/sites/0073526304/student_view0/glossary.html (accessed on December 22, 2008).

[112] World Federation of Scientists, 19.

[113] Ministry of Defence, Estonia, *Cyber Security Strategy*, 17.

[114] World Federation of Scientists, 22.

[115] Ibid., 32.

[116] George W. Bush, *The National Security Strategy of the United States of America*, (Washington D.C.: The White House, 2006), 36.

[117] Kristin Archick, "Cybercrime: The Council of Europe Convention," CRS Report for Congress RS21208, September 28, 2006, 1.

[118] Ibid., 2-3.

[119] Ministry of Defence, Estonia, *Cyber Security Strategy*, 18

[120] Richard L. Kugler, *Policy Analysis in National Security Affairs: New Methods for a New Era*, (Washington DC: National Defense University Press, 2006), 87.

[121] Fritz, 43.

[122] Declan McCullagh, "UN Agency Eyes Curbs on Internet Anonymity," *CNET News*, September 12, 2008, http://news.cnet.com/8301-13578_3-10040152-38.html?tag=nl.e703, (accessed October 16, 2008).

[123] World Federation of Scientists, 27.

[124] Ibid., 26.

[125] Ibid., 18.