Author(s)	Moore, Ryan J.
Title	Prospects for cyber deterrence
Publisher	Monterey, Calif. Naval Postgraduate School
Issue Date	2008-12
URL	http://hdl.handle.net/10945/3740

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PROSPECTS FOR CYBER DETERRENCE

by

Ryan J. Moore

December 2008

Thesis Advisor: John Arquilla
Co-Thesis Advisor: Dorothy Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2008	**3. REPORT TYPE AND DATES COVERED** Master’s Thesis

4. TITLE AND SUBTITLE Prospects for Cyber Deterrence

5. FUNDING NUMBERS

6. AUTHOR(S) Ryan Moore, Captain, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

In today’s Information Age, a nation’s dependence on cyberspace is becoming an increasingly important aspect of national security. As technology has improved, and more sectors of critical national infrastructure are interconnected in cyberspace, the level of risk to national security has increased dramatically. Neither security policies nor international laws have been able to keep up with the demands of the rapidly evolving cybersphere. Nations need to examine ways to influence their adversaries against attacking critical infrastructure via cyberspace. Deterrence concepts and policies need to evolve to a level that can be applied to various actors, from the state to the non-state level. The cost of entry to employ cyberspace capabilities is extremely low compared to what it takes to establish conventional or nuclear forces. If the Estonia and Georgia cyber attacks of 2007 and 2008 have taught us anything, it is that highly networked nations can be vulnerable to cyber attacks. If a significant investment is made in successful deterrence strategies, the outlook for adopting a fully networked society may not seem so threatening.

14. SUBJECT TERMS Cyber Deterrence, National Security, Critical Infrastructure, Tailored Deterrence, Computer Network Attacks, Computer Network Defense

15. NUMBER OF PAGES
99

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

PROSPECTS FOR CYBER DETERRENCE

Ryan J. Moore
Captain, United States Air Force
B.S., University of Pittsburgh, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
December 2008**

Author: Ryan J. Moore

Approved by: Dr. John J. Arquilla
Thesis Advisor

Dr. Dorothy E. Denning
Co-Advisor

Dr. Gordon H. McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In today’s Information Age, a nation’s dependence on cyberspace is becoming an increasingly important aspect of national security. As technology has improved, and more sectors of critical national infrastructure are interconnected in cyberspace, the level of risk to national security has increased dramatically. Neither security policies nor international laws have been able to keep up with the demands of the rapidly evolving cybersphere. Nations need to examine ways to influence their adversaries against attacking critical infrastructure via cyberspace. Deterrence concepts and policies need to evolve to a level that can be applied to various actors, from the state to the non-state level. The cost of entry to employ cyberspace capabilities is extremely low compared to what it takes to establish conventional or nuclear forces. If the Estonia and Georgia cyber attacks of 2007 and 2008 have taught us anything, it is that highly networked nations can be vulnerable to cyber attacks. If a significant investment is made in successful deterrence strategies, the outlook for adopting a fully networked society may not seem so threatening.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1

A. FOUNDATIONS OF CYBER DETERRENCE....1

B. CYBERSPACE AND THE FUTURE OF WARFARE....7

C. DEFINING CYBER ATTACKS AND CYBER WARFARE....8

D. OVERVIEW....10

II. FUNDAMENTALS OF STRATEGIC DETERRENCE....13

A. INTRODUCTION....13

B. DEFINING DETERRENCE....13

C. FORMATION OF DETERRENCE STRATEGIES....15

D. THE UNDERLYING PRINCIPLES OF DETERRENCE....16

1. Two Deterrent Situations....17

a. General Deterrence 17

b. Immediate Deterrence....18

2. Deterrent Methods....18

a. Conventional Deterrence 19

b. Nuclear Deterrence 21

c. Tailored Deterrence....24

III. THE GROWING CYBER THREAT....27

A. THE CYBERSHOT HEARD 'ROUND THE WORLD....27

B. EXPLORING THE CYBER ENVIRONMENT....29

C. TRANSFORMATION TO THE INFORMATION AGE....30

D. VULNERABILITIES AND THE IMPACT ON NATIONAL SECURITY....34

1. Rise of the Botnet Militia....34

2. Other Critical Vulnerabilities....39

E. THE NEED TO PREVENT A 'DIGITAL PEARL HARBOR'....40

IV. DETERRENCE STRATEGY IN CYBERSPACE....45

A. PREVENTING CYBER ATTACKS THROUGH CYBER DETERRENCE....45

B. APPLYING PRINCIPLES OF DETERRENCE TO CYBERSPACE....46

C. TAILORING DETERRENCE TO CYBERSPACE – ONE SIZE DOES NOT FIT ALL....47

D. ELEMENTS OF DETERRENCE IN CYBERSPACE....49

1. Denial....50

2. Develop and Demonstrate Overt Punishment Techniques....52

3. Develop Thresholds....55

4. Develop and Articulate National Policy....56

E. APPLICATION OF CYBER DETERRENCE METHODS....57

V. THE PROSPECTS FOR CYBER DETERRENCE....................61
A. CYBERSPACE CHALLENGES AND RECOMMENDATIONS....................61
1. Attribution....................62
2. The Private Sector....................64
3. International Acceptance....................66
4. Understanding Nth Order Effects....................67
B. IMPLICATIONS FOR NATIONAL SECURITY....................69
C. IS CYBER DETERRENCE ATTAINABLE?....................70

LIST OF REFERENCES....................77

INITIAL DISTRIBUTION LIST....................85

LIST OF FIGURES

Figure 1. Number of Worldwide Internet Users (From www.internetworldstats.com)....5
Figure 2. Flow Chart of Questions on Deterrence (After George & Smoke, 1974, p. 102)........16
Figure 3. Basic Botnet depiction (From *Business Week*)........35
Figure 4. Botnet evolution (From Issa, 2008, p. 2)........36
Figure 5. Number of Botnet C2 Servers, Dec '05 – Nov '08 (From www.shadowserver.org)........38
Figure 6. Number of active Botnet nodes, Dec '05 – Nov '08 (From www.shadowserver.org)........38
Figure 7. Course of Action Process Diagram (After Miller, 2006, p. 37)........68

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my gratitude to all those who gave me the ability to complete this thesis. I would like to thank my thesis advisors, Dr. John Arquilla and Dr. Dorothy Denning, whose recommendations and guidance have been invaluable in my research.

In particular, special thanks are due to my wife, Donna. Words alone cannot express my thanks for her encouragement, support, assistance, and never ending optimism, in addition to putting up with all of those long nights and working weekends. Her emotional support and enduring love helped me get through the stressful and difficult times.

I am grateful to all my friends in life for all the camaraderie and entertainment they have provided me.

Thanks to my parents, Bobbie and Tim Moore. They gave me both the freedom and support that I needed to become the person I am today.

To my dog, Cocoa, whose companionship was never-ending. No matter how long or bad my day was, she would always greet me with a wagging tail and joy as I walked in the door. She reminded me that, every once in a while, you need to take a break and have some fun.

Finally, I would like to thank my grandmother, Ruth Gumbert, who will forever remain in my heart. She helped raise me, taught me, supported me, and loved me. To her I dedicate my thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> ...technologies are morally neutral until we apply them. It's only when we use them for good or for evil that they become good or evil.
>
> — William Gibson

A. FOUNDATIONS OF CYBER DETERRENCE

Weapon innovations such as tanks, airplanes, and nuclear weapons have revolutionized the way warfare has been waged during the past century. Over the past two decades, the world has seen a new emerging weapon system — networked computers. Computers may seem a bit out of place among the list of kinetic weapons that have been historically responsible for massive destruction and countless deaths. However, the non-kinetic power that results from the use of computer viruses, worms, and denial of service attacks has caught the attention of both nations and businesses that rely on cyberspace to remain connected to the world market.

Cyberspace was founded on the principles of establishing a free and open society for the sharing and collaboration of information to all those who wanted it (Leiner et al., 2003; Lipson, 2002, p. 13). As more computers were networked in cyberspace, products and resources were developed that could be used by consumers to make lives easier. Banks and companies incorporated services for people to manage their money, pay bills, and shop for items from home. In addition to commerce, people were now able research information, read books or articles, and share thoughts with one another. Finally, companies found ways to network their worldwide services via cyberspace, not only allowing them to manage information, but also to control portions of their infrastructure through commands issued to machinery in remote locations.

So, how can computer systems, which operate in a virtual, electronic realm actually be classified as weapon systems? A weapon is defined as a tool used in "...attack or defense in combat for the purpose of subduing enemy personnel, or to destroy enemy weapons, equipment and defensive structures through application of force" ("Weapon," 2008). In general, weapons can be defined as the simplest mechanisms that use leverage to multiply force to deny, degrade, or destroy specified targets. More recently, development of non-lethal weapon systems has been adopted for use, and designed to incapacitate and reduce collateral damage to property and the environment. As seen in some cyber attacks, networked computers can deny, degrade, and even destroy their specified targets. Denial of service attacks can deny access to certain cyber systems and degrade communications nodes. Additionally, the Department of Homeland Security video of a cyber attack on a networked power generator illustrated how these attacks could physically destroy a piece of infrastructure.

Cyberspace is an enabling factor for computer systems to achieve their effects as a weapon. Although there is still discussion on how cyberspace is specifically defined, it is generally characterized as a man-made, virtual environment, without international boundaries, and designed for the creation, transmittal, and use of information in a variety of formats (Rattray, 2001, p. 65). As a society in today’s Information Age, it is difficult to imagine a world without cyberspace; however, those who initially developed computer systems in the 1950s may not have imagined a worldwide network of computers being used to deliver kinetic and non-kinetic attacks against an adversary. However, the threat is real and nations must develop strategies to deter cyber attacks on their critical infrastructure before adversaries can seriously affect their security.

In today’s post Cold War era, a national policy of traditional nuclear deterrence is a strategy that needs revision to fit the present Information Age. If the old nuclear deterrent depended on the frightful force of mass destruction, the new digital strategy needs to win the total information war (Der Derian, 1994). A nation’s security can benefit greatly from policies that secure its dependence on information technology from adversarial exploitation. Nations need a cyber deterrence strategy that allows them to tailor their strategies based on actor-specific models. In order to build an effective deterrent against those operating in the cyberspace domain, offensive and defensive capabilities must be built and sustained to operate in the environment. The purpose of this research is to examine the prospects of cyber deterrence as an effective means of reducing the threat of cyber attacks.

Strategic deterrence in cyberspace will focus on deterring a nation’s adversaries from attacking its critical infrastructure, both civil and military. If the information systems that control critical infrastructure are compromised, it can impact national security and ultimately the lives of the populace (Lipson, 2002, p. 11). Because information systems are a vital part of the critical infrastructure of a nation, our way of life is potentially at risk if they are not adequately protected. Critical infrastructure refers to the physical and cyberspace-based systems essential to the minimum operations of the economy and the government. The George Mason University School of Law Critical Infrastructure Protection Program[1] defines critical infrastructure as "what drives all the necessary functions upon which society depends on." Critical infrastructures are complex and highly interdependent systems, networks, and assets that provide the services essential in our daily life. They are currently organized into the following 17 critical infrastructure and key resource sectors:

- Banking & Finance
- Chemical
- Energy
- Dams
- Commercial Facilities
- Commercial Nuclear Reactors, Materials & Waste
- Defense Industrial Base
- Transportation Systems
- Telecommunications
- Emergency Services
- Food & Agriculture
- Postal and Shipping
- Government Facilities
- Information Technology

[1] More information on the GMU Critical Infrastructure Protection Program can be found at http://cipp.gmu.edu/cip

- National Monuments and Icons
- Public Health & Healthcare
- Drinking Water & Wastewater Treatment Systems

Although computers operate in a virtual environment, a computer attack through cyberspace can cause destruction, both in the virtual and physical environments. There are approximately 550 million hosts connected to the Internet today (Internet Systems Consortium, 2008); furthermore, Figure 1 shows that the number of worldwide users has grown to approximately 1.6 billion users today. With the tremendous growth in cyberspace the deterrent value of successfully tracking and tracing attackers is becoming increasingly vital to the survival of the Internet and the nations that depend on it (Lipson, 2002, p. 11).

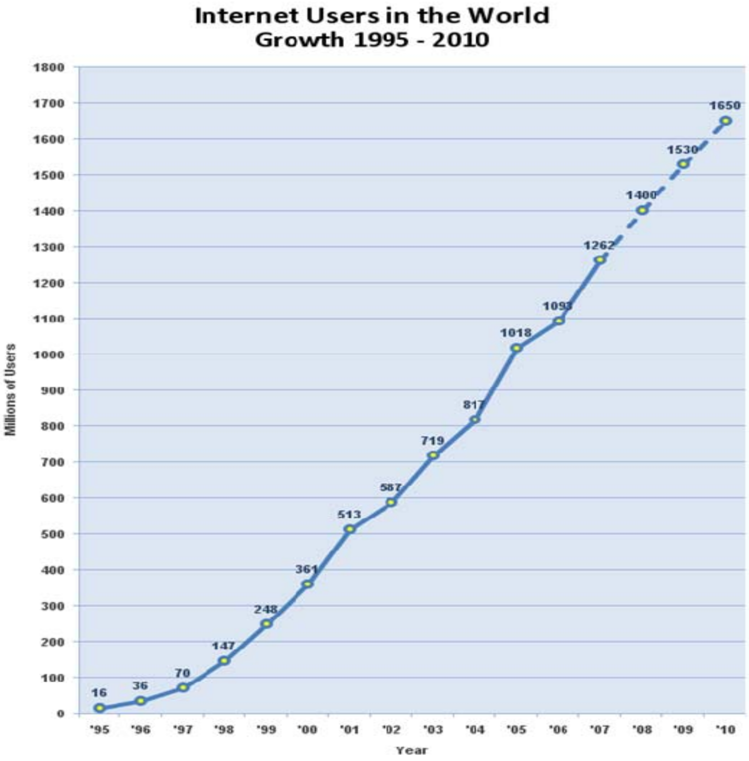

Figure 1. Number of Worldwide Internet Users (From www.internetworldstats.com)

The age we live in is constantly evolving; the world is becoming globalized in nature and interconnected vis-à-vis the Information Age. Within the Information Age, we see there is a dire need to protect a nation’s critical infrastructure; otherwise, the next large-scale attack against a nation could occur through a coordinated cyber strike on the systems that control its infrastructure. A well-coordinated hacker attack on systems that control nuclear power plants or hydroelectric dams could result in a devastating number of lives lost. A successful strike could potentially kill hundreds of thousands of people and could cripple a nation’s stability. Similarly, a cyber attack on a nation’s financial institutions could have a grave effect on its national economy and create unease in its national security (Cabana, 2000).

Networked control systems are increasingly being discussed among cyber security experts, because these systems control the main portion of a nation’s critical infrastructure. In October 1999, a hacker openly declared his intentions to release information on how to hack into power company networks and shut down the power grids of 30 U.S. utility companies (Riptech, 2001). Although many nations have seen occurrences of low-level cyber attacks on a daily basis, national leaders are concerned with the possibility of a major cyber attack (U.S. Department of Defense, 2008). Strategies are currently being discussed with the hope of deterring those who seek to attack a nation via cyberspace.

B. CYBERSPACE AND THE FUTURE OF WARFARE

The warning signs of terrorist attacks against a nation via cyberspace have been around for quite some time. But how can attacks by small, networked, non-state actors be effective against powerful nations, whose conventional and nuclear forces can not be matched on the battlefield? Are nations not prepared for and better defended against cyber attacks that could affect critical national infrastructure?

It is likely that some nation’s adversaries would like nothing more than to launch a cyber attack that cripples the nation and its citizens. Following the terrorist attacks on September 11th, the United States launched many initiatives to deter future physical attacks within its borders. However, the growing dependence on technology, networked within the public, private, and government sectors of a nation has created vulnerabilities to cyber attacks that could turn out to be a nation’s Achilles' heel (Goodin, 2008a; Goodin, 2008c; Iverson, 2004; Leyden, 2008; Meserve, 2007; Meserve, 2008).

Even though some cyber security experts feel many actors, both state and non-state, currently lack the capability to launch and sustain massive cyber attacks against an adversary’s critical infrastructure, they may not lack this capability for long (Greenemeier, 2007). Some believe that an attack large enough in scale to cause mass disruption in critical infrastructure systems requires at least two to four years to develop the tools and another six to ten years to coordinate and prepare for the cyber attack (Wilson, 2008, p. 18).

During a speech to the United States Naval Academy graduating class in May 1998, President Bill Clinton stated that “our foes have extended the fields of battle from the physical space to cyberspace....these adversaries may attempt cyber attacks against our critical military systems and our economic base” (Newsbytes News Network, 1998). This recognition by a world leader reveals that vigilance should be practiced over a nation’s cyber infrastructure, as cyberspace has become a new avenue to launch attacks from anywhere on the face of the earth. The issue here is that many countries have been complacent about protecting their information infrastructure (*The Economist*, 2007b).

The exponential technological growth and low cost of entry to operate within cyberspace have created a domain where state and non-state actors, including terrorist organizations, can safely hide in the shadows of anonymity that cyberspace provides. Cyberspace is proving to be a powerful arena to recruit, train, and equip new hackers, as well as to coordinate and launch cyber attacks (Allard, 2006).

C. DEFINING CYBER ATTACKS AND CYBER WARFARE

Before progressing too deeply into exploring the concept of cyber deterrence, it is worth noting that this research is not looking to deter every type of cyber attack that exists. For example, it is impractical to say that a nation is looking to deter hackers from penetrating and defacing websites. However, it is important to understand how this hacker penetrated the security in place. These situations provide those defending the networks with further understanding of vulnerabilities that must be fixed.

Computer network attacks, also referred to as cyber attacks, are a component of the information operations spectrum. Cyber attacks are “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves” (Schmitt, 2002, p. 367). The core of cyber attacks is that a data stream is relied on to execute the attack. Therefore, the means used set cyber attacks apart from other forms of information operations. These means vary widely; they include gaining access to systems to acquire control over them, spreading viruses to destroy or manipulate data, using logic bombs that sit idle in a system until triggered on the occasion of a particular occurrence or at a set time, inserting worms that replicate upon entry into a system and thereby overload the network, and employing sniffers to observe and/or steal data (Schmitt, 2002, p. 367). Like many attacks, there are often mitigation efforts to fix security vulnerabilities or deny attacks, although sometimes they are accomplished reactively as opposed to proactively.

Typically, the image cyber warfare brings to mind is one of generally bloodless attacks that remain in the cyber domain. While some of the basic outcomes of cyber attacks have been looked at as solely virtual thus far, ultimately what takes place in a cyber war may have consequences in the physical domain (Shimeall, Williams & Dunlevy, 2002, p. 16).

D. OVERVIEW

Prior to examining different tactics of cyber deterrence, there is a need to introduce the reader to the concept of cyber deterrence. This will acquaint the reader with its characteristics and will lay the foundation for discussing the application of cyber deterrence methods. This thesis will take a heuristic approach to the feasibility of a nation applying strategic deterrence concepts to the cyberspace domain. The ability to deploy successful cyber deterrence strategies may help a technologically reliant nation avoid becoming crippled from cyber attacks by other actors.

The second chapter on the evolution of strategic deterrence, which examines the methodology and theory through existing literature, is designed to serve a dual purpose. First, it will introduce the reader to the concept of deterrence, its characteristics as well as its achievements and problems. Some of these characteristics will be examined through a brief look at deterrence strategy as a part of a nation's security policy. Subsequently, the chapter will suggest that an update to the concept of deterrence is needed to synchronize with the Information Age we live in today. This will lay the foundation for discussing the concept of cyber deterrence later in this thesis.

The third chapter will examine the emergent cyberspace threat. This chapter will begin with defining the concept of cyberspace. Furthermore, it will discuss the rising challenges and vulnerabilities nations face with their increased dependence on cyberspace. This chapter will discuss why strong offensive and defensive cyber capabilities are needed for nations that employ a large dependence on cyberspace.

The fourth chapter will build on the analysis of deterrence and look heuristically at how deterrence strategies can be applied in cyberspace to lower the threat of a critical attack. The beginning of this chapter will marry the two concepts discussed in the previous chapters into how the concept of cyber deterrence can be defined.

Finally, the concluding chapter will broadly review the analysis of cyber deterrence and discuss its prospects. Furthermore, it will look at how cyber deterrence can be utilized within the national security policies of the United States. A review of the United States' *National Strategy to Secure Cyberspace* will be reviewed to see what policies are currently in place to defend United States its interests in cyberspace and to make recommendations for any changes that may be needed to include in its national security strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FUNDAMENTALS OF STRATEGIC DETERRENCE

> For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.
>
> — Sun Tzu, The Art of War

A. INTRODUCTION

Before we can begin to discuss how deterrence can be applied to cyberspace, it is essential to introduce the reader to the general concept of deterrence. Understanding the concept of deterrence and how it has been applied acquaints the reader with deterrence characteristics as well as its achievements and problems. Some of these characteristics will be examined through a brief historical look at the evolution of deterrence strategy as a part of a nation’s security policy. Subsequently, this chapter will suggest that deterrence needs to be updated to synchronize with the Information Age we live in today. This will lay the foundation of the future discussion on the concept of cyberspace-based deterrence.

B. DEFINING DETERRENCE

Deterrence is generally defined as influencing an opponent, either by denying potential gains or threatening the use of retaliation, in order to prevent the opponent from taking an action that you do not want him to take (Mearsheimer, 1983, p. 14; Morgan, 1977, p. 17). The use of a deterrent strategy is an attempt to avoid the escalation of a conflict to the use of military force. For a deterrent to be successful, the threat must be at a level in which the opponent’s cost of taking action outweighs his benefits. Furthermore, the threat must be one which is perceived as credible, therefore, the actor who is seeking to deter an opponent must show it has the capabilities and intent to follow through with the threat (Morgan, 1977, p. 32; Huth, 1988, p. 4).

In a simpler form, we can encapsulate the concept of deterrence by stating:

> Actor A desires to prevent Actor B from executing Z by denying or threatening actor B with X if it carries out Z

While this is similar to one of the definitions Patrick Morgan (1977) examined in his book *Deterrence: A Conceptual Analysis* (p. 19), it differs in the fact that those we seek to deter today are not only state actors, but also non-state actors, such as terrorists. Additionally, the introduction of the variable *X* represents applying a tailored threat response that is relevant to what the opponent values; further, *X* could imply the denial of its objectives through a defensive posture. More will be discussed on the stratagem of a tailored response later.

Furthermore, a nation typically employs the use of extended deterrence to protect its allies and vital interests from attack (Huth, 1988, pp. 1, 16). The deterrence situation is considered extended if the defender is trying to deter an attack on a third nation rather than on itself. For the analysis of strategic deterrence as it applies to national security, the use of extended deterrence should be assumed to fall under any deterrent strategy studied and presented in this paper.

C. FORMATION OF DETERRENCE STRATEGIES

The use of deterrent strategies has been around in warfare for quite a while. One classic example from Thucydides, described in his *Peloponnesian War* writings, involves instances where militaries sought advantages to entice their opponents away from starting or expanding a war, because the perceived risks were too great (George & Smoke, 1974, p. 12). George and Smoke (1974) compare what we term today as deterrence to the notion of the balance of power (p. 14). The actor who held the advantage in the balance of power often determined how the conflict would evolve. Nations in conflict sought advantages over their opponents to tip the balance into their favor.

Historically, militaries with strong defensive capabilities have had the advantage in land wars. The nation with the defensive advantage was typically able to impose the threat of heavier losses on the invading forces (Quester, 1966, p. 3). For this threat to effectively deter the aggressor, those leading the invading forces needed to perceive that the costs of attacking the target outweighed the benefits.

Most of the deterrence theory we see today was born from the introduction of nuclear weapons and the emergence of the Cold War between the United States and the Soviet Union (Sagan, 1991, p. 79). In order to maintain effective deterrence over adversaries, the development and application of deterrent strategies follow a process based on values, perceptions, capabilities, and actions of the aggressing actor and defending actor (George & Smoke, 1974, p. 97-103). The Flow Chart shown in Figure 2 reviews the fundamental questions that need to be examined in the process of using deterrence.

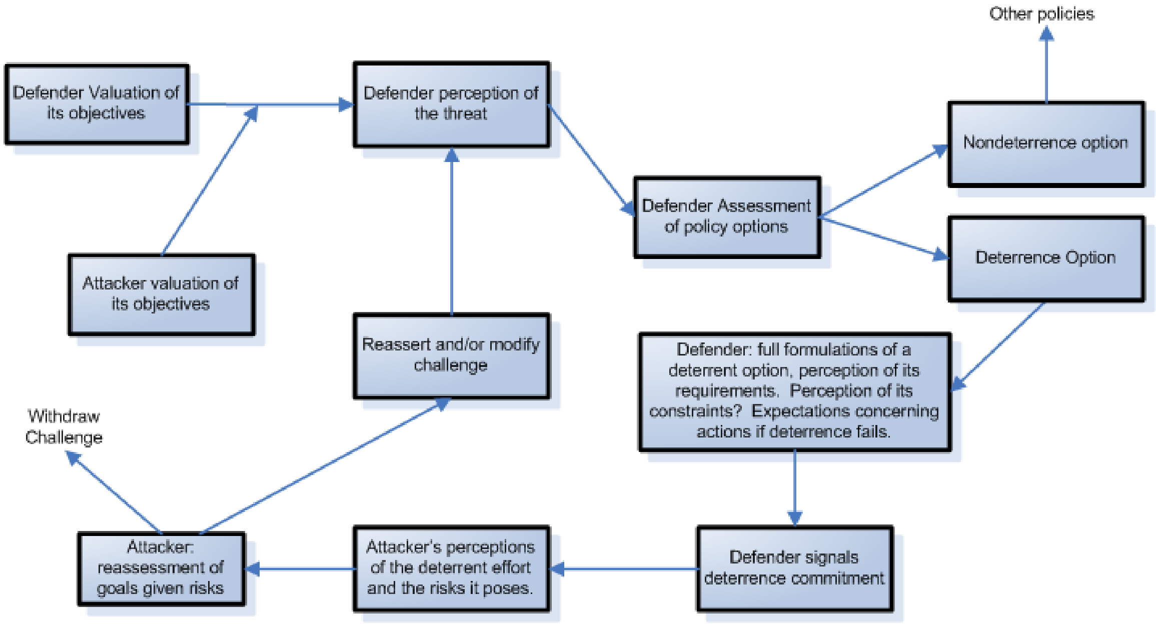
Other policies
Defender Valuation of its objectives
Defender perception of the threat
Nondeterrence option
Defender Assessment of policy options
Deterrence Option
Attacker valuation of its objectives
Reassert and/or modify challenge
Defender: full formulations of a deterrent option, perception of its requirements. Perception of its constraints? Expectations concerning actions if deterrence fails.
Withdraw Challenge
Attacker: reassessment of goals given risks
Attacker's perceptions of the deterrent effort and the risks it poses.
Defender signals deterrence commitment

Figure 2. Flow Chart of Questions on Deterrence (After George & Smoke, 1974, p. 102)

D. THE UNDERLYING PRINCIPLES OF DETERRENCE

When the offense has the advantage in a conflict, the balance of power is in the hands of the aggressor, and the prospects for peace are severely threatened (Quester, 1966, p. 4). The ultimate rationale behind a nation utilizing deterrence is to shift that balance of power back in favor of the status quo. Effective deterrence should been seen as both situation and application specific as we will examine below.

1. Two Deterrent Situations

Patrick Morgan (1977) discusses two different situations in which deterrence strategy exists; the first situation examined is what he terms *general deterrence*. The other situation is what Morgan describes as *immediate deterrence*.

a. General Deterrence

Morgan describes general deterrence as being a situation representative of international politics. Applied in the context of general political and military rivalry where the potential for a conflict is present, however, neither opponent antagonizes the other towards an imminent military confrontation (Morgan, 1977, p. 40). General deterrence is classically observed as a national policy stance on a given issue that could last many years. For instance, throughout the early period of the Cold War, the United States policy promised a massive nuclear retaliation against the Soviet Union should the Soviets launch a nuclear first strike. The United States recognized the threat behind the general policy would result in mutually assured destruction. As the Cold War drew on, the general deterrence policy shifted from massive retaliation to more discriminate methods (Schelling, 1967, p. 190). General deterrence should adapt to match the general environment in which a nation operates. As the general security environment evolves, so should the general deterrence policies of a nation.

b. Immediate Deterrence

Typically one practices and maintains general deterrence to avoid a situation that necessitates immediate deterrence (Morgan, 1977, p. 42). However, should a conflict escalate to a point where an aggressor is seriously considering launching an attack, then the use of immediate deterrence strategies is applied. Furthermore, the actors who seek to deter must be aware of the looming threat and prepare their forces. Immediate deterrence is based on understanding the aggressor's intent to use his or her forces to achieve specified objectives. An adversary merely having the capabilities to attack would fall under the realm of general deterrence (Morgan, 1977, p. 34).

2. Deterrent Methods

The level of defense (denial) and the strength of retaliation (punishment) play an enormous role in the ability to deter an aggressor from conducting attacks. Within the realm of deterrence, it is seen as essential to be ambiguous about the specific details of a response; however, the actor who is attempting to deter must make it clear that the retaliatory actions would have serious ramifications upon the aggressor if they carried through with the action (U.S. Strategic Command, 1995, p 5).

Currently, the methods of deterrence on the battlefield are through conventional, nuclear, and, more recently, tailored means. In John Mearsheimer's book (1983) he states:

> There is a well known distinction between deterrence based on punishment, which involves

> threatening to destroy large portions of an opponent’s population and industry, and deterrence based on denial, which requires convincing an opponent that he will not attain his goals on the battlefield. (pp. 14-15)

Within the context of this statement, Mearsheimer argues that deterrence based on punishment has been historically associated with the use of nuclear weapons; whereas, deterrence through denial has been more typically coupled with the use of conventional forces. The deterrence methods employed by militaries on the conventional battlefield have been around since the advent of warfare. As briefly mentioned earlier, the methodology applied in nuclear deterrence was born in the wake of World War II and the beginning of the Cold War.

Until recently, nations like the United States often practiced a one-size-fits-all mentality when it came to developing deterrence strategies (U.S. Department of Defense, 2006, p. 49). Unfortunately, this method is not suitable in a time when the security threat is constantly evolving; this is where the concept of tailored deterrence comes into being. Each of the respective sections below will define and scrutinize the different methodologies in greater detail.

a. Conventional Deterrence

Conventional deterrence is based on threatening punishment or denying an aggressor his battlefield objectives through the use of conventional forces and weapons (Mearsheimer, 1983, p. 15). In order to effectively apply conventional deterrence, the defenders need to project to the aggressors that they can sufficiently defend the potential attack; furthermore, the aggressors need to perceive that the defenders' retaliation would overcome their defenses and impose a significant cost. Only then can conventional deterrence have a chance of being successful.

Throughout time, nations have sought to develop new offensive and defensive military strategies or capabilities to employ on the battlefield and shift the balance of power to their favor. Once a weapon system was introduced to the conventional battlefield and showed its value there, it became a war over which side could raise the most numbers, or the most advanced version, of a combat system into their arsenals. Eventually, if the aggressors were able to shift the balance of power to their favor, the prospects of their being deterred from attacking would likely fail.

During the Industrial Age, new offensive concepts and military weapons further eroded the expectations of successful conventional deterrence. The advent of the airplane in 1903 and the introduction of armored tanks brought about revolutionary change in the strategies of warfare. The introduction of air forces into conflicts brought with it a level of offensive weapons capabilities that severely disrupted the balance of power. Offensive air firepower provided the military a capability to concentrate firepower and impose higher losses on a specified area. Prior to this, those who occupied the defensive area traditionally held the advantage in a conflict. The airplane shifted the balance of power to the offense in battle (Quester, 1966, p 2-4). Whoever went on the offensive first typically held the advantage. Pre-emptive strikes were the norm in conventional battles, even though no one actually desired war (Quester, 1966, p. 4-5).

Another example of conventional deterrence failure occurred during World War II. The Germans employed highly mobile and mechanized military doctrine, termed Blitzkrieg, in their use of armored warfare. The overall theory of the doctrine promised a quick victory at a very low cost (Mearsheimer, 1983, p 58). When aggressors believe that they can defeat their adversaries rapidly and decisively, deterrence is likely to fail (Mearsheimer, 1983, p. 203). The nature of warfare continued to evolve at the end of World War II. After the United States developed and used the first, and second, atomic weapons on Japan, a threat of apocalyptic proportions emerged in military doctrine in the form of nuclear deterrence.

b. Nuclear Deterrence

The premise behind nuclear deterrence theory was to influence an adversary’s actions by means of threatening the very existence of its homeland with a punitive nuclear attack (Payne, 1996, p 6). Nuclear weapons are purely offensive in nature. Building a nuclear deterrent strategy was considered extremely revolutionary compared to the concept of a retaliatory attack through conventional deterrence. The retaliation through the use of a nuclear weapon would come without the need to use conventional military forces first to defeat any defenses in place (Morgan, 1977, pg. 31).

The theory behind why nuclear deterrence has worked against those who do not possess nuclear capabilities is that it produces responsible behavior as a matter of self-preservation. Although one could continue to improve anti-ballistic missile technology, which aims at denial deterrence, it has never guaranteed a perfect defense against nuclear missiles. The cost of anything less than an infallible defense would be catastrophic in nature (Morgan, 1977, pp. 30-31).

One illustration of nuclear deterrence occurred prior to Operation DESERT STORM in January 1991. The United Stated conveyed a message that any use of weapons of mass destruction (WMD) by Iraq on any Coalition forces would be met with swift and severe consequences (Russell & Wirtz, 2002). The use of an ambiguous threat led many to believe that the United States would retaliate on a massive scale with nuclear weapons.

When President George H. W. Bush was asked directly by the press if the United States would use WMD in-turn, the president stated that “it’s better to never say what you may be considering” (U.S. Strategic Command, 1995, p. 7). The rationale behind the ambiguity is that it makes the aggressor think very carefully as to whether the benefits of the attack are worth the potential risks. In the case of nuclear retaliation, the consequences may be as high as the nation’s existence. Although there has been speculation about whether this deterrent actually succeeded in preventing Saddam Hussein from launching chemical or biological WMDs, one could argue the veiled threat was a success since WMDs were not utilized against coalition forces.

Although this threat may have been credible at the time, subsequent information released by the leadership involved said Bush’s nuclear threat was nothing more than a bluff (Bunn, 2007, p. 6). Unfortunately, by releasing this information to the public, should the United States leaders attempt to use nuclear deterrence again, their declaratory threats are much less credible in the eyes of their adversaries. The deterrent threat of nuclear retaliation is waning, and new deterrence doctrine needs to be established to match the nation’s international deterrence policies with its operational capabilities.

The use of nuclear weapons has its fair share of opponents around the world, who declare their use morally reprehensible because of the massive death and suffering they would cause. Ethically, could the United States or any other world power actually bring itself to use these weapons if it became necessary to follow through on a threat? If a nuclear nation truly wanted to use nuclear deterrence, doing so must be seen as morally acceptable to its own society in terms of retaliation (Bunn, 2007, p.7). Furthermore, it may be difficult to use nuclear weapons against an actor who does not have weapons of mass destruction.

In a transcript released on September 12, 2008, the Honorable James Schlesinger, serving as the Chairman of the Task Force for Nuclear Weapons Management, stated “what has been the long-time practice during the Cold War and subsequent years of developing the theory and doctrine of deterrence has more or less disappeared . . . the doctrine of deterrence has, to a large extent, been forgotten” (U.S. Department of Defense, 2008). The time has come to shed the Cold War nuclear deterrence mentality and look at ways to apply deterrence to the multiple actors that threaten the world stage.

c. Tailored Deterrence

Tailored deterrence is a new term coined by the Bush Administration in its 2006 Quadrennial Defense Review (QDR); however, the aspects that make it up, tailoring capabilities to meet a specific challenge, tailoring messages that are situation dependent, and tailoring actions to specific actors have been around and evolving over the past decade (Bunn, 2007, p. 2). The application and use of a tailored strategy truly turns deterrence into an art form. The art is in developing a message that is actor specific and tied to specific situations. Whereas nuclear deterrence was focused primarily on the punishment aspect of deterrence, tailored deterrence goes back to emphasizing the use of both denial and punishment (Bunn, 2007, p. 2).

To accomplish tailored deterrence, the 2006 QDR discusses applying a particular mix of the New Triad capabilities against specific challenges (Bunn, 2007, p. 1). The New Triad capabilities were described in the 2001 Nuclear Posture Review report[2] as being composed of

[2] The 2001 NPR was classified overall; however, the unclassified foreword by Donald Rumsfeld was released to the public.

offensive strike systems – both nuclear and non-nuclear; defensive systems – both active and passive; and revitalized defensive infrastructure (Rumsfeld, 2001, p. 1). The use of the New Triad capabilities for tailored deterrence allows for the use of a mixture of nuclear and non-nuclear weapons, both kinetic and non-kinetic, and may help a nation meet the cyber challenges in today’s Information Age.

Tailoring communications will allow a nation to focus the message of its intent to specific actors (Bunn, 2007, p. 1). The message that a nation seeks to spread in deterring an actor from specific actions may vary in peacetime and crisis situations. The message conveyed during each of these situations would be a part of a nation’s general and immediate deterrent strategies.

In the 2006 QDR, the declaration for the need of a wider range of non-kinetic strike capabilities calls upon the use of cyberspace as a means for future operations (U.S. Department of Defense, 2006, p. 49). Within the realm of cyberspace, the Department of Defense (2006) recognizes that it needs to strengthen the coordination of defensive and offensive cyber missions (p. 51) to counter the growing threat to its national security within cyberspace. Deterring actors from cyber attacks will be needed to meet the challenges in the face of the growing cyber threat.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE GROWING CYBER THREAT

> The enemies of peace realize they cannot defeat us with traditional means. So they are working on new forms of assault: cyber attacks on our computer systems.
>
> - President Bill Clinton, 1999[3]

A. THE CYBERSHOT HEARD 'ROUND THE WORLD

For more than three weeks in April and May 2007, the government of Estonia was the target of multiple computer network attacks in both its public and private sectors. The results of these attacks were briefly crippling, as much of the country's critical infrastructure is integrated into its cyber infrastructure. The reported origin of some of these attacks was Russian government servers, which led people to believe it was a state sponsored attack. However, further analysis showed that most of the attacks came from non-government servers in Russia and other countries (Landler & Markoff, 2007).

In the assault, computer hackers used robotic cyber armies, termed Botnets[4], to flood Estonian critical infrastructure nodes with so much data that they could no longer process their legitimate traffic. The data load targeting these nodes was measured by security experts at

[3] The White House Office of the Press Secretary, "Remarks by the President On Keeping America Secure For the 21st Century," January 22, 1999, www.whitehouse.gove/WH/new/htm1/19990122-7214.html, August 31, 1999.

[4] A Botnet is defined by Wikipedia (http://en.wikipedia.org/wiki/Botnet) as a collection of software robots, or bots, that run autonomously and automatically often while hidden to the actual owner of the machine. They run on groups of computers compromised by hackers and controlled remotely. This term can also refer to the network of computers using distributed computing software.

90 megabits of data per second[5] for 10 straight hours (Landler & Markoff, 2007). This data stream cut off contact to online banking systems, online news agencies, and government communications. What we have here is the first instance of an international cyber conflict.

It is believed that these attacks stemmed from the removal of a World War II-era Soviet statue in an Estonian city plaza (*The Economist*, 2007a). Who should be to blame for the attacks? There was serious speculation that the Russian government was behind the attacks, because they appeared unwilling to quell them (Evron, 2008, p. 124). There were many early warning signs of the impending attacks on Estonia’s cyberspace infrastructure. Russian-language Internet forums had multiple posts with both basic instructions on how to carry out the attacks and target lists that maneuvered in reaction to Estonian defenses (Evron, 2008, p. 122-123).

The anonymity that the Internet provides made it nearly impossible to tie the Russian government directly to the attacks. In the analysis following the attacks, technical data seemed to confirm that at least one of the nodes in the attack was within the Russian government. This computer could have been a command and control node which initiated the attacks; however, it could have also been a spoofed IP address or compromised machine that was a part of the Botnet (Evron, 2008, p. 125). While the Estonian government took rapid defensive action in attempt

[5] The data rate of 90 megabits per second (Mbps) is the equivalent of downloading the entire Microsoft XP operating system every six seconds.

to thwart the attacks, will the Estonian government maintain a grudge over this attack and retaliate in the near future?

If the cyber attacks were more organized and used viruses to target certain systems for destruction rather than denial of service, the attackers could have more seriously crippled the Estonian government. If the attackers had found a way to manipulate critical infrastructure control systems, like power plants, dams, or transportation systems, the results could have cost many lives. Governments need to be wary of cyberspace and the threat it poses. If they continue to ignore the potential challenges that remain in cyberspace, these governments might just as well put a bull’s eye on their networked critical infrastructure. This particular incident in Estonia may just be the beginning of future conflict in cyberspace.

B. EXPLORING THE CYBER ENVIRONMENT

In today’s cyber environment, security threats originate from a variety of actors with different motivations. The threat is no longer solely on a state-versus-state level, as the world has dramatically changed since the Cold War. Since the Internet provides a basic, inexpensive, and relatively risk-free avenue to achieve effects that put national security in jeopardy, nations need to be cognizant of the various actors who exist and operate within cyberspace (Evron, 2008, p. 126). In an attempt to establish defense against emerging cyberspace threats, merely understanding the modus operandi of one type of actor will not establish models applicable to other actors.

Furthermore, actors bring to the table their own motivations for pursuing offensive actions in cyberspace. A fall 2008 working group that examined the different levels of cyberspace analysis discussed a variety of things that may motivate different actors. A few examples are that they enjoy the challenge, are curious, seek money, seek notoriety, are ideological, want revenge, want to coerce an opponent, are patriotic, seek to intimidate, and look to demonstrate their capabilities.

Every actor brings their knowledge and motivation to the forefront when exploring and exploiting vulnerabilities in their intended target’s infrastructure. As hackers look for new methods to exploit computer code, the vulnerabilities found within hardware and software platforms are plentiful. Take the Microsoft Windows operating system as an example. The number of lines of computer code in Windows is in the tens of millions; inevitably, techniques have been and will continue to be developed to exploit the flaws found in various software codes (Mitnick & Simon, 2006, p. 35-36).

C. TRANSFORMATION TO THE INFORMATION AGE

The world today is in the midst of a digital revolution, which is influencing the way many nations and corporations operate on a daily basis. Over the past several years, the cyberspace threat has steadily increased to such a level that cyber dependent nations should be cognizant of the danger. It should come as no surprise that cyberspace has become a desired avenue for adversaries to attack, as countless vulnerabilities exist within cyberspace technology that can be exploited by those who understand them; further, cyber attacks can be launched by hackers from anywhere on the globe. Cyberspace allows even small non-state actors, like terrorists, a chance to inflict damage against traditional superpowers. This is a result of the lower cost of entry for adversaries who would be considered weak or non-existent with regard to conventional or nuclear capabilities (Zanini & Edwards, 2001, p. 48). This should be a cause for great concern among state actors.

Although the Estonia cyber attack was dealt with swiftly and the effects were limited, a lesson learned in the aftermath is that a nation’s cyberspace infrastructure can be targeted by its adversaries as a center of gravity. Degrading or preventing access to the Internet can wreak havoc on a nation and undermine the trust the populace exhibits in the system.

An August 2005 computer security report conducted by IBM stated there were over 237 million worldwide cyber attacks reported in the first half of the year (Wilson, 2008, p. 15). This equates to an astounding average of more than 1.3 million daily cyber attacks on systems connected to the Internet. The IBM report looked at attacks as an event, or set of events, deemed to be malicious and intended to cause damage. Approximately 64 percent of these cyber attacks were rather minute in scale and were nothing more than a nuisance; examples include reconnaissance probes to detect vulnerabilities and web defacements (“IBM Report,” 2005). Meanwhile, approximately 36 percent of these attacks had the potential to cause severe damage to targeted systems by shutting down services (“IBM Report,” 2005).

In 2003, cyber attacks cost worldwide businesses approximately $186 - $228 billion (Cashell et al., 2004, p. 10-11). The estimate for 2004 by British firm Mi2g was around $250 billion (Cashell et al., 2004, p. 10-11). Unless defenses improve, this figure will continue to increase as the spread of and dependence on technology and the sophistication of attacks increases. From a national standpoint, governments should be worried by these figures and concerned about the security of their cyberspace infrastructure and the critical infrastructure nodes that ride on its backbone. The only hope to reduce the overall cost, both financially and to national security, is to find a way to deter those staging the attacks.

In 1998, President Bill Clinton launched two presidential directives in an attempt to secure the United States critical communications infrastructure from attacks (Newsbytes News Network, 1998). Although these directives were launched approximately 10 years ago, it appears as if nothing much has been done to secure the nation’s cyberspace infrastructure. The recent Comprehensive National Cybersecurity Initiative is a recent program underway that highlights national resources being invested in securing the nation’s cyberspace infrastructure.

On December 7, 2005 the U.S. Air Force changed its overarching mission to “deliver sovereign options for the defense of the United States of America and its global interests – to fly and fight in Air, Space, and Cyberspace.” The main difference from its old mission was the addition of cyberspace as an area of defense for the United States and its global interests. The impetus for the change is symbolic of how vital cyberspace has become to global powers. The addition of cyberspace highlights the focus and appeal of maintaining our security in cyberspace from those wanting to do harm to a technologically advanced society. The military needs to view computers as a weapons system operating in the cyber domain, much like fighter and bomber aircraft are weapons systems operating in the air domain, and assert that they must be treated as such.

Although the United States, along with many other nations, is increasing its attention to securing cyberspace, it takes a good amount of time and money to develop robust offensive and defensive cyber capabilities. Up until the cyber attacks on the Estonian cyberspace infrastructure in 2007, governments typically felt that security against cyberwarfare meant keeping hackers out of important government computers (*The Economist*, 2007b). Much less thought had been given to protecting against a mass disruption from cyber attacks against the public infrastructure. This leads us to develop a new arena in cyberspace for exploring the application of deterrence. Exercises and real events, like Moonlight Maze and Titan Rain, have proven that cyberspace is far from secure; however, these events have given the United States an opportunity to study the outcome and apply new methods of security. Only time will tell if the current “efforts” to thwart crippling cyber attacks on national critical infrastructure were too little, too late.

D. VULNERABILITIES AND THE IMPACT ON NATIONAL SECURITY

November 2, 2008, marked the 20-year anniversary of the first major attack on the Internet, the Morris worm (Lipson, 2002, p. 5; Marsan, 2008). The worm disabled approximately ten percent of all Internet-connected systems, an estimated 60,000 machines at the time (Marsan, 2008). The effects of the Morris worm opened the eyes of those who were using the Internet to the fact that security needed to be taken more seriously.

Although the damage from the Morris worm was minimal, the launch of an attack that large could be catastrophic today. The effect of disabling ten percent of the nodes today would result in approximately 55 million nodes offline. If every person of a cyber-dependent nation owned a computer and operated in cyberspace it would be roughly equivalent to the populations of the United Kingdom, Italy, or South Korea. [6] If an actor were to develop an attack that could concentrate on an adversary on a scale of magnitude like that of the Morris worm in 1988, the actor could severely impact many nations.

1. Rise of the Botnet Militia

One highly damaging attack tool that has seen increased growth over the past several years is the

[6] According to Wikipedia (http://en.wikipedia.org/wiki/List_of_countries_by_population), retrieved November 8, 2008, the population of the United Kingdom is 61 million, Italy is 59 million, and South Korea is 48 million.

establishment of robotic networks, or botnets. These networks are made up of computers that have been compromised with malicious code, typically unbeknownst to the owner of the machine, which can be controlled remotely from a command and control node through the Internet (Issa, 2008, p. 1; Wilson, 2008, p. 5). Figure 3 is a simple depiction of how a botnet operates. The “botmaster” or person who is responsible for distributing or controlling the bot program launches the malicious software that takes control of the victim’s machine. Once this machine is infected it becomes a zombie under the control of the botmaster and sometimes even spreads to other machines, forming a network that appears hierarchical in nature (Wilson, 2008, p. 6). The botnet then can be used for various purposes like forwarding spam, stealing personal information, or launching distributed denial of service attacks (DDoS).

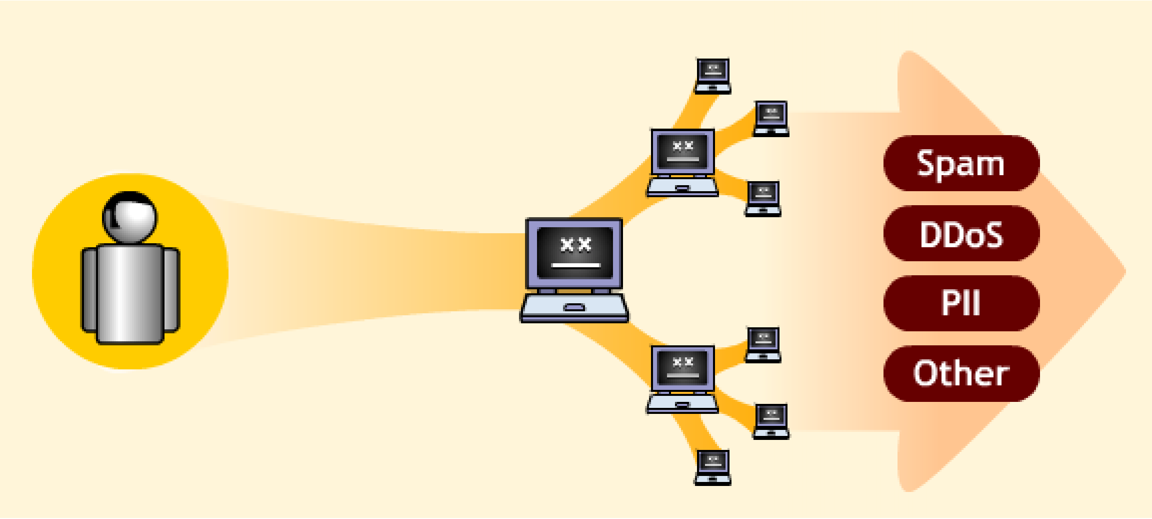

Figure 3. Basic Botnet depiction (From *Business Week*)

Over the past five years, we have seen an astonishing increase in the number of machines infected by malicious software that has been tied to a botnet. Figure 4 depicts the various viruses and worms launched that connected their victims’ machines to particular botnets. Along the y-axis the growth represents the numbers of machines that were tied to the botnets. Some machines have been infected when end-users opened malicious e-mail attachments. Other techniques have found ways to compromise machines without the need for end-user actions. These techniques can exploit vulnerabilities when a user visits websites running infectious code through cross-site scripting and iFrames (Bort, 2007).

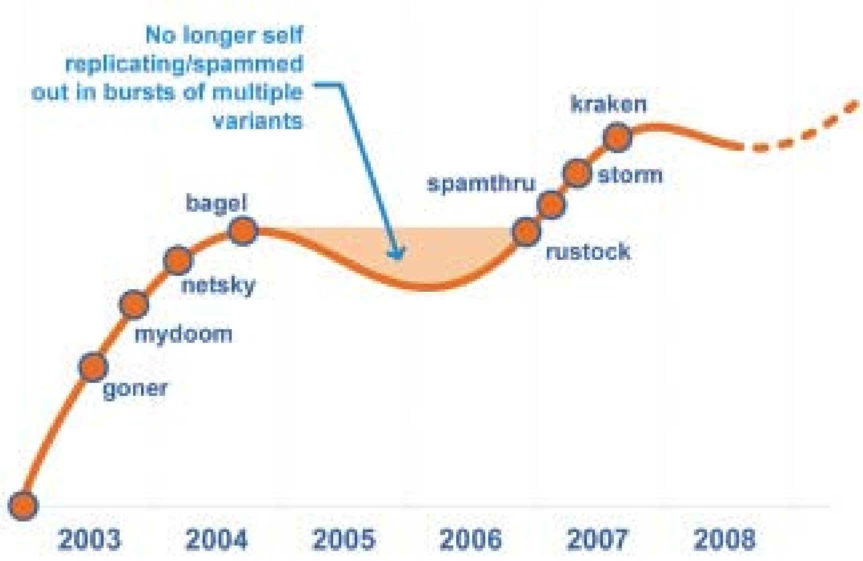

Figure 4. Botnet evolution (From Issa, 2008, p. 2)

Malicious software has created an opportunity for botmasters to rent out their cyber botnet mercenaries on the black market. The criminal cyber element, coupled with the botnets, brings a level of sophistication to the computer network attack arena. It makes it easier for those who rent botnets to target their attacks without much computer knowledge. One such botmaster supposedly made $100,000 from advertisers to infect machines he owned with malicious software (Wilson, 2008, p. 5). While the criminal element is seemingly using botnets more for fraud, extortion, and spam (Wilson, 2008, p.6), nations need to be mindful of the potential use by terrorists or other actors to launch attacks on vulnerable critical infrastructure that may affect national security.

If we examine Figure 5 and Figure 6 provided by the Shadowserver Organization,[7] we see a trend in botnet activity from December 2005 until November 2008. In the first figure we see that the number of command and control servers has doubled from approximately 1500 to 3000. The more troubling figure is the latter, as it explores the number of active botnets out in the wild. If we look at the trends we see an average of 250,000 to 500,000 active bots; however, there was a spike in the number between April to mid-June 2007 that hovered around 3 million active bots. While the significant drop in numbers could have come from security patches to compromised machines, it is believed that there are a large number of inactive bots in hiding until the time is right, remaining hidden as long as possible so that the nodes are not compromised (Bort, 2007).

[7] Source: http://www.shadowserver.org, retrieved November 15, 2008.

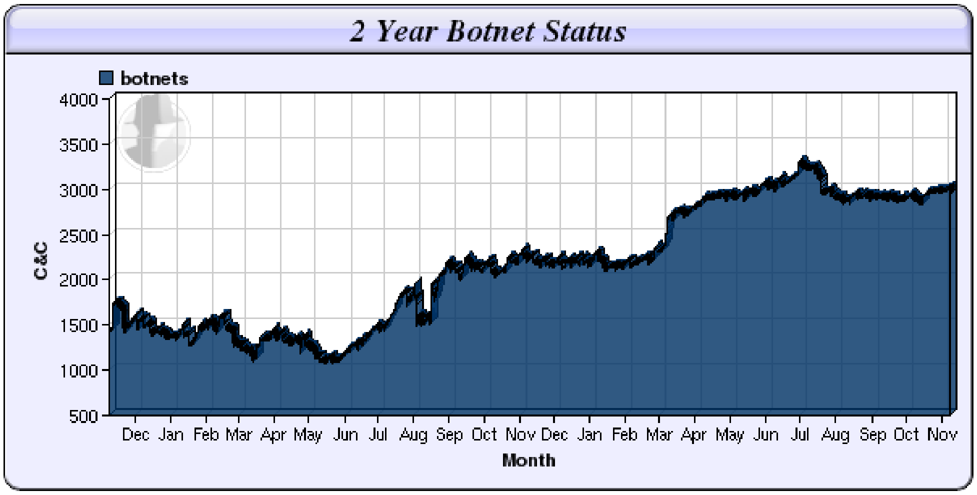

Figure 5. Number of Botnet C2 Servers, Dec ‘05 – Nov ‘08 (From www.shadowserver.org)

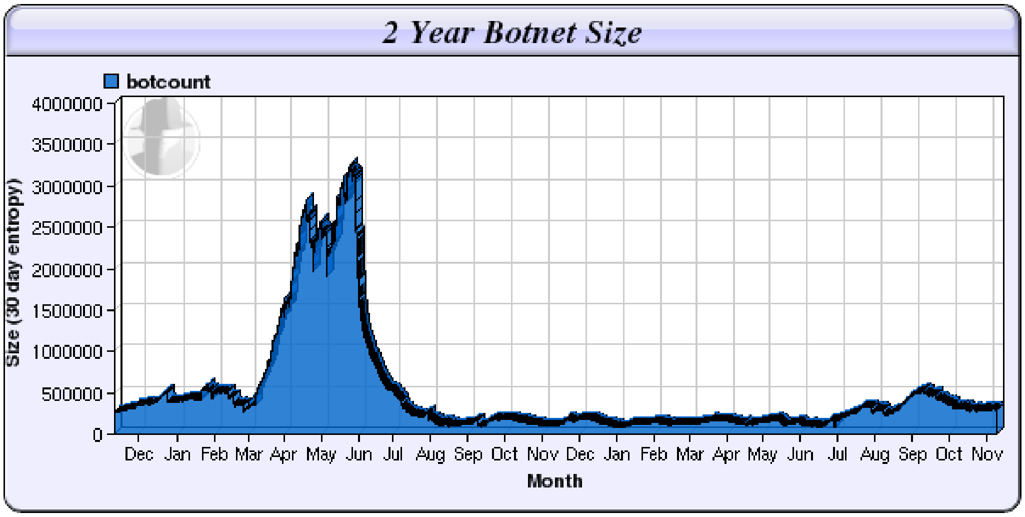

Figure 6. Number of active Botnet nodes, Dec ‘05 – Nov ‘08 (From www.shadowserver.org)

As discussed in the Estonia example earlier, the use of botnets played a key role in degrading and denying information flow to portions of the country’s critical infrastructure. Even more frightening is that the spike in nodes from April to mid-June, shown in Figure 6, coincided with the DDoS attacks on Estonia. The spike in active botnets may offer support that there are many inactive and hidden nodes waiting to launch attacks on unsuspecting targets. This particular incident in Estonia provides evidence that the threats to national security from botnets are real. A concentrated mass botnet DDoS on transportation systems, such as air traffic control networks, could disrupt command and control of aircraft in flight, putting aircraft at risk. Another attack could cripple networked emergency service nodes, slowing or degrading responses to emergency situations and putting lives in jeopardy.

2. Other Critical Vulnerabilities

At the August 2008 Black Hat convention in Las Vegas, security expert Dan Kaminsky unveiled his team’s discovery of a serious Domain Name System (DNS) cache poisoning flaw. DNS is a critical function of the Internet which resolves web addresses, like www.cnn.com, into IP addresses, such as 64.236.90.21. To simplify it further, DNS is like the phone book for the internet.

The DNS cache poisoning flaw allowed the attacker to add a DNS entry to a targeted server, which, if successful, could redirect a user to an alternate site with malicious intent. This attack floods the targeted DNS server with multiple requests for a specific domain name with different variations – for instance xy36.yahoo.com, zb92.yahoo.com and so on – while the attacker attempts to respond to the given server with the random transaction number assigned (Goodin, 2008b). This random transaction number, one of 65,536 possible IDs, is used to thwart corruption of the session. Once the attacker responds back with a correct ID he can subvert the entry in the DNS server with the IP address of his or her choosing (Davis, 2008; Halley, 2008).

Once this flaw is executed, the attacker can redirect traffic to a site that could install malicious software onto the victim’s machine or mirror the victim’s intended site. The latter example could be especially problematic as the mirrored site could be set up to capture login and password information from the victims, otherwise known as “pharming.” Pharming can be set up to appear legitimate to the end-user as the web address entered is legitimate, but since the DNS server was altered it redirects to the alternate IP address (Davis, 2008; Halley, 2008). Pharming of login information may typically be focused on the criminal element for financial gain; however, this information could be used by an actor looking for administrator access to control and exploit pieces of the national critical infrastructure.

E. THE NEED TO PREVENT A ‘DIGITAL PEARL HARBOR’

Over the past decade, the media have been focusing on how vulnerabilities within cyberspace could be turned to affect national security. Supervisory Control and Data Acquisition (SCADA) systems are being discussed by cyber security experts, because these systems are increasingly vulnerable to cyber attacks. Since these systems are used to control the main portion of a nation’s critical infrastructure, the loosely secured systems pose a serious weakness to a nation.

Historically, threats to SCADA systems were mostly internal, resulting from accidents, acts by disgruntled employees, or other inappropriate employee activity (Iverson, 2004). Analysts have seen that from 1982 to 2000 approximately 70 percent of the problems came from insiders while the remaining 30 percent were from external sources. However, times are changing as the world is becoming ever more connected through the Internet. The number of externally generated security incidents has jumped to approximately 70 percent in reports from 2001 to 2003 (Iverson, 2004).

SCADA control systems typically run two operating systems. The first uses Windows or UNIX for the operator console. The security on this system is role-based, determined by the employee’s position (Brown, 2002). The second operating system is the actual control processor which responds to commands with changes to the physical infrastructure system. This is the system a hacker would use to shut down a power grid or enter commands that could physically destroy the equipment.

There is a great misconception that SCADA systems reside on a physically separate network (Riptech, 2001). This second operating system typically lacks security as it was originally designed to operate in isolation. Ideally, these systems should have been connected to the main control centers through private telecommunications links; however, this method was tremendously expensive and companies found a way to let the Internet carry the SCADA system information (Brown, 2002).

A May 2008 report addressed concerns that the infrastructure of the Tennessee Valley Authority, the United States' largest public power company with over 9 million customers, had multiple cyber vulnerabilities (Epstein, 2008; Goodin, 2008a; Meserve, 2008). A quick look at the TVA public website, http://www.tva.gov, shows that the company maintains 3 nuclear power plants, 46 dams & reservoirs, and 18 fossil fuel power plants. Vulnerabilities like this are not specific to the United States. In the United Kingdom, after recent targeted Trojan attacks, a warning was issued that cyber-terrorists were attempting to take out their national power grid (Leyden, 2008).

In September 2008, SCADA attack code was released to the public by a penetration tester following the software vendor deflecting the severity of the exploit (Goodin, 2008c). This exploit would have allowed hackers to insert code into the system and given them authority to control the infrastructure of gas refineries. While some could argue that the release of the attack code was to fix the flaw rather than instigate malicious intent, it did convey a great risk to that sector of the critical infrastructure. For those who believe that a cyber attack could not actually affect the physical infrastructure that controls critical national infrastructure, the United States Department of Homeland Security demonstrated a cyber attack on a test power generator that eventually destroyed the generator (Meserve, 2007).

Since the Morris worm was first launched 20 years ago, we have seen an evolution of various actors and motivations for cyber attacks. Many of the early attacks involved individual hackers looking for challenges and notoriety as part of the hacking elite. Over the past several years, the trend has shifted to individuals and small organizations that are more interested in the economic value these exploits bring. Now, we are seeing warnings being raised, as nation-states and non-state actors may soon possess and utilize their cyber capabilities to affect national security through attacks that could significantly degrade portions of a nation’s critical infrastructure (Meserve, 2007; Epstein, 2008; Goodin, 2008a; Goodin, 2008c). These warnings expound the greater risk of cyber attacks by an adversary for more than just criminal economic motives. Further, a successful attack on vulnerable critical infrastructure could lead to an effect of disastrous proportions.

The level of sophistication and severity found in recent exploits has increased the level of risk associated in cyberspace. Do these prospects sound alarming? They should. There is a dire need to prevent these attacks from being carried out by actors on critical infrastructure before it is too late.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DETERRENCE STRATEGY IN CYBERSPACE

> Safeguarding our own cyber capabilities while engaging and disrupting our opponents' capabilities is becoming the core of modern warfare.
>
> - Michael W. Wynne

A. PREVENTING CYBER ATTACKS THROUGH CYBER DETERRENCE

The threats in cyberspace are real, and the stakes increase each passing day. The hope to reduce the overall cost, both financially and to national security, is to find a way to eliminate or deter potential cyber terrorist attacks. Although historically conventional and nuclear forms of aggression have been subject to traditional deterrent methods[8] used by many nations, these methods are expensive, time consuming, and potentially too extreme to be employed against an adversary that may be no more than a small hacker group of non-state actors.

In the information domain, where equal damage can be inflicted by individuals or nation-states with an infinite variety of motives, incentives, and notions of rationality, and in which attribution is an unsolved problem, traditional notions of deterrence need rethinking. The past two chapters allowed us to look at the concept of deterrence and explore the ubiquitous threats found in

[8] Traditional deterrent methods are conventional deterrence, which is more denial-based, and nuclear deterrence, which is more punitive-based. Conventional deterrence says that the United States will threaten to send the physical military forces and weapons to fight an adversary. Nuclear deterrence is one that the United States says it will threaten to launch nuclear weapons against an adversary if they attack.

cyberspace. These chapters allowed us to build a framework for analyzing how deterrence can be applied to the cyberspace environment. In order to build an effective deterrent against actors operating in the cyber domain, offensive and defensive capabilities must be built and sustained to operate in the cyberspace environment. These capabilities will be engaged to meet the challenges actors inflict upon the cyber domain.

B. APPLYING PRINCIPLES OF DETERRENCE TO CYBERSPACE

In Patrick Morgan's (1977) book *Deterrence: A Conceptual Analysis,* he defined deterrence simply as the "calculated attempt to induce an adversary to do something, or refrain from doing something, by threatening a penalty for non-compliance" (p. 18). The fundamentals of deterrence, denying the gains from an attack and threatening retaliation if attacked, will not change as technology and warfare evolve, but the stratagems used to employ the methodology will need to change to sustain its effectiveness. Unfortunately, the practice of deterrence today remains in-line with the Cold War mentality.

Taking from what Mearsheimer, Morgan, and all other strategists who studied deterrence wrote, we can apply core concepts to build the definition of cyber deterrence. Cyber deterrence is defined as influencing an actor, either by denying the potential gains of the actor or by threatening punishment through the use of retaliation, in order to prevent the actor from utilizing cyberspace as a means to degrade, disrupt, manipulate, deny, or destroy any portion of the critical national infrastructure.

Deterrent strategy attempts to keep a conflict from escalating to the use of military force, ironically, by means of threatening the use of force. For deterrence to be successful, the threat must be at a level where the actor recognizes that the cost and risk of taking action outweighs the benefits. Furthermore, the threat must be one that is perceived as credible, so the nation seeking to deter an opponent must show it has the capabilities and intent to follow through with the retaliatory threat (Morgan, 1977, p. 32).

C. TAILORING DETERRENCE TO CYBERSPACE – ONE SIZE DOES NOT FIT ALL

In Chapter III, we briefly explored the various actors and motivations that play a role in the cyber domain. Since the end of the Cold War, there has been a shift in the environment which now requires a nation to broaden its strategic deterrence towards a more adaptable approach (Bunn, 2007, p. 1). Ms. Bunn wrote that although the vision for the new environment emerged in official United States' documents in 1995, the term tailored deterrence was not developed until the 2006 *Quadrennial Defense Review Report* (Bunn, 2007, p. 2). Prior to this shift, the United States typically applied the same conventional and nuclear deterrence model to its adversaries. This model was out of touch with the modern world environment.

Patrick Morgan (1977) laid out the two fundamental different deterrence situations, general and immediate deterrence, which describe how a deterrent should be developed against threats to national security (pp. 25-43). Although Morgan may not have been aware of how effective this would have been 30 years later, what he accomplished provided a tremendous framework for how a nation should build effective deterrence policies. It is necessary to understand the rationale behind each situation as it applies to cyberspace.

First, there is a need to have a policy in place that is universally applicable to all threats to national security in cyberspace (Gray, 2003, p. 450); this is the basis for a general cyber deterrence policy. General deterrence relates to opponents who sustain offensive and defensive capabilities to regulate their relationship, even though neither is anywhere near mounting an attack (Morgan, 1977, p. 28).

In Chapter II, it was explained that immediate deterrence reflects a relationship between opposing actors when at least one side is seriously considering an attack, and the opposing side is mounting a threat of retaliation to prevent the attacks (Morgan, 1977, p. 28). Immediate deterrence strategies are considered situation and actor dependent. Strategies that work with one actor may not have the same effect on another actor. Applying the context Morgan provides in his book suggests that in cyberspace there could be more than one given immediate deterrent strategy at a time. In addition, due to the anonymous nature of cyberspace there is a level of unknown that permeates the environment. This is an innate challenge that will be covered in further detail in Chapter V.

For an effective immediate deterrent, there is a level of cultural intelligence needed to understand the attacker.

Comprehending the cultural characteristics of an aggressor is important, as it provides the basic understanding of what defines this type of actor (Inkson & Thomas, 2004, p. 62). The value gained from accurate cultural intelligence is that it allows for the development of immediate deterrent strategies, which could have greater impact on an actor. Building effective cultural intelligence averts applying “mirror-imaging” techniques that could be futile. The basis of “mirror-imaging” is that a nation assumes its adversaries would act just the way the nation would act in a given situation (Lowenthal, 2003, p. 8). A perfect example took place in 1941, when no United States leader would have believed that Japan would start a war with the United States due to the power gap between the two nations (Lowenthal, 2003, p. 8). This gap in power was the very reason Japanese leaders believed that it needed to start a war sooner rather than later. If United States’ leaders had effective cultural intelligence on the Japanese during this rising conflict, they may have built more convincing immediate deterrence strategies to prevent a Japanese attack.

D. ELEMENTS OF DETERRENCE IN CYBERSPACE

In order to develop capabilities to deter cyber attacks, four key elements are necessary: denial, punishment, thresholds, and a clearly articulated national policy. While these elements are essential to cyber deterrence, there are still challenges that must be overcome to strengthen the deterrent effect. These challenges will be explained in more detail in Chapter V.

1. Denial

The concept of denial within cyberspace is critical to successful deterrence strategy. Kenneth Watman, Dean Wilkening, et al. (1995) state the following:

> Deterrence by denial attempts to dissuade an adversary from attacking by convincing him that he cannot accomplish his political and military objectives with the use of force or that the probability of accomplishing his political objectives at an acceptable cost is very low. (p. 16)

For denial in cyberspace, the nation that is applying deterrence must first have strong defenses, able to prevent the benefits gained from cyber attacks, and demonstrate resiliency within its networks.

The concept of defense in cyberspace often conjures the notion of establishing firewalls to protect the perimeters of a network from those outside the network who intend to do harm. Firewalls are an important addition to network defense; however, they are not the end all solution, as they have weaknesses. DDoS attacks against firewalls can easily be used to saturate the bandwidth of the intended target so that no legitimate information would be able to pass through the system. Think of a firewall as similar to a medieval castle. If one launches enough data at it, one will eventually be able to overwhelm the defenses. Moreover, firewalls only recognize and repel what they are programmed to do. Inevitably, there will be openings within the defenses to allow "legitimate" traffic to pass. Skilled hackers have no problems penetrating the defenses of a firewall. Hackers often utilize tools to determine the types of traffic that are allowed to pass through and search for weaknesses in their design. Additionally, hackers can find legitimate computers internal to the network which may have exposed vulnerabilities. The hackers can exploit the vulnerabilities within the networks as a way to bypass firewalls.

The 2006 QDR suggested adopting a defense-in-depth planning approach to protect critical information from a nation's adversaries (U.S. Department of Defense, 2006, p. 51). A defense-in-depth approach would layer network defenses, giving the defender more time to react and respond to the attacking adversary. From a historical perspective, the defense-in-depth approach has been superior for the defender to combat a blitzkrieg attack from its adversaries (Mearsheimer, 1983, p. 49). As seen in cases of cyberwarfare, one may view a computer network attack as a type of blitzkrieg strategy, a "bitskrieg", employed through cyberspace. Attacks are typically launched in such a way as to quickly penetrate any current cyber defenses in place, steal or manipulate data, place backdoors on the system, and leave. A well-designed defense-in-depth network may slow cyber attacks down enough for security experts to shift defensive resources in response to attacks and prevent large-scale attacks.

Next, resiliency of the network should be exhibited to thwart attempts by actors attacking the national critical infrastructure. Resiliency can be maintained through scheduled backups, so that the critical information maintained within a system can be quickly restored after an attack. Additionally, alternate data paths and alternate equipment should be readily available to implement contingency plans during sustained attacks. These devices and network paths can be kept offline until necessary. Some governments and/or organizations may already have contingency plans in place if their current cyberspace infrastructure becomes inaccessible. Reliable backup provides extra redundancy to critical nodes in the infrastructure, which adds to the resiliency of its network. The strength behind resiliency in regards to deterrence is that it drives the cost of a successful cyber attack up for an adversary to achieve his or her intended effects.

Finally, nations should continue to develop and leverage tactics, techniques, and procedures from computer network attacks and computer network exploitation activities to improve overall network defense. This means that a nation should use penetration testing to explore and find its own vulnerabilities before another actor can take action upon it.

2. Develop and Demonstrate Overt Punishment Techniques

Instituting denial via defense-in-depth and resiliency only presents the defensive portion of the New Triad in a tailored deterrence approach through cyberspace. In order to build effective deterrent cyber forces, offensive capabilities are needed as well. The second portion of an effective deterrent is that a nation will need to maintain means for holding attackers accountable for their actions – this is through punishment. The punishment of attackers is predicated on the ability of a nation being able to attribute the attacks to a specific actor.

Punishment should not be leveraged solely through the use of cyberspace; a nation should consider punishment over a broad range of all the instruments of power, using diplomatic, informational, military, and/or economic means. The choice of which instrument of power a nation uses as its threat of retaliatory punishment would depend on the type of actor who launched the cyber attack. This returns to the notion of tailoring the deterrent to specific actors and leveraging threats specific to what the adversary believes is important.

Furthermore, a nation should continue to develop offensive capabilities in cyberspace so that it can effectively launch attacks against an actor in this realm. In some cases computer network attack tactics may be the only way to retaliate. One such cyber offensive standoff weapon, discussed by Colonel Williamson, is a military botnet (2008). Unlike traditional botnets that compromise worldwide computers, Williamson’s botnet would be comprised of military computers explicitly set up for this. Although Williamson likened his approach to carpet bombing, his analogy seems a bit sloppy as a botnet would be more like precision guided munitions.

Williamson’s notion of a nationalized botnet raises a question regarding Shadowserver’s botnet data observed earlier in Figure 6. Their data showed an average of 250,000 to 500,000 active bots from December 2007 until November 2008; however, there was a spike in the number from April to mid-June 2007 that soared to approximately three million active bots. In the same figure from July to September 2008 there was another small surge in active bots, although nowhere near the magnitude of the April to June surge. This may correspond to another DDoS attack which occurred in August 2008 against several Georgia government websites that effectively took the sites offline (Danchev, 2008). A frightening hypothetical question to consider is if these attacks against Estonia were actually state-sponsored through Russia, could Russia in fact have its own distributed botnet? While some could argue that the use of unwitting computers from civilian non-combatants could violate the Law of Armed Conflict, distributed botnets are not officially considered militarized weapons. Further, if United States leaders were to write off the possibility of a nation state compromising international computers to form a nationalized botnet, they may fall into a trap of “mirror-imaging.” Unfortunately, the question of a Russian national botnet may be difficult to answer, as the anonymity of the Internet may hide the true explanation for the botnet surge and corresponding attacks. What should be considered is that there is a strong offensive cyber weapon hidden within the shadows of cyberspace. The potential strength of a hidden massive botnet army increases the need for a nation to build better deterrence through denial.

One issue in developing offensive capabilities in cyberspace centers on classification concerns. A specialized tool or tactic may be classified due to the nature of an exploit that an actor may want to keep secret. This is logical enough since once specific details are released, then other actors may acquire the same offensive capabilities, or actors may be able to take defensive actions to stop such an attack. The notion of overt offensive capabilities should focus on the capacity to launch offensive attacks and the ability to demonstrate such attacks. Even the nuclear weapon was developed in secrecy, but once it was developed the United States demonstrated its ability to effectively use the weapon. Further nuclear tests reiterated that the offensive capabilities could be replicated if needed. The same should be done with regards to offensive cyberspace capabilities. A perfect example was the 2007 video release of the Department of Homeland Security cyber attack on a power generator (Meserve, 2007). While the methods that employed the attack were not publicly released, viewers could readily see how the executed cyber attacks physically destroyed the generator after several successful remote commands. Publicizing successful tests of cyber attacks may demonstrate that a nation has the capabilities to launch offensive cyber attacks.

3. Develop Thresholds

Until a deterring party can focus tightly on setting priorities about the assets it desires to protect, and exposing noticeable actions to both protect and respond, it seems likely to be in a permanent defensive posture. The concept of a threshold suggests that a nation’s leaders will develop criteria as to what would constitute a cyberspace attack that would trigger an offensive response to the action. Without a strategy in place where thresholds are developed to measure a given attack, deterrence would not exist. The nation can attempt to understand its measures of tolerance through modeling and simulation scenarios. The scenarios can provide data points for different outcomes – from there it would be up to a nation to classify the probable outcomes into its threshold levels. A nation can build its deterrent strategies from the potential outcomes of cyber attacks. A nation's thresholds should not be public in nature as they would articulate what an actor may be able to get away with; however, a nation's intent to respond to a given attack via cyberspace must be publicly known through its national security policy.

4. Develop and Articulate National Policy

In the case of cyber deterrence, the general cyber deterrent policy of a nation builds on the definition of cyber deterrence given earlier and explains how the nation plans on handling any threats. While a successful cyber deterrent can be built by a nation that has overt offensive capabilities and strengthened cyber defenses, one cannot begin to deter without a clearly articulated policy. Without a clearly articulated message that is received by, relevant to, and understood by other actors, deterrence will likely fail (Bunn, 2007, pp. 6-7).

At a fall 2008 workshop hosted by the National Defense University on Cyber Deterrence, there was debate as to whether a cyber deterrent policy should be explicit or ambiguous in nature. The majority view was that the declaratory policy should be ambiguous in nature, similar to Israel's obscure nuclear deterrent strategy. An example of cyber deterrence policy could be that a nation perceives an attack via cyberspace directed towards any of its components of critical infrastructure as an act of war. A nation could further compare an attack in cyberspace to a kinetic attack on itself or its allies, and state that it will respond to that attack proportionately. The policy should be worded in such a way that applies to all actors that threaten a nation’s security. An ambiguous policy would keep actors guessing if their actions would generate a retaliatory response from the nation once attacked. However, an ambiguous threat can sometime lead to deterrence failure if the message is not received and understood by the adversary.

E. APPLICATION OF CYBER DETERRENCE METHODS

What must be remembered in deterrence is that, for the deterrent threat to be perceived as credible, the one who is seeking to deter must show it has the capabilities to deny the adversary its objectives and launch a successful counter-strike. Although it may be possible to deter actors solely through denial, the lack of retaliatory responses can inhibit the prospects for successful cyber deterrence. The defender must show its intentions to follow through with the threat of retaliation. The deterrence concepts through denial and punitive actions are the basis of a valid deterrent in cyberspace. The problem lies with the need to overtly show that an actor possesses some offensive and defensive cyber capabilities without showing its full hand. Since many cyber capabilities might be used in a single shot capacity before being rendered ineffective, actors may use their tools solely in a covert or clandestine fashion. Without making its intentions and a few of its capabilities known to the aggressor, the aggressor may not accurately perceive the message and cyber deterrence would fail. Furthermore, the deterrent threats issued by a nation must be morally acceptable to its own society, otherwise the deterrent will be perceived as worthless by the opposing actor (Bunn, 2007, p. 7).

Once policies and thresholds are established, the nation will need to quickly determine the proportionality of response once attacked. A nation should take great care to determine the level of response to prevent escalation of a conflict. The response should be costly enough to the actor that he or she can rationalize that the cost of further attacks would outweigh the benefits. Additionally, immediate deterrence must continue to be practiced to prevent further escalation. There is a need to ensure the level of response does not reach a tipping point where the actor believes they have no choice other than to escalate.

When asked how the concern of cyberwarfare towards national security could be implemented in an Air Force Strategic Command, the Honorable James Schlesinger stated “cyberwarfare is one of our serious problems and that it is – leads to the same kinds of considerations that one has with regard to nuclear deterrence – in this case, deterrence of cyberattacks” (U.S. Department of Defense, 2008). Many believe actors found within cyberspace are ramping up to sustain a battle fought asymmetrically. If one reads the articles being published, one might think that doomsday is right around the corner. The art of deterrence can be applied to alleviate the threats to national security. To effectively build deterrence in cyberspace, a nation’s leaders need to understand the fundamental principles, necessary elements, and essential processes; however, there are challenges that still need to be overcome. These challenges will be discussed in further detail in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE PROSPECTS FOR CYBER DETERRENCE

> Some problems are so complex that you have to be highly intelligent and well informed just to be undecided about them.
>
> — Laurence J. Peter

A. CYBERSPACE CHALLENGES AND RECOMMENDATIONS

Cyber deterrence may prove to be a wicked problem – one that evolves as new solutions are considered and/or implemented (“Wicked Problems,” 2008). As vulnerabilities are fixed in cyberspace or solutions are added to make cyberspace more secure, new problems are often created. To surmount these challenges, further research and analysis should be undertaken. The challenges in cyberspace are derived from technological limitations, policy and regulation issues, and the ripple effect of poorly understood changes.

When the Internet began its modest life in 1969 as ARPANET, protocols were developed to ensure the survivability of the network. However, security was simplistic and sometimes even non-existent (Lipson, 2002, p. 13-14; Mitnick & Simon, 2002, pp. 7-8). As experts look back on the development of protocols now, this lack of attention to security is seen as a serious design flaw. Requirements to track and trace malicious actors across international borders may never have been envisioned (Lipson, 2002, p. 14). Although this chapter addresses four challenges to cyber deterrence, these are not the only ones. As cyber security evolves, increasing security and building avenues to overcome these challenges, new challenges may emerge.

1. Attribution

The first challenge, attribution, is a serious concern when analyzing computer network attack operations. The Internet provides a level of anonymity that makes it extremely difficult for defenders to understand who may be conducting cyber attacks. While intrusion detection systems and other sensors may identify suspicious activity within a nation’s networks, it may be difficult to determine where this activity originates and what motivates it. In real events like Titan Rain, cyber intelligence techniques have been able to trace the source back to a specific region of the world (Shannon & Thornburgh, 2005). However, it has been extremely difficult to determine who was behind the attack or even whether it was a nation-state or non-state actor. The lack of attribution for cyber attacks significantly limits the prospects for precise retaliatory actions.

The anonymity offered by the Internet allows attackers to conceal their locations. Botmasters, for example, often use their international networks of computers to launch DDoS attacks on their intended targets. The command and control nodes are typically computers that have been compromised. This leaves a network of nodes separating, both physically and virtually, the botmaster from the immediate sources of attack. The other methods of attack, described in Chapter I also offer elements of anonymity.

Cyber attack tools (computer programs) can be written and executed without revealing ownership of the “weapons.” While some networks require usernames and passwords to gain access, hackers are often able to circumvent the security through social engineering or the exploitation of software vulnerabilities. The possibility of actors gaining access to a network under the auspices of another identity only adds to the difficulty of attributing cyber attacks to a specific actor.

One recommendation for establishing better attribution of cyber attackers is to require stronger authentication. For authentication in cyberspace to work, the redevelopment of network protocols will need to incorporate global authentication features into the network address headers of IP packets. This may assist in examining computer forensic evidence of malware as it spreads; the protocols could provide the route to the originating sender of the malware, identifying the specific person who launched it.

Stronger authentication could implement security measures that incorporate methods of multi-factor authentication. For example, many financial institutions, and even the Department of Defense, are incorporating two-factor authentication into standard processes before users can enter their networks. Two-factor authentication is based on using two of three security features to authenticate access to a system: something a user knows, such as a password; something a user has, like an information-embedded smart card or a token; and some characteristic of a user, namely a biometric (Mitnick & Simon, 2002, p. 84). Three-factor authentication uses all three factors (“Two-factor Authentication,” 2008). Using three-factor authentication makes it even more difficult to repudiate a user’s identity.

The difficulty in developing new infrastructure protocols is that they are often expensive to implement and many people may not support them due to the freedoms lost with this level of security. Further, a major design overhaul of network protocols could take a while to implement. While the cost of development and deployment may appear to be too high for some to support, the cost of compromised data or a loss of national security could be immeasurable depending on the system. Additionally, the implementation of the new protocols could be difficult as multiple systems may have interoperability issues. All too often solution platforms that are developed by different vendors are incompatible with one another and information from one set of systems will not pass information to others. Incompatible security platforms can also increase costs by creating a need to find and build ways to bridge cyber security gaps.

2. The Private Sector

The private sector plays a vital role in national security as it owns most of the critical infrastructure of a nation. Furthermore, the private sector also faces the challenge of developing stronger methods for security in cyberspace. Most pieces of critical infrastructure are not owned by the government, but rather by private companies. Currently, with regards to cyber security, coordination is still lacking in some areas between the private sector and the government. Some initiatives, such as the George Mason University Critical Infrastructure Protection Program, seek to combine security research, inform critical communities, explore concepts, and develop solutions for protecting critical infrastructure systems. However, to protect companies that are found within a nation's critical infrastructure, national regulatory guidelines should be established.

Depending on the regulations, it may be a challenge to get the private sector to adhere to regulatory guidelines for operating in a nation's cyberspace infrastructure. However, it is in their best interest to get involved. Critical infrastructure protection is not only about national security, but also about the strength of a nation's competitiveness in the world market.[9] For example, at the 2008 National Defense University workshop on Cyber Deterrence, one panelist stated that the private industries operating within the United States' national critical infrastructure contribute roughly $6 billon to the nation's gross domestic product. While the financial gains are critical for the government to be competitive in the world market, security in cyberspace should also be critical to the nation.

Successful cyber attacks on any of the industries within the realm of critical infrastructure can severely jeopardize national security and the lives of a nation's populace (Lipson, 2002, p. 11). Furthermore, cyber

[9] The notion of critical infrastructure protection being linked to a nation's competitiveness in the global market was raised by panelists during a collaborative workshop on Cyber Deterrence at the National Defense University from October 20-21, 2008.

security is critical for the privatized industry’s survival. If the United States government should learn one thing from the $700+ billion financial bailouts of 2008, it is that when trouble looms that can weaken the overall strength of a nation, private corporations affected will look upon the government to help save the day. These financial bailouts challenge the perception that the private sector can self-regulate when needed. While developing a system that is fully regulated by the government would create visions of a shift towards socialism, establishing guidelines for the critical private industry to follow may be a safe middle road.

3. International Acceptance

Cyberspace does not belong to any one nation; however, the physical infrastructure does. Furthermore, the openness of information across borders has created vulnerabilities to national security. While closing a nation’s cyber borders to foreign traffic for a significant time may reduce damages from a cyber attack, it could also arrest international trade and the nation’s economy. While cyberspace laws exist within many countries, these laws typically cease to exist outside the borders. The only cyberspace laws that exist in the international arena stem from nations that have treaties with one another. International laws and global standards that define acceptable international cyberspace behavior need to be established.

One such avenue would be to expand the powers of the International Telecommunications Union (ITU) to include development of acceptable international cyberspace standards. The ITU is made up of 191 nations and more than 700 sector members and associates within industry.[10] One recent initiative the ITU is examining is the concept of IP traceback (Rutkowski, 2008). The overall concept calls for next generation networks to consider traceback methods to help law enforcement catch cyber criminals. Regulations and initiatives stemming from a consortium with an international scope this broad may allow for greater international acceptance.

4. Understanding N^{th} Order Effects

As described in Chapter IV, cultural intelligence gives a nation an understanding of its adversaries. A nation’s understanding of its adversaries and their weaknesses are the core for the nation’s retaliatory threats in its deterrence strategy. However, when a nation employs retaliatory threats in its cyber deterrence strategy, the nation needs to ensure it understands the second, third, fourth, and N^{th} order effects. For example, hacking back, or taking a demonstrative action that shuts down or damages computers or network links through which the cyber attack is routed, may or may not reach the attacking party in a timely manner; however, it could cause enormous collateral damage to non-adversaries or to one's own economy, society, or security. This means that any action taken, whether it is kinetic or non-kinetic, can

[10] These numbers come directly from the International Telecommunications Union website at http://www.itu.int, retrieved November 18, 2008.

have consequences outside the scope intended, thereby creating other concerns with which to deal.

Since the negative consequences of an action may be greater than the benefits, the ability to understand Nth order effects of retaliatory responses to cyber attacks is critical to build effective cyber deterrence strategies. In this sense, the nation may stop itself from taking a particular course of action and select another course. Figure 7 contains a course of action process diagram that allows strategy planners to formulate offensive threats that can flush out unintended effects an action may cause. A nation may never know all the effects of an action, but the best it can do is to plan around the effects it can surmise.

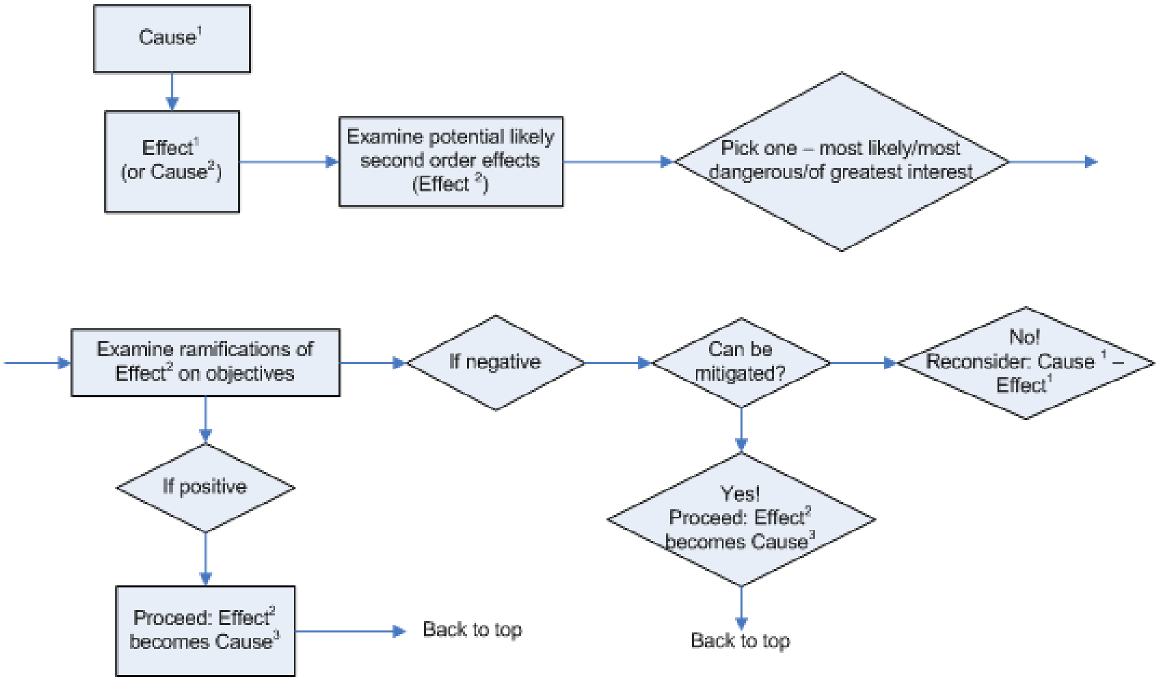
Cause^1
Effect^1 (or Cause^2)
Examine potential likely second order effects (Effect ^{2})
Pick one – most likely/most dangerous/of greatest interest
Examine ramifications of Effect^2 on objectives
If negative
Can be mitigated?
No! Reconsider: Cause ^{1} – Effect^1
If positive
Yes! Proceed: Effect^2 becomes Cause^3
Proceed: Effect^2 becomes Cause^3
Back to top
Back to top

Figure 7. Course of Action Process Diagram (After Miller, 2006, p. 37)

B. IMPLICATIONS FOR NATIONAL SECURITY

Although Estonia came away from their cyber conflict relatively unscathed, a good deal of attention should be paid to understanding the nature of these cyber attacks. Gadi Evron, an Israeli security expert who was brought in to analyze the aftermath of cyber attacks, suggested that governments need to ensure they have a plan in place to defend against a cyber assault. The plan should have a clear chain of command and provide the authority to take certain steps (Nichols, 2008). Evron’s rationale stemmed from his observation that the Estonian defense team lacked the authority to enforce its recommendations to the various government entities being attacked. Additionally, Evron suggested that law enforcement needs better resources to cope with the growing cyber threat and greater collaboration needs to take place (Nichols, 2008).

The ability of a nation to deter aggressors in cyberspace worked its way into the 2003 Unites States’ *National Strategy to Secure Cyberspace*. While the document does not discuss the creation of a deterrence policy in cyberspace, the strategic objectives within the document are consistent with strengthening the denial aspect of a cyber deterrence strategy. The overall U.S. strategic objectives for cyber security stated (p. viii) are as follows:

- Prevent cyber attacks against America’s critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks that do occur

The *National Strategy to Secure* Cyberspace overtly informs the international audience that the United States takes the cyberspace threat seriously. Although the *National Strategy to Secure Cyberspace* provides a sound foundation for defensive measures in cyberspace, further strategies are needed retaliate against actors who conduct cyber attacks against the nation.

The United States has launched a classified program termed the Comprehensive National Cybersecurity Initiative. Department of Homeland Security Secretary Michael Chertoff describes the work being done in this initiative as the Manhattan Project for the Information Age (Jackson, 2008). The initiative is a step in the right direction, as senior government leaders come to understand that the threats in the cyber world can be as serious as the threats in the physical world. These threats need to be met with a strategy to deter attacks from occurring against the United States and its vital global interests.

C. IS CYBER DETERRENCE ATTAINABLE?

Throughout this analysis the fundamentals of strategic deterrence have been dissected, the growing threat in cyberspace discussed, and the rudimentary characteristics of cyber deterrence examined. The ultimate question is whether cyber deterrence will work if a nation establishes national policies, thresholds for response, strengthened defenses, and overt punishment techniques. While parts of the strategy can be successfully applied today, like stronger defenses, significantly more development is necessary before cyber deterrence can truly be effective.

First, a nation will need to determine what it considers a cyber attack. Whatever a nation defines as its thresholds, should be kept secret. The reason for this is that if a nation’s thresholds were public knowledge, attackers would knowingly get away with every cyber action up to the threshold level that defines an attack. Public knowledge of a nation’s thresholds may actually increase attacks by actors attempting to operate just below them. Conversely, thresholds that are withheld from public knowledge may encourage a “try-and-see” mentality for aggressors to see what actions they may be able to get away with. However, publishing thresholds for response may force a nation to respond which may be inappropriate when all circumstances of the cyber attack are taken into account. A nation that does not respond to a specified cyber attack that met a publicized threshold would ruin its credibility. While the idea of having publicized or secretive thresholds may be a double-edged sword, internal thresholds kept away from public knowledge may have a better deterrent effect by keeping the adversary guessing as to whether or not a nation will respond to cyber attacks. The established internal thresholds are the foundation on which a nation’s decisions to respond and retaliate to a given cyber attack will be made. Cyber deterrence policy will be based on a nation’s concept of its thresholds, the understanding of its ability to deny attacks, and the capacity to retaliate against a known attacker.

Second, a nation will need to formally declare its policy to show that it will defend itself from or retaliate against the perpetrators of cyber attacks against the nation’s critical infrastructure. Without a policy in place, the nation does not have a clear means of communicating that it will respond to cyber attacks; therefore, the deterrent effect is non-existent. While it was argued by some people at the 2008 National Defense University workshop on Cyber Deterrence that a national security policy on cyber deterrence needs to be explicitly clear in nature, the national security policy should be defined in an ambiguous manner. The problem with an explicitly clear policy in response to cyber attacks is similar to the threshold issue. A clear policy could give the attacker the advantage of building the response of a nation into his or her calculus for launching an attack. An example of an ambiguous policy by a nation could be that it states it will retaliate against all cyber attacks against its critical infrastructure, but the nation would not go into the thresholds of what it considers an attack nor will it describe its levels of response. The advantage of a more ambiguous policy is that the attacker would have to fear more of the unknown. The disadvantage of an ambiguous policy is that the attacker may misconstrue the signals and attack.

In the aftermath of the Russo-Georgian War in August 2008, some believed that attacks in cyberspace against the nation helped enable kinetic attacks by the Russian military in the region. While there is no hard proof that Russia was behind these attacks, it is interesting to note that there are similarities between the Georgian attacks and those against Estonia. Cyberspace has given adversaries the capacity to inhibit a technologically dependent nation’s ability to use cyberspace. As actors across the international spectrum are gearing up for conflict in cyberspace, stronger capabilities need to be instituted within international alliances. Such actions must be accompanied by a revitalization of both NATO and the United States' traditionally robust capacity to meet the threats in cyberspace. Specifically, some recognize that NATO must improve capacity to conduct both offensive and defensive cyberwarfare operations to prepare for the future of warfare (O'Donnell & McNamara, 2008, p. 3). In the aftermath of the Estonian cyber attacks, the nation called on Article 4 within the North Atlantic Treaty.[11] Article 4 of the treaty states that "the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened" ("North Atlantic Treaty," 1949). It is possible that Article 4 gave NATO allies an opportunity to analyze the attacks and prepare stronger defensive countermeasures for future conflicts of the same nature.

In cyberspace, the threat is chronic, yet there has never been a major cyber attack that threatened the lives of a nation's populace. Hackers are lurking within the shadows, mapping the networks, building their cyber weapons caches, exploring their options, and perhaps patiently waiting for the most opportune times to strike. Some of

[11] This information was presented by panelists at the 2008 National Defense University workshop on Cyber Deterrence. The panelists were discussing the aftermath of the Estonian conflict and said that since there was no precedent in cyberspace as the attacks being defined as an act of war, which would have triggered Article 5 of the North Atlantic Treaty, it enacted Article 4 to receive support from its allies.

the strength and adaptability shown in the Estonia attacks demonstrates that the actors are able to mass on a target and maneuver to circumvent defenses in place. Much more work in overt offensive and defensive methodologies needs to be established before there can be successful deterrence in cyberspace.

Greater emphasis needs to be put on strengthening the defenses for national critical infrastructure – this will bolster a nation’s ability to deter through denial. Basic perimeter defense is not the answer; however, nations, like the United States, seem to depend on it (Defense Science Board, 2008, p. 19). Some nations seem to be responding to the growing challenges in cyberspace and are allocating resources to develop better solutions. The United States 2009 fiscal budget allocates several billion dollars to the Comprehensive National Cybersecurity Initiative to strengthen the nation’s defensive posture in cyberspace (Pincus, 2008). Specific details are classified, but one would assume that the effort includes looking at security across all critical infrastructures.

Finally, a nation needs to examine its options for establishing retaliatory threats in its cyber deterrence strategies. Since there are a multitude of actors who could attack a nation in cyberspace, different retaliatory approaches are needed. An attack by a nation-state should be handled differently than one by a group of ideological actors. With nation-states there may be more retaliatory options; against another nation-state, a nation may apply a broader array of its instruments of power than against non-state actors. The confidence in deterring powerful nation-states with threats may likely be greater than in deterring other actors because nation-states are more likely to be risk-averse (Bunn, 2007, p.3). Rogue states and non-state actors will be more difficult to deter as these actors may be more willing to take risks; however, a nation should attempt to deter them by understanding, and targeting its threats against, what these actors value (Bunn, 2007, p. 3).

Deterrence can be relatively successful when it affects an actor’s calculus for launching an attack. Deterrent strategies need to be perceived as legitimate and credible and applied in such a way that the costs of an act of aggression outweigh the benefits. Until a nation is able to overcome the challenges in cyberspace, a nation will likely have to emphasize denial deterrence, because the veil of anonymity makes punitive deterrence extremely difficult to accomplish.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allard, T. (2006). “Fighting Jihad in Cyberspace.” In *The Sydney Morning Herald*. Retrieved May 26, 2008, from http:// www.smh.com.au/news/world/fighting-jihad-in-cyberspace/2006/12/01/1164777791383.html?page=fullpage

Bort, J. (2007). *Attack of the Killer Bots*. Retrieved August 23, 2008 from http://www.networkworld.com/research/2007/070607-botnets.html

Brown, A. S. (2002). *SCADA vs. the hackers*. Retrieved July 14, 2008, from http://www.memagazine.org/backissues/membersonly/dec02/features/scadavs/scadavs.html

Bunn, M. E. (2007, January). “Can Deterrence be Tailored?” In *Strategic Forum*, No. 225. Retrieved July 29, 2008, from http://www.ndu.edu/inss/Strforum/SF225/SF225.pdf

Bush, G.W. (2006). *National security strategy of the United States of America*. Retrieved February 2, 2008, from http://www.whitehouse.gov/nsc/nss/2006

Business Week. (2008). *Botnet Threat*. Illustration by Mena, A. Retrieved October 28, 2008, from http://images.businessweek.com/ss/05/05/hacker_botnet/index_01.htm

Cabana, N. C. (2000). *Cyber Attack Response: The Military in a Support Role*. Retrieved September 9, 2008 from http://www.airpower.maxwell.af.mil/airchronicles/cc/cabana.html

Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. (2004, April 1). *The Economic Impact of Cyber* Attacks. CRS Report for Congress. Retrieved July 23, 2008, from http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

Danchev, D. (2008, August 11). *Coordinated Russia vs Georgia cyber attack in progress*. Retrieved October 25, 2008 from http://blogs.zdnet.com/security/?p=1670

Defense Science Board. (2008, August). *Defense Imperatives for the New Administration*. Retrieved October 5, 2008, from http://www.acq.osd.mil/dsb/reports/2008-11-Defense_Imperatives.pdf

Derian, J. D. (1994). [Article on Cyber Deterrence]. Retrieved August 19, 2007, from http://www.wired.com/wired/archive/2.09/cyber.deter_pr.html

Epstein, K. (2008, May 21). *TVA: Vulnerable to Cyberattack*. http://www.businessweek.com/bwdaily/dnflash/content/may2008/db20080521_789460.htm?chan=top+news_top+news+index_news+%2B+analysis

Evron, G. (2008). Battling Botnets and Online Mobs: Estonia’s Defense Efforts during the Internet War. *Science & Technology*, Winter/Spring 2008, 121-126.

George, A. L. & Smoke, R. (1974). *Deterrence in American Foreign Policy: Theory and Practice*. New York, NY: Columbia University Press.

Goodin, D. (2008a, May 22). *Electrical grid overlords take drubbing over cyber attack vulnerability*. Retrieved November 1, 2008, from http://www.theregister.co.uk/2008/05/22/electrical_grid_vulnerable/

Goodin, D. (2008b, August 6). *Kaminsky (finally) reveals gaping hole in internet*. Retrieved November 3, 2008, from http://www.theregister.co.uk/2008/08/06/kaminsky_black_hat/

Goodin, D. (2008c, September 8). *Gas refineries at Defcon 1 as SCADA exploit goes wild*. Retrieved November 3, 2008, from http://www.theregister.co.uk/2008/09/08/scada_exploit_released/

Gray, C. S. (2003). “The Reformation of Deterrence: Moving On.” *Comparative Strategy*, 22, 429-461.

Greenemeier, L. (2007). *Electronic jihad app offers cyberterrorism for the masses*. Retrieved on June 1, 2008, from http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=200001943

Halley, B. (2008, October 20). *How DNS cache poisoning works*. Retrieved November 2, 2008, from http://www.networkworld.com/news/tech/2008/102008-tech-update.html

Huth, P. K. (1988). *Extended Deterrence and the Prevention of War*. New Haven, CT: Yale University Press.

IBM Report. (2005, August 2). *IBM Report: Government, financial services and manufacturing sectors top targets of security attacks in first half of 2005*. Retrieved August 30, 2008, from http://www.ibm.com/news/ie/en/2005/08/ie_en_news_20050804.html

Inkson, K. & Thomas, D.C. (2004). *Cultural Intelligence: People Skills for Global Business*. San Francisco: Berrett-Koehler Publishers, Inc.

Internet Systems Consortium. (2008). *The ISC Domain Survey*. Retrieved October 11, 2008, from https://www.isc.org/solutions/survey

Issa, A. (2008, July). *The Botnet Threat: Targeting Your Business*. Retrieved August 28, 2008, from http://whitepapers.zdnet.com/abstract.aspx?docid=383568

Iverson, W. (2004, November 1). *Hackers step up SCADA attacks*. Retrieved July 14, 2008, from http://www.automationworld.com/print.php?id=957

Jackson, W. (2008, April 8). *Chertoff outlines goals of national cybersecurity initiative*. Retrieved November 12, 2008, from http://www.gcn.com/online/vol1_no1/46080-1.html

Landler, M. & Markoff, J. (2007, May 29). *Digital fears emerge after data siege in Estonia*. Retrieved February 12, 2008, from http://www.nytimes.com/2007/05/29/technology/29estonia.html

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C. et al. (2003). *A Brief History of the Internet*. Retrieved October 15, 2008, from http://www.isoc.org/internet/history/brief.shtml

Leyden, J. (2008, August 26). *Minister warns of national grid hack threat*. Retrieved October 1, 2008, from http://www.theregister.co.uk/2008/08/26/uk_minister_grid_hacker_warning/

Lipson, H. F. (2002, November). *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Retrieved August 15, 2008, from www.cert.org/archive/pdf/02sr009.pdf

Lowenthal, M. (2003). *Intelligence: From Secrets to Policy* (2nd ed.). Washington, DC: CQ Press.

Marsan, C. D. (2008, October 30). *Morris worm turns 20: Look what it's done*. Retrieved November 3, 2008, from http://www.networkworld.com/news/2008/103008-morris-worm.html?fsrc=rss-security

Mearsheimer, J. J. (1985). *Conventional deterrence*. New York, NY: Cornell University Press.

Meserve, J. (2007, September 26). *Sources: Staged cyber attack reveals vulnerability in power grid*. Retrieved September 15, 2008, from http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText

Meserve, J. (2008, May 21). *Study finds TVA vulnerable to hacking*. Retrieved September 18, 2008, from http://www.cnn.com/2008/US/05/21/cyber.attack/index.html

Miller, M. G. (2006). *Thinking About Second & Third Order Effects: A Sample (And Simple) Methodology*. Retrieved November 10, 2008, from http://www.au.af.mil/info-ops/iosphere/iosphere_summer06_miller.pdf

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception*. Indianapolis, IN: Wiley Publishing, Inc.

Mitnick, K. D., & Simon, W. L. (2006). *The Art of Intrusion*. Indianapolis, IN: Wiley Publishing, Inc.

Morgan, P. M. (1977). *Deterrence: A conceptual analysis*. Beverly Hills, CA: Sage Publications.

Newsbytes News Network. (1998, May 25). *Clinton Orders Feds to Protect Networks from Terrorists*. Retrieved May 28, 2008, from http://proquest.umi.com/pqdweb?did=29680772&Fmt=7&clientId=65345&RQT=309&VName=PQD

Nichols, S. (2008, May 23). *Expert dissects Estonia cyber-war*. Retrieved July 1, 2008, from http://www.itnews.com.au/News/76651,expert-dissects-estonian-cyberwar.aspx

O’Donnell, R. & McNamara, S. (2008, September 9). *Confronting the Russian Bear After the Georgian War*. Retrieved November 3, 2008, from http://www.heritage.org/Research/RussiaandEurasia/upload/wm_2056.pdf

Payne, K. B. (1996). *Deterrence in the second nuclear age*. Lexington, KY: The University Press of Kentucky.

Pincus, W. (2008, July 21). *Cybersecurity will take a big bite of the budget*. Retrieved November 8, 2008, from http://www.washingtonpost.com/wp-dyn/content/article/2008/07/20/AR2008072001641.html

Quester, G. H. (1966). *Deterrence before Hiroshima*. New York, NY: John Wiley & Sons, Inc.

Rattray, G. J. (2001). *Strategic warfare in cyberspace*. Cambridge, MA: The Massachusetts Institute of Technology Press.

Riptech, Inc. (2001). *Understanding SCADA system vulnerabilities*. Retrieved July 14, 2008, from http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf

Rumsfeld, D. H (2002). *Nuclear Posture Review Report (Foreward only)*. Retrieved August 20, 2008, from http://www.defenselink.mil/news/Jan2002/d20020109npr.pdf

Russell, J. A. & Wirtz, J. J. (2002, August). “Nuclear Weapons, War with Iraq, and U.S. Security Strategy in the Middle East.” In *Strategic Insights*, Vol. I, Issue 6. Retrieved August 19, 2008, from http://www.ccc.nps.navy.mil/si/aug02/middleEast.asp

Rutkowski, A. M. (2008, May 31). *Basic Information on the ITU-T IP-Traceback and International Caller-ID capability Initiatives*. Retrieved November 20, 2008, from http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/Rutkowski_IPtraceback_callerID_rev0.pdf

Sagan, S. D. (1991). History, Analogy, and Deterrence Theory. In *Journal of Interdisciplinary History*, Vol. 22, No. 1, pp. 79-88. Cambridge, MA: MIT Press.

Schelling, T. C. (1967). *Arms and Influence*. New Haven, CT: Yale University Press.

Schmitt, M. N. (2002, June). *Wired Warfare: Computer network attack and jus in bello*. Retrieved September 28, 2008, from http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/5C5D5C/$File/365_400_Schmitt.pdf

Shannon, E., & Thornburgh, N. (2005, August 25). *The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)*. Retrieved August 18, 2008 from http://www.time.com/time/magazine/article/0,9171,1098961-6,00.html

Shimeall, T., Williams, P., & Dunlevy, C. (2002). "Countering cyber war." In *NATO Review*. Winter 2001/2002. p. 16-18.

The Economist. (2007a, May 10). *A cyber-riot*. Retrieved April 14, 2008, from http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598

The Economist. (2007b, May 24). *Newly nasty*. Retrieved April 15, 2008, from http://www.economist.com/world/international/displaystory.cfm?story_id=9228757

Two-Factor Authentication. (2008). Retrieved November 5, 2008, from Wikipedia Web site: http://en.wikipedia.org/wiki/Two-factor_authentication

U.S. Department of Defense. (2006). *Quadrennial Defense Review Report*. Retrieved February 18, 2008, from http://www.defenselink.mil/qdr/report/Report20060203.pdf

U.S. Department of Defense. (2008, September 12). *DoD Special Briefing With Secretary Gates; James Schlesinger, Chairman, Task Force for Nuclear Weapons Management on The Task for Nuclear Weapons Management Report from the Pentagon Briefing Room, Arlington, VA*. Retrieved September 13, 2008, from http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=4284

U.S. Strategic Command (1995). *Essentials of Post Cold-War* Deterrence. Retrieved September 6, 2008, from http://nautilus.org/archives/nukestrat/USA/Advisory/essentials95.txt

Wattman, K., Wilkening, D. et al., (1995).*US Regional Deterrence Strategies*. Santa Monica, CA: RAND Corporation.

Weapon. (2008). Retrieved October 28, 2008, from Wikipedia Web site: http://en.wikipedia.org/wiki/Weapon

Wicked Problems. (2008). Retrieved November 13, 2008, from CogNexus Institute Web site: http://www.cognexus.org/id42.htm

Williamson, C. W. III. (2008, May). “Carpet bombing in cyberspace.” In *Armed Forces Journal*. May 2008, pp. 20-21.

Wilson, C. (2008, January 29). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* CRS Report for Congress. Retrieved August 28, 2008 from http://italy.usembassy.gov/pdf/other/RL32114.pdf

Zanini, M. & Edwards, S. J. A. (2001). “The Networking of Terror in the Information Age.” In *Networks and Netwars: The future of terror, crime, and militancy* (Arquilla & Rofeldt ed.) Santa Monica, CA: RAND Corporation.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California