Offensive Cyber Capability: Can it Reduce Cyberterrorism?

A Monograph
by
Major Stephen M. Marshall
U.S. Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2010

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	2010Dec02	SAMS Monograph, January 2010 – December 2010

4. TITLE AND SUBTITLE
Offensive Cyber Capability: Can it Reduce Cyberterrorism?

5. FUNDING NUMBERS

6. AUTHOR(S)
Major Stephen M. Marshall (United States Army)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
Gibbon Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

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

Command and General Staff College
731 McClellan Ave.
Fort Leavenworth, KS 66027-1350

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

The subject of cyberterrorism has become a topic of increasing importance to both the U.S. government and military. Offensive cyber capabilities provide a means to mitigate risk to U.S. systems that depend on the Internet to conduct business. In combination with passive security measures, offensive cyber capabilities seem to add to the level of Internet security thereby securing cyberspace for all Americans. The intent of this monograph is to identify the strengths and weaknesses of an offensive cyber capability in order to visualize the various options and tradeoffs necessary to achieve an acceptable level of security.

The findings of the monograph highlights an offensive cyber capability can reduce the threat of cyberterrorism. It is clear from the agent based model that the addition of this resource with passive defensive measures can lead to higher cyberterrorist kills and fewer nodal compromises. An offensive cyber capability grants the state the ability to take direct action against a perceived threat however, the risk is high for attacking an innocent bystander. In order for the U.S. to achieve an acceptable level of security, it cannot be too reliant on offensive cyber capabilities.

14. SUBJECT TERMS
Cyberterrorism

15. NUMBER OF PAGES
60

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
(U)	(U)	(U)	(U)

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Stephen M. Marshall

Title of Monograph: Offensive Cyber Capability: Can it Reduce Cyberterrorism?

Approved by:

_____ Monograph Director
Alexander J. Ryan, Ph.D.

_____ Second Reader
John J. Marr, COL, IN

_____ Director,
Wayne W. Grigsby, Jr., COL, IN School of Advanced Military Studies

_____ Director,
Robert F. Baumann, Ph.D. Graduate Degree Programs

Abstract

OFFENSIVE CYBER CAPABILITY: CAN IT REDUCE CYBERTERRORISM? by MAJ Stephen M. Marshall, U.S. Army 60 pages.

The subject of cyberterrorism has become a topic of increasing importance to both the U.S. government and military. Offensive cyber capabilities provide a means to mitigate risk to U.S. systems that depend on the Internet to conduct business. In combination with passive security measures, offensive cybercapabilities seem to add to the level of Internet security thereby securing cyberspace for all Americans. The intent of this monograph is to identify the strengths and weaknesses of an offensive cyber capability in order to visualize the various options and tradeoffs necessary to achieve an acceptable level of security.

The idea of convergence continues to bring together separate technologies using the Internet in order to interact and become more efficient. The effect of this phenomenon has increased the speed with which information is shared, helped business become more competitive and provided different means to distribute information. This same convergence has made the Internet a prime target as it has the potential to affect the economy, critical infrastructure and limit the freedoms of others in the cyberspace arena. Due to the increasing complexity of technology, vulnerabilities will continue to surface that can be taken advantage of. Technology is also becoming cheaper and easier to operate granting any motivated individual with access to the Internet the ability identify network vulnerabilities and exploit them. These themes are important as they identify that the U.S. is highly dependent on the Internet making it imperative that feasible security options must be identified in order to secure cyberspace.

A cyberterrorist act has not occurred therefore there is no empirical evidence to develop case studies upon and generate learning. An agent based model using basic parameters learned from the literature review and logical deductions reveals key several key relationships. First, there is a balance between an offensive cyber capability and passive defensive measures that must be achieved in order to attain an acceptable level of network security. Increased passive defensive measures can reduce vulnerabilities, thereby mitigating the threat of cyberterrorist attack. However, public and industrial interests will continue to challenge the strength of the passive defensive measures, creating network vulnerabilities that can be taken advantage of. Second, an offensive cyber capability can reduce the threat of cyberterrorism. It is clear from the agent based model that the addition of this resource with passive defensive measures can lead to higher cyberterrorist kills and fewer nodal compromises. It grants the state the ability to take direct action against a perceived threat however the risk is high for attacking an innocent bystander. However, for the U.S. to achieve an acceptable level of security, it cannot be too reliant on offensive cyber capabilities.

Table of Contents

Introduction

The traditional military domains of air, land and sea have recently expanded to include cyberspace. The technological advances in computer hardware, software and the expansion of the Internet have spawned intense debate on the threat of cyberterrorism. The term has many different definitions. This is a source of confusion, fear and misunderstanding, which influences public opinion in various ways. Some argue that cyberterrorism is a legitimate threat, whereas others discount the concept as there has yet to be a documented account of an attack. Whatever one's stance, cyberterrorism has been the subject of increasing public and academic attention. This combination of confusion and increasing attention contributes to the importance of developing a clear understanding of cyberterrorism.

The subject of cyberterrorism is important for many reasons. First, it is clear that everyone who has access to the Internet is potentially vulnerable. An act of cyberterrorism has the potential to affect any one of us due to the freedom offered by the cyber domain. Physical limitations such as terrain features, borders or laws do not restrict the flow of electrons from one terminal to another, creating a vulnerability that can be exploited. Second is the increased focus and study on cyber issues. In the past decade alone, the volume of scholarly works, policy and military doctrine has steadily increased to address the issues that rapid technological change has brought about. The third trend is that of self-protection. Cyberspace is largely a commercial enterprise that governments have little control over. Governments do not have the ability to secure cyberspace without taking away freedom on the Internet. Individuals and corporations alike must take measures to secure their networks in order to safeguard against attacks. The last trend is that of cooperation. Information sharing between the government and industry is necessary to learn from the different methods of cyberattack and how best to deal with the threat. Could this lead to corporations taking on security or enforcement roles that we would normally grant the government to conduct?

This paper will explore if an offensive cyber capability will reduce the threat of cyberterrorism. Military professionals and policy makers are the intended audience for this monograph, however it is not limited to that demographic. Currently, U.S. Strategic Command (STRATCOM) has initiated a U.S. Cyber Command (CYBERCOM) headquarters to address the battle domain of cyberspace and information on this topic will contribute to a greater awareness of the options and the risks associated with it. The concept of a military offensive cybercapability has been put forward in addition to current network security measures in order to secure cyberspace. This monograph will synthesize different perspectives into a brief document that can be used as a planning consideration for those planners concerned with the cyberterrorist threat.

There is no academically accepted and published example of a cyberterrorist act. In order to understand cyberterrorism a thorough literary review focusing on the body of academic work, U.S. policy and current discourse will substitute for lack of historical data. The major themes and synthesis gained from the research will serve to build a scenario for constructing a NetLogo agent based model of cyberterrorism. The data gained from the purposeful driven actors within the model will be used to determine whether or not an offensive cyber capability is a viable option in the fight against cyberterrorism.

Currently, there is no recorded account of an act of cyberterrorism, therefore it is essential to go beyond the literature review by modeling the threat. Primary sources such as national policy and civilian/military reactions to cyber defense, scholarly journals and books, and various articles will serve as a foundation to outline common themes and issues that are associated with cyberterrorism. Other sources will outline various theories and multiple perspectives on the use of cyberterrorism as a means to an end. Central to answering the question of the utility of an offensive cyber capability will be the use of the NetLogo model to simulate the possibility of attack and the effect of an offensive cyber capability against cyberterrorism. This model will highlight the strengths and weaknesses of an offensive cyber capability in order to

visualize the various options and the tradeoffs necessary to achieve an acceptable level of security.

This monograph will demonstrate that an offensive cyber capability can reduce the threat of cyberterrorism. However, the risk for collateral damage increases with a higher dependence on an offensive cyber capability. In order to achieve an acceptable level of Internet security there must be a balance between an offensive cyber capability and passive defensive measures.

Historical Context of the Cyberterrorist Threat

The Internet began as a Department of Defense research project named ARPANET (Advanced Research Projects Agency Network). The primary reason for the creation of ARPANET was to develop a means of reliable communication in the case of nuclear war. In the early 1980s, the Transmission Control Protocol/Internet Protocol (TCP/IP) was adopted as the primary transmission means as it did not depend on a direct connection between hosts like the traditional phone system.[1] "IP first chops up the message into packets from the sending host in preparation to send the packets to the receiving host computer. Then, TCP delivers those packets to the desired computer host at the destination. TCP further ensures that the received packets are reorganized in proper order."[2] This transmission protocol is standard for any machine seeking access to the Internet, yet it has a major flaw. Vulnerabilities such as "TCP session hijacking, IP spoofing and synchronization (SYN) flooding are just three examples of simple yet effective attacks against TCP/IP based networking."[3] The TCP/IP protocol was built to ensure reliable transmission of information, not the security of it. From the very beginning of the Internet, vulnerabilities in the system were apparent.

---

[1] James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2003), 55.

[2] Bruce D. Caulkins, *Proactive Self-Defense in Cyberspace* (Virginia: The Institute of Land Warfare, 2009), 2.

[3] Ibid., 2.

The Internet experienced rapid growth and has been a primary driver for interconnectedness, thereby contributing to globalization. Individuals and groups of people now have a voice. Businesses can reach their customer directly and tasks that would previously require travel can be done with a click of a mouse. The National Intelligence Council stresses the increasing importance the information flow provided by the Internet, contributing to globalization.

> **We see globalization**—growing interconnectedness reflected in the expanded flows of information, technology, capital, goods, services, and people throughout the world—**as an overarching "mega-trend," a force so ubiquitous that it will substantially shape all the other major trends in the world of 2020**.[4]

Global corporations and multi-ethnic groups use the Internet to integrate with the world, challenging traditional notions of the nation-state. The U.S. dependence on information and technology, both major components within the cyberspace arena, are challenging the "significance of boundaries, sovereignty, power, representation, and interdependence."[5]

The interconnectedness that the Internet provides has many positive attributes for individuals and groups, however it will cause governments to reassess security. The 2010 NSS states:

> In the two decades since the end of the Cold War, the free flow of information, people, goods and services has accelerated at an unprecedented rate. This interconnection has empowered individuals for good and ill, and challenged state based international institutions that were largely designed in the wake of World War II by policymakers who had different challenges in mind. Nonstate actors can have a dramatic influence on the world around them.[6]

---

[4] National Intelligence Council, "Mapping the Global Future: Report of the National Intelligence Council's 2020 Project, 2004," http://www.foia.cia.gov/2020/2020.pdf (accessed July 03, 2010), 10.

[5] David Newman, *Boundaries, Territory and Postmodernity* (New York: Frank Cass, 1999), 11.

[6] U.S. President, "National Security Strategy of the United States, 2010," http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed July 03, 2010), 7.

The Internet will continue to provide unimpeded transfer of ideas and their proliferation. These ideas may contradict the policies of the state, further hindering the ability of the state to govern. The use of the Internet can also operate outside the control of the state further complicating governance.

Maintaining the security of cyberspace has become important to the defense of our nation. As identified by The National Strategy to Secure Cyberspace, "Our economy and national security are fully dependent upon information technology and the information infrastructure."[7] All aspects of the U.S. public and private institutions (energy, transportation, finance, banking etc.) are intertwined and highly reliant on cyberspace. President George W. Bush stated that, "Cyberspace is their nervous system—the control system of our country."[8] Disruptions to cyberspace through global market change or those with hostile intentions can expose market vulnerabilities that can generate huge financial losses. Our military is also highly dependent on information systems to command and control the battlefield and shares the vulnerabilities that other public and private institutions have. Tools such as Command Post of the Future, Joint Network Node and network communications are highly dependent on the Internet to provide the backbone for command and control, further establishing the U.S. need for maintaining security of the Internet.

The term cyber has increasingly become more important in the political and military sphere. The 2006 version of the National Security Strategy (NSS) only uses the term cyber once, whereas the 2010 version has 26 references and features a chapter on securing cyberspace.

> The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient. Our digital infrastructure, therefore, is a strategic

---

[7] U.S. President, "The National Strategy to Secure Cyberspace, 2003," http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed July 03, 2010), viii.

[8] Ibid., vii.

> national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority.[9]

The NSS is clear that we face threats from both state and non-state actors that may use technology to disrupt and destroy. In order to prevent cyber intrusions or attacks the NSS pledges to strengthen partnership with international governments to develop common cyberspace conduct and establish cybercrime laws. The government will also invest in people and technology in order to improve innovation and cyber security awareness to address vulnerabilities.

Information technologies and cyberspace have changed how the U.S. and other countries view warfare. "The advent of information technologies expands physical battlespace and the area of military operations far beyond traditional boundaries to include economic, financial, psychological, and political sectors."[10] Mastery of the traditional battlespaces of land, sea and air alone can no longer provide adequate defenses as cyberspace bypasses geography. In post-industrial societies, two global trends add to the vulnerabilities that cyberterrorists can exploit. The first is network convergence—the merging of voice and data such that all communications are transported over one common network structure. The second is channel consolidation—the concentration of data collected on individual users by the service providers.[11] The U.S. is highly reliant on information technologies and cyberspace to conduct everything from business to the national defense. This dependence on cyberspace can be leveraged by state or nonstate actors in order to counter the U.S. dominance of land, sea and air warfare. "The post-industrial society is

---

[9] U.S. President, "The National Security Strategy of the United States, 2010," http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed July 03, 2010), 27.

[10] Robert L. Pfaltzgraff and Richard H. Shultz, *War in the Information Age: New Challenges for U.S. Security Policy* (Washington: Brassey's, 1997), 9-10.

[11] U.S. Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence, 2010," http://www.dni.gov/testimonies/20100202_testimony.pdf (accessed July 04, 2010), 3.

likely to be the object of relatively inexpensive information warfare attacks waged against its sophisticated military and civilian infrastructure by less developed societies and groups."[12]

Literature Review

An offensive cyber capability seems like an intuitive addition to the defense of the Internet and our nation. However, it is important to understand the current debate and literature on cyberterrorism to understand the positive and negative benefits of the offensive cyber capability. Understanding of the literature review will provide the reader an overview as to why there is no definitive definition of cyberterrorism, grant a greater appreciation of the vulnerabilities of the Internet and understanding as to why the U.S. government cannot be the sole answer for the defense of cyberspace.

Seven major themes emerged throughout study of the literature on cyberterrorism: defining cyberterrorism, establishing the threat, vulnerabilities, policy, tensions between cyber freedom and security, taking action, and deterrence. The first theme centers on definition of the cyberterrorism threat. No consensus on a definition for cyberterrorism exists, so most authors develop their own definition. The establishment of the threat and vulnerabilities of cyberspace generate intense scholarly debate. The constant struggle between theory and policy became readily apparent through the many studies of the threat of cyberterrorism and their recommendations for policy makers. Directly related to this concept are the tensions and tradeoffs that the policy maker must confront in order to satisfy and protect the populace. Some policy recommendations have the potential to limit freedoms or the competitive edge of business, leading to compromise or encouraging inaction. Many authors focus their work on educating the policy makers and the public on the actions that are necessary to protect against an act of cyberterrorism. The last theme focuses on the feasibility of deterrence. Note that while sources

[12] Robert L. Pfaltzgraff and Richard H. Shultz, *War in the Information Age: New Challenges for U.S. Security Policy* (Washington: Brassey's, 1997), 13.

have been categorized by these themes, each author contributes to multiple themes. The authors all agree that vulnerabilities in cyberspace exist and must be acknowledged. Debate centers on whether a cyberterrorist attack is feasible and what should be done to secure the network. Further analysis of the national implications of cyberterrorism will be explored to highlight how states view cyberterrorism.

Defining Cyberterrorism

In order to understand cyberterrorism, we must first look at the root terms of cyber. The term cyber

> is derived from "cybernetics", which began being used early in the twentieth century to describe relationships between people and machines. "Cyber" is the Greek word for "pilot." When computers came along in the late 1940s, cybernetics was a word in vogue, and "cyber" began finding its way into the language as a prefix for anything involving computers.[13]

The term cyber has been combined with the term space to identify interactions between online computer networks and the end nodes (devices). Cyberspace is defined by the National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[14] DOD defines cyberspace as "*A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and*

---

[13] Dunnigan, James F., *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2003). 20.

[14] U.S. President, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009," http://www.wired.com/images_blogs/threatlevel/2009/05/cyberspace_policy_review_final.pdf (accessed July 04, 2010), 1.

associated physical infrastructures."[15] This definition is applicable to the traditional client-server, peer-to-peer[16], grid computing[17] and cloud computing[18] models as the computers share information through the interconnected network of computer systems enabled by the electromagnetic spectrum and hardwired connections.

The term terrorism, as well as cyberterrorism, are contested concepts as they continue to garner debate on their use and meaning. Walter Bryce Gallie, a British social scientist that forwarded the argument that key concepts such as democracy cannot be irrefutably defined. According to his framework, contested concepts will have different accreditation of value achievement by different people. What may be terrorism or cyberterrorism to one person would not qualify for another. Each term is internally complex and diversely describable causing constant debate and analysis of its inner workings or observation. The meanings are still open to interpretation and reciprocal recognition of the terms has not yet been achieved.[19] The current FM 1-02 and JP 1-02 do not define cyberterrorism though a definition had been provided by the Army in the *Cyber Operations and Cyber Terrorism Handbook* published in 2005. There is no universally accepted exemplar that would model the behavior of the terms and the progressive competition of quality arguments between debating parties continues. Because of this, we will not

---

[15] U.S. Defense Department, "The National Military Strategy for Cyberspace Operations (U), 2006," http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed July 04, 2010), ix.

[16] A decentralized file sharing system like BitTorrent,Gnutella or Kazaa where computers that download data also store that data and serve it to other downloaders, "FOLDOC: Free On-line Dictionary of Computing," http://foldoc.org/peer+to+peer (accessed November 18, 2010).

[17] Grid computing (or the use of a *computational grid)* is the applying the resources of many computers in a network to a single problem at the same time, "SearchDataCenter," http://searchdatacenter.techtarget.com/definition/grid-computing (accessed November 18, 2010).

[18] A loosely defined term for any system providing access via the Internet to processing power, storage, software or other computing services, often via a web browser, "FOLDOC: Free On-line Dictionary of Computing," http://foldoc.org/cloud+computing (accessed November 18, 2010).

[19] David Collier, Fernando Daniel Hidalgeo and Andra Olivia Maciuceanu, "Essentially contested concepts: Debates and applications," http://polisci.berkeley.edu/people/faculty/CollierD/Collier%20Gallie.pdf (accessed August 26, 2010).

seek a definitive definition of terrorism or cyberterrorism. Rather, we intend to survey various definitions in the literature and provide a working definition for this monograph.

Trinquier defined modern warfare (terrorism) in his experiences in the first Indochina War and the Algeria war. He described it as an "interlocking system of actions—political, economic, psychological, military—*that aims at the overthrow of the established authority in a country and its replacement by another regime*" without the need for a battle between opposing armies. [20] What makes terrorism so difficult to define is that the ideology, political affiliation and endstate changes between various terrorist entities. Further, what one man would view as a freedom fighter, another may view as a terrorist, serving to add to the difficulty of defining the term.

The commonality between the different definitions of terrorism is the incorporation of violence, targeting of noncombatants, and the use of fear to further their cause. Daniel Cox et al., an assistant professor of Political Science at Missouri Western State College, define terrorism as:

> Any premeditated violent act perpetrated against civilian noncombatants by subnational or international groups, clandestine agents, or individuals sympathetic to larger terrorist groups and movements, with the intent to influence a target audience larger than the intended victims toward or against a particular policy action.[21]

Robertson, a researcher focused on global security, provides another definition primarily focused on policy. "Terrorism is a political strategy whereby groups or individuals use violence against civilian or symbolic targets to persuade a government to change a specific policy."[22] The JP 1-02 defines terrorism as, "The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are

---

[20] Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (Fort Leavenworth: Combat Studies Institute, 1985), 6.

[21] Daniel G. Cox, John Falconer and Brian Stackhouse, *Terrorism, Instability, and Democracy in Asia and Africa* (Boston: Northeastern University Press, 2009), 21.

[22] Ann E. Robertson, *Terrorism and Global Security* (New York: Infobase Publishing, 2007), 5.

generally political, religious or ideological."[23] Common terrorist tactics used to achieve their objectives are intimidation, coercion, bombing, hijacking, kidnapping and narcoterrorism. The majority of these tactics are bloody, spectacular attacks primarily waged against the populace.

The term cyberterrorism, just like the word terrorism, has different variations of definition and meanings based upon the source used. The word was created by combining cyberspace and terrorism and became widely accepted by various organizations, though no documented account of cyberterrorism exists. The Federal Bureau of Investigation (FBI) defines it as,

> A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.[24]

The FBI, in calling cyberterrorism a criminal act, infers that the act is a law enforcement issue. The U.S. Army fully endorses the definition in the 2005 version of the "Cyber Operation and Cyber Terrorism Handbook", however the assertion that cyberterrorism is a criminal act may cause the Department of Defense (DOD) to redefine cyberterrorism. Currently, DOD and U.S. Government do not have a definition of cyberterrorism that would recognize the act as more than a crime.[25]

There are alternative definitions that elevate the act of cyberterrorism above a law enforcement issue. Lawrence Brown defines cyberterrorism as, "the use of computers as weapons, or as targets by politically motivated international, or sub-national groups, or

---

[23] U.S. Defense Department, "Joint Publication 1-02: The Department of Defense Dictionary of Military and Associated Terms, 2010," http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed July 04, 2010), 472.

[24] U.S. Army Training and Doctrine Command, *DCSINT Handbook No. 1.02. Cyber Operations and Cyber Terrorism* (Ft Leavenworth KS: Government Printing Office, 2005), Glossary 1.

[25] Dykman, Peter. "Terrorism and Cyberspace" (Research paper, Kansas State University, 2009), 11.

clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies."[26] Dorothy Denning, a published information security researcher, testified before the House Armed Services Committee defining cyberterrorism as,

> generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[27]

In both Brown's and Denning's definition, cyberterrorism is not relegated to just a criminal act and action above criminal prosecution may be required in order to protect the civilian populace.

Brown provides several distinctions useful for understanding cyberterrorism.[28] He identifies three types of computer attack: physical attack, electronic attack and computer network attack. Physical attack is a conventional weapons attack on the computer or the network, electronic attack is an electromagnetic interference that overloads circuits of the targeted computer, and computer network attack is a malicious code or an exploited vulnerability, which is usually seen as the primary means for a cyberterrorist attack. In his definition of cyberterrorism quoted above, Brown integrates the three forms of cyberattack with two views that separate cyberattack from cyberterrorism. The first view is effects-based, which focuses on the disruptive effects that generate fear. The second view is intent-based, which focuses on the computer attacks

---

[26] Lawrence V. Brown, *Cyberterrorism and Computer Attacks* (New York: Novinka Books, 2006), 7.

[27] Denning, Dorothy E., "Special Oversight Panel on Terrorism Hearing on Terrorist Threats to the United States: Statement of Dorothy E. Denning, 2000," http://armedservices.house.gov/comdocs/testimony/106thcongress/00-05-23denning.htm (accessed July 04, 2010), 1.

[28] Lawrence V. Brown, *Cyberterrorism and Computer Attacks* (New York: Novinka Books, 2006).

used to cause economic damage or to influence a government to do the will of the attacker.[29] Brown takes great care in ensuring that all methods of attack are addressed as well as including the effects-based and intent-based view in his definition of cyberterrorism. Brown also identifies that Congress may wish to explore the possible effects on the economy and the military after a coordinated attack, as well as the international reaction following a U.S. military response to a cyberattack. The book is written for anyone with interest in the subject very similar to the self-help works of Dunnigan.[30] However, the references to Congressional considerations seem to suggest the authors would like to influence policy. The work is still relevant today and provides a comprehensive overview on the issues that comprise cyberterrorism.

Gabriel Weimann, a full professor of Communications with Haifa University in Israel, book explores the ways in which modern terrorist organizations use the Internet.[31] Wiemann's definition of cyberterrorism, "the use of computer networks to sabotage critical national infrastructures (such as energy, transportation, or government operations)" does not address business or the military.[32] At the same time, it is overly broad, as it does not require the terrorist to have any political, social, or ideological motivation. However, there are those that argue that an act of cyberterrorism must be as destructive as a traditional acts of terror, hence the author's focus on the infrastructure. He claims that terrorists are becoming more exposed to the digital world in where cyberterrorism may become an attractive option.

In 2008 a large compilation titled *Cyber Warfare and Cyber Terrorism* was published to share information on the multiple ways that technology can be used to affect a state, a community

---

[29] Lawrence V. Brown, *Cyberterrorism and Computer Attacks* (New York: Novinka Books, 2006), 62.

[30] James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2003).

[31] Gabriel Weimann, *Terror on the Internet: The New Arena, The New Challenges* (Washington, DC: United States Institute of Peace Press, 2006).

[32] Ibid., 148.

or the individual and lessons learned from technological advancements.[33] The primary audiences for the work are the information technology and information security specialists that will use the information to detect, prevent and respond to cyber threats. However, the information is applicable to various government agencies and others that have interest in the subject as well. The book argues that technological advances and the Internet have become increasingly efficient as an information resource. This efficiency has led to an increasing dependence and centralization of technologies into cyberspace. This act of convergence will continue to reveal vulnerabilities that can be exploited by terrorists.

The book defines cyberterrorism as the "*premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets."*[34] The editors claim, "the predominant wish of a terrorist of any type is to create fear and harm among the widest possible spectrum of society."[35] Traditional forms of terrorism are effective in expressing dissatisfaction, yet the work argues that terrorists are growing increasingly dependent on the cyberspace realm to plan and initiate attacks, indicating that cyberterrorism is becoming more of a possibility.

The Center for Technology and National Security Policy published a book in 2009 that introduces a theory of cyberpower and explores all aspects of cyber concluding with recommendations to policy.[36] *Cyberpower and National Security* represents the first study of the theory of cyberpower with the primary focus of examining how cyberspace can be leveraged to

---

[33] Lech J. Janczewski, and Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism* (New York: Information Science Reference, 2008).

[34] Ibid., xiii.

[35] Ibid., xxvii.

[36] Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington DC: Potomac Books, Inc, 2009).

provide the U.S. an advantage in the pursuit of national and security interests. They define cyberterrorism as:

> a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. . . . *Attacks that disrupt nonessential services or that are a costly nuisance would not* [*be cyber terrorism*].[37]

This definition is similar to Dennings with the addition of extended power outages as a means to create fear and the addition of religious or ideological instead of social under terrorist motivation. The book is an extensive work similar to *Cyber Warfare and Cyber Terrorism* in the methodology of exploring the issues and threats however the work is geared more towards the creation of a framework to understand and utilize cyberpower more than that of a means to share lessons learned and information. The term cyberpower is defined as, "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."[38]

In all of the above-mentioned definitions, violence against non-military targets is used to establish the criteria for a terrorist attack. Other forms of violent terrorist activity (car bombs, suicide bombers, etc.) when successful, can cause mass destruction and cause a scene that will instill fear in the civilian populace. The idea of generating the same amount of fear through the click of a mouse can seem far-fetched. Some argue that cyberterrorism does not exist, due to the fact that any disruption of air traffic control systems, emergency communications networks or power grids will cause a nuisance rather than mass panic.[39] Adding to the case against

---

[37] Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington DC: Potomac Books, Inc, 2009), 438.

[38] Ibid., 48.

[39] Ann E. Robertson, *Terrorism and Global Security* (New York: Infobase Publishing, 2007), 24.

cyberterrorism is the lack of documented evidence of any cases. Critics argue that critical computer system are not connected to the Internet, but are "air gapped[40]," lowering the possibility of cyberterrorist activity. Terrorism has always used unconventional and/or conventional means to target the populace in order to achieve their ends, however we must understand what violence truly means to address these critiques.

The term violence prompts one to focus on some type of extreme force or some type of intense activity in the physical dimension. Stathis Kalyvas defines violence as, "the deliberate infliction of harm on people."[41] To inflict harm, you do not have to resort to a spectacular form of attack. Computer attacks do have the capability to cause economic disruption or restrict access to valuable information, both of which are capable of causing fear that may intimidate a government or people to act in accordance with terrorist demands. In post industrial countries like the U.S., dependence on cyberspace has exposed vulnerabilities that can be leveraged, thereby contributing to the possibility of cyberterrorism. "Death and destruction are not usually the terrorists' ultimate goal; it is power and influence. Terrorists seek political and social change, and their objective is to influence populations in ways that support that change. To accomplish this, they engage not just in physical, but also informational operations, and the integration of these."[42] A terrorist act does not have to cause death to be considered violent.

All of the above-mentioned sources have effectively argued credible definitions based upon perspective and the years of debate on the subject. However, cyberterrorism is a contested

---

[40] In networks, air gap is a type of security where the network is secured by keeping it separate for other local networks and the Internet, "Webopedia," http://www.webopedia.com/TERM/A/air_gap.html (accessed November 18, 2010).

[41] Stathis N. Kalyvas, *The Logic of Violence in Civil War* (New York: Cambridge University Press, 2008), 19.

[42] James J. F. Forest ed., *Countering Terrorism and Insurgency in the 21st Century: International Perspectives V.2* (Connecticut: Praeger Security International, 2008), 378-379.

concept therefore the definition will continue to change based upon debate. For the purposes of this paper, we will use the definition from "Cyberpower and National Security" introduced above:

> a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. . . . *Attacks that disrupt nonessential services or that are a costly nuisance would not* [*be cyber terrorism*].[43]

The definition does not limit an act of cyberterrorism to a criminal offense or the spectacular attacks often associated with terrorism.

Establishing the Threat

Currently, there is no academically accepted example of a cyberterrorist act. However, there has been a vast body of work that logically identifies the reasons for an attack and the risk that is currently accepted. Dan Verton, a former CIA and Pentagon intelligence database operator/trainer and current investigative reporter with Computerworld, uses a scenario based on a real world exercise (Black Ice) in order to examine the capabilities of terrorist cells to conduct an act of cyberterrorism.[44] His primary argument is that terrorists have the potential to target information age technologies that control critical infrastructures in order to achieve their goals. The book examines the idea of convergence, as it references many different technologies, such as emergency systems, banking, and public utilities increasingly becoming reliant on the Internet for control. He also focuses on the idea of a cascade effect by stating that "networks are becoming more connected and dependent on each other, creating a situation where a failure in one network

---

[43] Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington DC: Potomac Books, Inc, 2009), 438.

[44] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill, 2003).

can cause cascading failures throughout many other networks."[45] Peter Dykman, a student from Kansas State University conducting research on terrorism and the Internet, does not believe that the threat of the cascade effect is high, as most critical systems have a human operator in the system.[46] This fail-safe can override automatic systems if necessary, thereby preventing the cascade effect. Reports of this phenomenon are rare and the reports that do exist fall under scholarly scrutiny due to misreporting or false statements. Verton states that cyberterrorism can exist and he proposes that real time intelligence sharing can mitigate acts of cyberterrorism. LeBaron also argues that terrorists will use cyberspace to conduct attacks because the terrorist is not in any immediate danger, the cost is low, it would be highly disruptive and high profile news, it is difficult to trace and many targets can be attacked at any time, and lastly an act of cyberterror has the potential to inflict more damage than most conventional weapons.[47]

The U.S. Army produced a Cyber Operations and Cyber Terrorism handbook in 2005 as a supplement to a Training and Doctrine Command (TRADOC) terrorism study.[48] This handbook recognizes that no terrorist groups have used cyberattack yet as a means to exploit weakness, however it acknowledges that terrorist groups may have the ability to do so in the future. The document outlines the objectives, potential targets, tools of a cyberattack, and the various actors that would conduct the act. The document points out that the military is heavily dependent on the global information grid, which is not controlled by the Department of Defense. U.S. military dependence extends across a variety of military operations, including troop and equipment movement, information gathering and dissemination, and technology support. The work

---

[45] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill, 2003), xxiii.

[46] Peter Dykman, "Terrorism and Cyberspace" (Research paper, Kansas State University, 2009), 17.

[47] Wayne D. LeBaron, *Five Deadly Arrows of Terrorism: A Manual of Information and Protection* (New York: Nova Science Publishers, Inc., 2007), 24.

[48] U.S. Army Training and Doctrine Command, *DCSINT Handbook No. 1.02. Cyber Operations and Cyber Terrorism* (Ft Leavenworth KS: Government Printing Office, 2005).

concludes by acknowledging that cyberspace based attacks will continue, terrorists will capitalize on known weakness in the system, and actors will continue to identify new vulnerabilities in the system to exploit. The document was intended primarily for military use, however it could be used by any governmental or civilian agency that needs information about terrorism techniques, tactics and procedures. The document did not address what would be the expected functions of the military in case of a cyberattack against U.S. civilian targets. The handbook does not elaborate on this subject, leading the reader to assume that the military is responsible for its own networks and nothing more.

Cyberterrorism is a plausible alternative to modern terrorism in that it has the potential of bypassing the conventional forces or physical barriers of states.

> Security is no longer defined by armed forces standing between the aggressor and the homeland. The weapons of information warfare can outflank and circumvent military establishments and compromise the common underpinnings of both U.S. military and civilian infrastructure, which is now one and the same.[49]

The Internet offers anonymity that allows the terrorist to operate in places that may not agree with their ideology or activities. It also offers easy access, little to no outside control, access to a huge audience, instantaneous information flow, interactivity, and low cost. Terrorists are already taking advantage of the multimedia environment by creating videos, songs, and presentations that are entertaining and memorable. Finally, terrorists are using the Internet to shape perceptions through the mass media.[50] Terrorists can also use the Internet to threaten the public, causing anxiety within the targeted audience. The threat does not have to be credible. The threat alone can create a conditioned reflex that will to succumb to demands of the terrorists.

---

[49] Frank J. Cilluffo, Bruce D. Berkowitz and Stephanie Lanz eds., *Cybercrime…Cyberterrorism…Cyberwarfare….:Averting An Electronic Waterloo* (Washington DC: The CSIS Press, 1998), xiii.

[50] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 29-30.

Currently, terrorists use the Internet to plan, raise funds, recruit members, spread propaganda, collect data for future actions and procure funding. However, terrorists are further leveraging cyberspace and technologies to forward their agendas. "Some government experts believe that terrorists are at the point where they may be able to use the Internet as a direct instrument to cause casualties, either alone or in conjunction with a physical attack."[51] The Internet is naturally supportive of decentralized groups as it gives them the ability to network and share information and the attacker is not in a place to be physically harmed. "Cyber-attacks offer terrorists the possibility of greater security and operational flexibility. Theoretically, they can launch a computer assault from almost anywhere in the world without exposing the attacker to physical harm."[52] Terrorist movements are learning organizations that will continue to leverage technology and the Internet to assist in their causes. Factors such as low cost, improvement of technology, convergence, terrorist learning, and existing vulnerabilities seem to point toward the possibility of a cyberterrorist attack. What is key to note is that there is no source that has made the statement that cyberterrorism is not a possibility.

Vulnerabilities

In order to focus attention on threat of cyberterrorism, it is necessary to identify the vulnerabilities and the risks that exist due to inaction. In 1998, the Center for Strategic and International Studies released a study addressing the threat of cyberterrorism.[53] Their primary intent was to inform and shape policy decisions in the cyber arena. The paper explores the idea of information warfare (IW) and identifies the four types of IW threats. Strategic IW, consisting of

---

[51] U.S. Army Training and Doctrine Command, *DCSINT Handbook No. 1.02. Cyber Operations and Cyber Terrorism.* (Ft Leavenworth KS: Government Printing Office, 2005), II-7.

[52] Anthony H. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport CT: Praeger Publishers, 2002), 28.

[53] CSIS Task Force Report, *Cybercrime…Cyberterrorism…Cyberwarfare…: Averting an Electronic Waterloo* (Washington D.C.: The CSIS Press, 1998).

extended terrorist campaigns and other types of targeted information technology campaigns, was listed as the most important threat due to the potential consequences. Strategic IW represents a clear alternative to the conventional power of the U.S., is low cost to employ, and targets the U.S. dependence on information technology. The paper made recommendations to prevent an act of cyberterrorism. Recommendations included development of national security policies focused on technology, increased focus on information dominance as a national security objective, protection of the digital infrastructure, development of cooperation between government and the private sector, and preparing the military for IW. Current policy has addressed the key recommendations of the paper, however there are some limitations to the report.

The primary weakness of the CSIS report is the lack of a working definition of cyberterrorism. The concepts and recommendations were logically thought out and presented however lack of a working definition can lead to confusion. The authors did not separate the term cyberterrorism from other acts such as cybercrime or hacking, serving to detract from the message of the paper. The paper graphically depicts a Defense Science Board (DSB) report that a "Major strategic disruption of the United States" is likely by 2005.[54] Those who discount cyberterrorism can easily make the argument that the incorrect prediction is proof that the threat is overstated. However, the authors were not trying to say that an attack would happen by 2005, but that a major disruption would not happen before 2005, as conditions would not warrant that type of attack. This work was important as it was one of the first studies that identified the vulnerabilities in cyberspace.

Homeland Security Directive 7 provided the policy to identify and protect Critical Infrastructure and Key Resources. Currently there are 18 identified, including Energy, Information Technology, Banking and Finance, Communications, Government Facilities,

---

[54] CSIS Task Force Report, *Cybercrime…Cyberterrorism…Cyberwarfare…: Averting an Electronic Waterloo* (Washington D.C.: The CSIS Press, 1998), 22.

Emergency Services and Nuclear Reactors Materials and Waste. DHS acknowledges that protection is important as a successful attack can disrupt functioning of commercial and public sectors, create a cascade effect debilitating more than just the targeted attack. Such an attack could produce catastrophic losses that can damage public morale and confidence.[55] Further complicating matters is that the majority of facilities are under private control, and are driven primarily by profits, not security. Also, the ongoing partnership between government and private sectors is limited by communication and bureaucratic struggles, further exposing vulnerabilities to cyberterrorists.

U.S. Policy on Cyberspace and Cyberterrorism

"The National Strategy to Secure Cyberspace" was published in 2003 and intended to address vulnerabilities to the cyber systems supporting U.S. critical infrastructures.[56] The strategic objectives of the document are to prevent cyber attack against U.S. critical infrastructure, reduce national vulnerability to cyber attacks and to minimize damage and recovery time from cyber attacks. In order to address the strategic objective the document identifies five critical priorities for cyberspace security and delineates responsibilities to all government agencies and group actors in order to manage the threat and reduce vulnerability in cyberspace. The document makes it clear that the federal government alone cannot secure cyberspace and appeals to "every American who can contribute to securing part of cyberspace" and private sector business to partner with the U.S. Government in order to mitigate malicious

[55] U.S. Department of Homeland Security, "Department of Homeland Security." http://www.dhs.gov/files/programs/gc_1189168948944.shtm (accessed July 05, 2010).

[56] U.S. President, "The National Strategy to Secure Cyberspace, 2003," http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed July 03, 2010).

cyberspace activity.[57] The document does not refer to the term cyberterrorism. However, it does highlight the threat by stating "Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy or national security."[58] This policy addresses concerns highlighted by the CSIS, Verton and Dunnigan and marks the U.S. government's first attempt to address the security concerns of cyberspace.

The National Security Strategy (NSS) 2006 update uses the term cyber for the first time since the inception of the document.[59] The NSS calls for transformation, as major institutions of American national security must change in order to meet the new challenges of the future. The NSS also directs change to the Department of Defense (DOD) to meet traditional, irregular, catastrophic, and disruptive challenges. Under disruptive challenges, the NSS directs DOD to adapt and build capabilities in order to mitigate challenges from state and non-state actors that employ cyber capabilities. This identifies DOD as a key player in cyber security, however various draft military doctrine places primary focus on the protection of military networks.

The National Defense Strategy (NDS) also addresses the cyber threat in the in the 'deter conflict' portion of its five key objectives. According to the NDS, deterrence is necessary for enhancing security. In the contemporary strategic environment, the challenge is one of deterring or dissuading a range of potential adversaries from taking a variety of actions against the U.S. and our allies and interests. These adversaries could be states or non-state actors; they could use nuclear, conventional, or unconventional weapons; and they could exploit terrorism, electronic,

---

[57] U.S. President, "The National Strategy to Secure Cyberspace, 2003," http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed July 03, 2010), xiii.

[58] Ibid., 6.

[59] U.S. President, "The National Security Strategy of the United States, 2006," http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/ (accessed July 03, 2010).

cyber and other forms of warfare."[60] The NDS also acknowledges that small groups or individuals can exploit vulnerabilities in cyberspace to cause economic damage and interrupt critical services, identifying the possibility of cyberterrorism.

The "Cyberspace Policy Review" (2009) was directed by President Obama in order to assess policies and structures dealing with cyber security in his first 60 days in office.[61] The document acknowledges that state and non-state actors are using the Internet as a means to target the U.S. potentially leading to technological and economical weakness. The review provides a working structure to address oversight, accountability and cooperation between various government department/agencies and acknowledges that the government cannot secure cyberspace by itself. The document recommends that the public awareness should be increased in the topics of digital safety, digital ethics and cyber security education. It is also recommended that private business require higher security standards for their networks and share detection methods with the Federal government and other businesses. The information gathered would be used to create a common operational picture, key to the enhancement of incident response capabilities and cyber security across all structures. What is problematic with the document is the idea of information sharing between private business and the government. First, business will continue to be hesitant to share information as it may hinder their competitive edge over other businesses and reduce the efficiencies that the Internet provides. Second, continual sharing of information with the government will be seen as an intrusion to the working of free commerce. Lastly, these recommendations depend on the willingness of businesses to cooperate.

---

[60] U.S. Defense Department, "National Defense Strategy, 2008," http://www.defense.gov/pubs/2008NationalDefenseStrategy.pdf (accessed July 03, 2010), 11.

[61] U.S. President, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009," http://www.wired.com/images_blogs/threatlevel/2009/05/cyberspace_policy_review_final.pdf (accessed July 04, 2010).

The nation has taken action through the Department of Defense (DOD) and Department of Homeland Security (DHS) to address cyberspace vulnerabilities. The Secretary of Defense directed the establishment of U.S. Cyber Command (USCYBERCOM) in June 2009 in order to gain unity of command and leverage expertise in the cyberspace realm.

> USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[62]

The focus of this command is to protect DOD systems and to conduct full spectrum operations in the cyberspace domain. In order to directly protect the American people, the DHS addresses the domain of cyberspace in its 'mitigate vulnerabilities' objective. "We can, however, mitigate the Nation's vulnerability to acts of terrorism, other man-made threats, and natural disasters by ensuring the structural and operational resilience of our critical infrastructure and key resources and by further protecting the American people through medical preparedness."[63] Both DOD and DHS are actively pursuing vulnerabilities in order to protect the American populace and retain freedom of use in the domain of cyberspace.

The NSS of 2010 acknowledges that cyber security threats have become one of our nation's most serious threats.[64] The document proposes to protect the digital infrastructure by investing in people and technology and strengthening partnerships between government and business. Both of these initiatives are a positive signal that cyberspace has become more of a

---

[62] U.S. Defense Department, U.S. Cyber Command Fact Sheet, 2010," http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf (accessed July 03, 2010), 1.

[63] U.S. Department of Homeland Security, "National Strategy For Homeland Security, 2007," http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed July 03, 2010), 27.

[64] U.S. President, "The National Security Strategy of the United States, 2010," http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed July 03, 2010).

focal point for the U.S. government. However, the strategy does not address the problematic nature of information sharing between the individual, business and the government. The self-help message of Dunnigan and LeBaron seems to be reflected in the policy. The U.S. Government acknowledges that it will not play the key role of defense, rather individuals and businesses will.

Tensions Between Cyber Freedom and Security

Martin Golumbic, a professor of computer science with Haifa University, work addresses the regulatory dilemma of freedom of information versus the protection of the public through intrusion.[65] The author does not focus on cyberterrorism, however the work is relevant because the balance between the need for security and safeguarding of civil liberties is central to the exploration of cyberterrorism. Unlike the LeBaron work, Golumbic does distinguish between a cybercrime and cyberterrorism by focusing on the aims of the perpetrator. The book defines cyberterrorism as the use of cyberspace to make a political statement through the means of harming the individual.[66] The author also claims that the state has declined in power due to the increased power of corporations, a claim that is commonly associated with globalization, and the idea that computer code can be used as a substitute for the law. The idea of the "invisible handshake" marks the abdication of power from the government to large corporations in order to perform certain government functions. Code can provide a level of protection, reducing reliance on the state to provide protection or enforcement of laws. The book provides recommendations to legislators, focusing on whether or not there is a need for increased regulation in cyberspace. tradeoffs are important, as policy makers have to weigh security versus freedom. Their choices have direct implications on security, the economy and the daily end user experience of cyberspace.

---

[65] Martin C. Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (Israel: Springer Science and Business Media, 2008).

[66] Ibid., 17.

Though civil liberties are important to the American citizen, the current security situation has caused a shift in priorities. "Americans are willing to trade a degree of civil liberty for other valued benefits, such as the prevention of terrorism."[67] A primary example of this is the passage of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism act of 2001" (PATRIOT). This act, signed into law in just over one month, passed through Congress in three days with only one vote of opposition. However the cost of empowering the government to conduct surveillance and recordings of our activities in cyberspace can infringe on the right to privacy and freedom of speech.[68] Knowing that the government has an extensive monitoring capability may even serve to limit what the individual has to say thereby further infringing on freedom of expression. The American Civil Liberties Union (ACLU) has voiced concern based upon the increased monitoring capability the PATRIOT act grants the government. They emphasize that the continual increase of surveillance technology and gradual decrease of legal restraints on privacy protection can have adverse affects on the rights to privacy and free speech.[69] Just because Americans are currently willing to sacrifice civil liberty for protection does not mean that preference will continue. As priorities shift and if freedom of the Internet becomes more of a priority to the American citizen, policy and regulation will have to change.

---

[67] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 224.

[68] Martin C. Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (Israel: Springer Science and Business Media, 2008), 37.

[69] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 218.

Taking Action

James Dunnigan, a respected military analysist, addresses the threat of cyberterrorism in his 2003 book.[70] The book is geared toward the general public or non-technical user of the Internet. His primary argument is that electronic networks and the information transmitted are being used as weapons and that the future of cyberwarfare is the direct attack on the individual user. Dunnigan acknowledges that the major players (large corporations and the government) have the talent and resources to mitigate threats that originate from the Internet and the information contained in the book will grant the common Internet user the knowledge necessary to protect themselves. What is important about this book is the fact that the primary audience is the common Internet user. Dunnigan uses attack scenarios, explanations and priorities of threats in order to define the threat and initiate action from the reader to safeguard themselves. He heavily recommends that the reader turns off scripting, deletes any file attachment that comes from an unknown source, and turn off the macro execution in order to gain greatest amount of protection out of the 11 total recommended actions. The historical study is very thorough and has the capability to generate understanding of the current cyberterrorism debate by the general populace. What would have increased the credibility of the work would have been a chapter exploring the counter argument to the existence of cyberterrorism.

The role of the Department of Homeland Security (DHS) in combating terrorism was explored in the book *Homeland Security* published in 2005.[71] The primary purpose of the work is to outline the nature of the threat of terrorism and what actions are being taken in order to respond to the threat. Carafano and Sauter explore the policies, strategies, principles, organizations and programs that our nation has developed to protect the homeland and how counterterrorism efforts

---

[70] James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2003).

[71] James J. Carafano and Mark A. Sauter, *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism* (New York: McGraw-Hill, 2005).

from the federal government all the way down to the private citizen are being integrated. The book is intended for professionals and citizens. They argue: "It is no longer an option, but a civic obligation, for Americans to understand the issues that confront our national and do their part to defend both security and civil liberties. Every American has a role to play in the war against terrorism."[72] The Internet is decentralized medium and regulation is inconsistent across recognized borders. The Internet is not easily controlled by authorities as the state does not have the resources to control all nodes of communications. Governments cannot keep up with the technological changes and new development is happening all the time.[73] These factors illuminate the fact that the government does not have the capability to protect the individuals accessing the Internet. In support of Dunnigan's theme, the authors agree that individuals must protect themselves. The authors also state that terrorists use cyberspace to conduct psychological warfare, generate publicity and spread propaganda, as an information gathering/sharing repository, and to plan and coordinate their operations. The majority of the chapter was more focused on defensive measures (cyber security) rather than a true explanation of the cyberterrorist threat. The term cyberterrorism is used twice in the Digital Battlefield chapter and at no time is the threat defined. However, this work can help the intended audience to become more proactive with cyber security, helping to reduce vulnerabilities.

Wayne LeBaron, an author of several survival books, published a book in 2008 on five versions of terrorism including cyberterrorism.[74] He highlights what can be done to protect oneself and ones' interests from the various acts of terrorism. The relevancy of this book is that it

---

[72] James J. Carafano and Mark A. Sauter, *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism* (New York: McGraw-Hill, 2005), xvi.

[73] Steven R. Corman and Jill S. Schiefelbein, "Communication and Media Strategy in the Jihadi War of Ideas, 2006," http://comops.org/publications/CSC_report_0601-jihad_comm_media.pdf (accessed August 26, 2010), 16.

[74] Wayne D. LeBaron, *Five Deadly Arrows of Terrorism: A Manual of Information and Protection* (New York: Nova Science Publishers, Inc., 2007).

places the act of cyberterrorism on the same level of importance with radiological dispersion devices, chemical, biological, and nuclear weapons. The author uses the FBI and U.S. National Infrastructure Protection Center (NIPC) definitions of cyberterrorism, yet fails to examine how the definitions differ and why. Most importantly the NIPC uses "criminal act" in its definition raising the issue of what level of jurisdiction an act of cyberterrorism resides within. LeBaron states that a cyber attack can cause an inability to obtain basic sustenance items, loss of utilities (i.e. water, gas, sewage, electricity) and loss of public services (i.e. banking, TV, radio). The author recommends that families have a designated rally point with enough cash and emergency supplies on hand to last about two weeks.

The authors make it clear that the government is not central to the defense of the cyberspace. The 2010 NSS outlines that the individual or the government cannot secure cyberspace alone and cooperation is necessary. The work lets the audience know that they are vulnerable and must take action to defend themselves, thereby contributing to the greater security effort.

Deterrence

Martin Libicki, a senior scientist with the RAND Coorporation, explored the idea of cyber deterrence in a monograph sponsored by the U.S. Air Force (2009).[75] He argues that "cyberspace is so different a medium, the concepts of deterrence and war may simply lack the logical foundations that they have in the nuclear and conventional realms."[76] It is also argued that there is no UN dictum or international treaty that specifies cyber attack as an act of war. This in turn limits the retaliatory options of the state. The work focuses on the threat of retaliation (an overwhelming offensive cyber capability) as the deterrence method versus traditional denial

[75] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica CA: RAND Coorporation, 2009).

[76] Ibid., 5.

defenses such as firewalls and increased security measures. Libicki distinguishes cyber deterrence from nuclear deterrence (unrestricted retaliation causing extreme destruction) and criminal deterrence (the prevention of members of society from committing crimes due to the fear of lawful punishment) and concludes that cyber deterrence is problematic.

Literature Review Conclusion

The U.S. does not enjoy military dominance in cyberspace like the traditional domains of land, sea and air. The cyberspace arena does not conform to recognized state borders and 85% of American cyber infrastructure is in private hands.[77] According to the 2010 NSS, "Our digital infrastructure is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority."[78] The major issue with this statement is that cyberspace is not owned by anyone, nor do state borders bound it. Private companies are primarily driven by profits and achieving a competitive edge against peer companies. Adopting new security measures above and beyond what is currently working may detract from profits and cede their competitive edge. Also, cyberterrorists can gain an advantage through the weakest link. "When one company incurs the costs of adding safeguards to the part of the infrastructure it operates and another company does not, the result is to displace the terrorist threat to where security controls are the weakest."[79] Not only does the company who invests in cyber security erode their profits, but they can still be compromised due to the interconnected nature of cyberspace. It is also important to note that the government is further hindered from establishing stringent security measures due to the demand for freedom of information. The U.S. public will not sacrifice the right to privacy unless their security is directly threatened.

---

[77] Stephen Flynn, *The Edge of Disaster* (New York: Random House Publishing, 2007), 139.

[78] U.S. President, "The National Security Strategy of the United States, 2010," http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed July 03, 2010), 27.

[79] Stephen Flynn, *The Edge of Disaster*, (New York: Random House Publishing, 2007), 138.

No software designer or end user wants vulnerabilities in his or her system, however it is the nature of technology. Vulnerabilities "occur because of a gap between theory and practice. In theory, a system should do only what its designers and operators want it to. In practice, it does exactly what its code (and settings) tells it to. The difference exists because systems are complex and growing more so."[80] The Internet is replacing other forms of communications. The merging of other communications technologies (i.e. cable, phone services) directly contributes to the growth of cyberspace. This growth also encourages the interconnection that makes security dependent on the weakest link. Other major issues that contribute to vulnerabilities are the lack of knowledge of the technology in use. For example, outdated operating systems missing important security patches or systems configured incorrectly due to ignorance of network security adds vulnerabilities that cyberterrorists can take advantage of.

Terrorists have used the Internet to plan, recruit and distribute propaganda in order to further their cause. The following three reasons make the Internet inviting for terrorists. "First the Internet is, by design, decentralized and is not subject to easy control by authorities. Second, laws have not yet caught up with the new media so there are many opportunities to operate outside regulation (as do offshore Internet gambling operations), and what regulations exist are inconsistent across countries. Third, the new media are (after all) new, so big government has not caught up to technology in many respects."[81] Terrorists groups as well as state actors are capable of learning new ways to "exploit and attack networks, computers, data storage, and other information systems."[82] As American businesses and government are leveraging cyberspace to

---

[80] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica CA: The RAND Coorporation, 2009), xiv.

[81] Corman, Steven R. and Jill S. Schiefelbein, "Communication and Media Strategy in the Jihadi War of Ideas, 2006," http://comops.org/publications/CSC_report_0601-jihad_comm_media.pdf (accessed July 08, 2010), 16.

[82] Anthony H. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport CT: Praeger Publishers, 2002), 12.

reduce expenditures and streamline operations, they are creating vulnerabilities for others to take advantage of. Terrorist and hostile states' knowledge of cyberspace is increasing and these skills have the propensity to be used more aggressively in the future.[83]

The seven major themes of the literature review have outlined four major ideas that are central to the debate on cyberterrorism. First, the term cyberterrorism is a contested concept and the definition will change based upon the entity defining it. In order for the U.S. government to allocate resources and effectively deal with the threat an agreed upon definition is necessary to focus action. Second, deterrence is problematic as a cyberterrorist is not as threatened by deterrent action as a traditional terrorist due to the anonymity that the Internet provides. Although the U.S. enjoys conventional military superiority that can be projected worldwide in support of policy, the deterrence effect is negated by the anonymity. A cyberterrorist has little to fear from U.S. reprisal and can exploit vulnerabilities in support of their interests. This idea will be further explored in National Implications of Cyberterrorism section below. Third, the government does not have the ability to fully protect the individual citizen from a cyber attack. Security of cyberspace is dependent on the cooperation between government, industry and the individual. Without this cooperation, everyone is at risk due to the interconnectedness of the Internet. The vulnerabilities inherent with computers combined with the inability to control the Internet means that all computer users are vulnerable to attack. Lastly, the demand for freedom of the Internet is always in conflict to some extent with security. This further limits the U.S. government's ability to secure the Internet.

Agent Based Model of Cyberterrorism

Cyberterrorism is not a simple problem that can be solved with an existing solution. There is an inherent complexity in cyberterrorism as there are many different actors that are

[83] Anthony H. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport CT: Praeger Publishers, 2002), 12.

constantly interacting based upon their understanding and interests. Because of this, we can view cyberterrorism as a problematical situation. The term is careful to avoid "the word 'problem' since this implies 'solution', which eliminates the problem forever."[84] A problematical situation consists of conflicting worldviews and purposeful action by the agents within the system. Every agent has a worldview that may change or stay constant based upon experiences and will act purposefully in order to satisfy their interests. In order to focus inquiry into a concept that has not occurred yet, it is important to model purposeful cyberterrorism activity relevant to this investigation. The model is not intended to be definitive, however it will highlight relationships and define questions that may serve useful in the planning against the threat of cyberterrorism.

In order to garner the initial data needed to construct the model we must first outline a scenario. "Scenarios are rigorous, logical, but imaginative stories about what the future might be like, designed to help people plan. Scenarios are not predictions. They are tools for preparation."[85] Outlier events such as unknown possibilities (i.e. the winner of the next presidential election) and improbable events (i.e. wildcard events that are minimally possible yet their effect would be highly influential) would also be identified. Lastly, indicators that would signal the possibility of the identified scenario must be recognized in order to properly commit resources to address the problematical situation. If done correctly, scenario planning will answer the questions, "What can conceivably happen? Or: 'What would happen if. . . ?'"[86] Answering these questions can identify risk allowing the planning participants to institute risk management measures increasing the success of the interaction with the problematical situation.

---

[84] Peter Checkland and John Poulter, *Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students* (England: John Wiley & Sons, Ltd, 2006), xv.

[85] Joel Garreau, *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies—and What It Means to Be Human* (New York: Broadway Books, 2005), 78.

[86] Mats Lindgren and Hans Bandhold, *Scenario Planning: The link between future and strategy* (England: Palgrave Macmillan, 2003), 22.

Cyberterrorism Scenario

In 2025, the U.S. has achieved strategic success in both the Iraq and Afghanistan campaigns. The U.S. military has minimal footprints in both countries and America is no longer on a war footing. In both theatres of war, surge tactics were instrumental in the restoration of the legitimate governments and conventional military operations have lessened the effects of terrorist activity. The risk of terrorist activity in the U.S. is seen as low. Most Americans would much rather preserve freedom of the Internet than ensure security due to their perception of the risk of a terrorist strike. Terrorist activity has not been eliminated; however military action by state actors in the traditional domains of land, sea and air has become more effective due to lessons garnered from the "Long War." In response, terrorist organizations have turned towards identifying untapped vulnerabilities in cyberspace.

The U.S. government, no longer at war, concentrates on the growth of the economy. American businesses are primarily focused on expansion using the Internet to connect with new customers. Convergence of different communications mediums – telephony, cable television, and computer networks – continues at an accelerating pace due to the added benefit of access to additional customers and the ability to streamline operations, thereby maximizing profits. Businesses prefer to keep security measures at minimal levels in order to allow access to a broad spectrum of customers and reduce the costs of Internet security. Cooperation between businesses and the U.S. government has been problematical. Businesses continue to distrust competitors and do not want to relinquish information to the government, fearing increased government oversight. Profit, not security, is the main driver guiding business decisions.

The Internet continues to grow as more actors have the means to connect and communicate. The price of technology continues to decrease while the processing power and transmission speed of hardware continues to increase. Software also follows the same trend with the addition of increasingly intuitive functioning. More and more traditional coding has been

replaced with simplified language or point and click functions, making advanced programming possible to the novice computer user. Hackers, cybercriminals and the like continue to supply a vast array of instructional pamphlets and shareware designed to enable others to engage in related activity. These same individuals continue to brag about their successes against military, government and business targets, generating interest from terrorists.

Terrorists have developed increased expertise in networks, hardware and software operations. The anonymity granted by Internet operations provides terrorist cells with the ability to mitigate the threat of conventional military action. The growth of the Internet has served as the impetus for terrorist cells to develop their own IT professionals (cyberterrorists). While it would have been quicker to outsource the capability, the ideological differences between computer criminals and terrorist were seen as too great to risk compromise. The cyberterrorist uses the readily available shareware tools, commercial off the shelf technology, and increased network skills to attack locate and exploit vulnerabilities in the network.

Explanation of the NetLogo Model

NetLogo is a programmable modeling software that can replicate purposeful behavior based upon understanding of the environment.

> NetLogo is particularly well suited for modeling complex systems developing over time. Modelers can give instructions to hundreds or thousands of "agents" all operating independently. This makes it possible to explore the connections between the micro-level behavior of individuals and the macro-level patterns that emerge from the interaction of many individuals.[87]

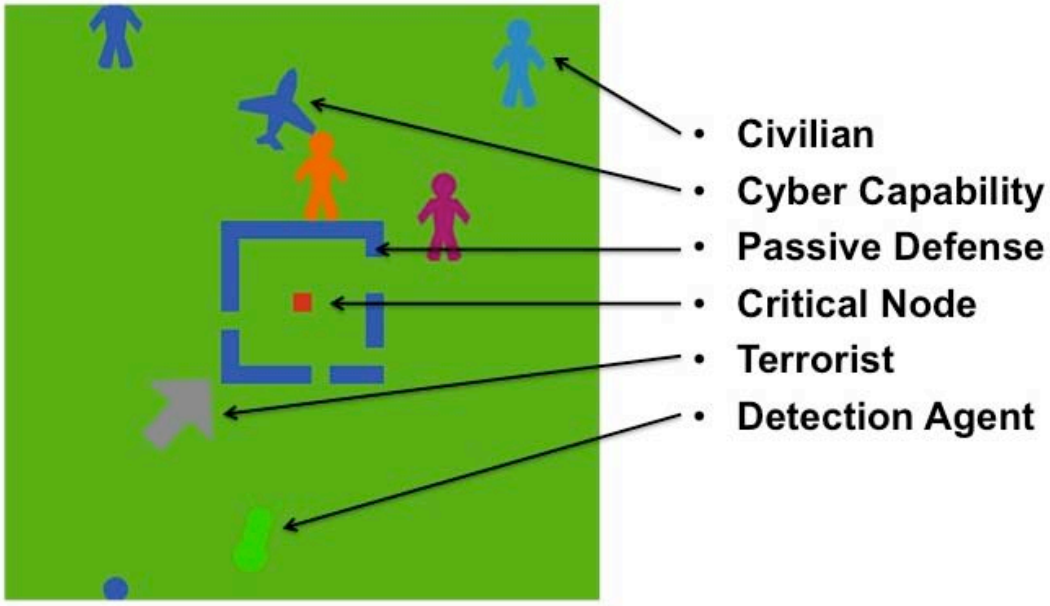
The absence of a legitimate cyberterrorism event adds to the usefulness of the NetLogo model. The lack of empirical evidence on cyberterrorism leads to a concept where there are numerous possibilities. The strength of modeling cyberterrorism is that this allows for unlimited parameters

[87] NetLogo 4.1.1 User Manual, http://ccl.northwestern.edu/netlogo/docs/ (accessed Sept 30, 2010).

to be added and explored. Upon further study of the concept or an actual cyberterrorist attack, the new data can be inputted into the model, generating further learning.

The model replicates the protection of a critical node through a passive defense and an offensive cyber capability. Agents within the environment an be affected by and can access the critical node, depicted as a red square in the center of the environment. Every agent within the defensive barrier (represented by a blue border around the critical node) has the ability to conduct an attack on the node. The terrorists are represented by multicolor arrows (except white) and civilians are depicted as multicolor people (except white). Detection agents are depicted as multicolor bugs with the mission of identifying terrorists. When the detection agents register a positive identification, they paint the identified arrow or misidentified person white, thereby flagging them as terrorists. The cybercapability depicted by multicolor airplanes seek out flagged terrorists and kills them. The screenshot from the NetLogo model (see Figure 1) illustrates how the program visually represents the agents in the system. The agents have been increased in size (from 1.5 to 5 in the original source code) and the number of agents modeled in the simulation has been decreased in order to more clearly show the different agents.

Figure 1. Screen capture of the NetLogo cyberterrorism model display.



Explanation of Parameter Settings

The literature review showed that no cyberterrorist attack has been publicly recorded, which motivates the requirement to simulate cyberterrorism. Assumptions guided by the material covered in the literature review were necessary in the absence of empirical evidence in order to provide the initial parameters to the model. Many of the parameters were set at arbitrary values due to a lack of data. As better data becomes available, the model introduced in this paper can be updated to refine this initial analysis. However, the purpose of this model is not to generate an accurate simulation of a specific cyberterrorist attack, but to develop a more abstract and general model to explore tradeoffs involved in countering cyberterrorist threats. The findings generated by these experiments have identified useful relationships that need further examination in order to develop a better understanding of the cyberterrorist threat and how effectively to deal with it.

In each experiment, there were 5 cyberterrorist actors among 100 civilian actors in all of the experiments. While this number seems high, the anonymity granted by the Internet and availability of malicious software can enable those with religious, ideological and political issues the ability to make a statement. The idea of convergence serves to increase the numbers of possible cyberterrorists.[88] The actual number of cyberterrorist actors and those who sympathies with their cause is unknown, however the initial setting does not overload the system with easy cyberterrorist targets, yet is high enough to be effectively targeted and generate statistically significant results.

The second setting is that a detection agent has a 10% chance of correct identification of a terrorist and a 0.2% chance of misidentifying a civilian as a cyberterrorist. The technological advances of the U.S., China, Russia and other nations dependent on the Internet have increased their capabilities to detect unlawful behavior. These states have highly trained personnel and

[88] Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington DC: Potomac Books, Inc, 2009), 161.

technologically advanced equipment that has the ability to effectively identify a cyberterrorist. However, the percentages also allow for misidentification and the friction involved with identification. The percentages chosen replicates the additional time necessary to overcome legal obstacles (domestic and international) and development of the case in order to prove that the person is truly a cyberterrorist.

The passive defense settings (50% Low, 80% Med and 95% High) were chosen based upon the current, optimal and unobtainable levels of passive security. Most businesses, government and home computers have virus protection, firewalls and intrusion detections devices built into the programming and do try to address vulnerabilities in their network. Most of these passive defensive measures run in the background transparent to the user protecting the network. However, advanced security settings serve to annoy the user or can limit access to a wider audience. The 50% passive defensive setting is closest to the current usage of passive defensive measures as it represents the lowest amount of protection necessary to secure the network. The 80% solution is intended to represent a closer working arrangement between business and the government. Lastly, the 95% setting was made to examine the effects of heavy passive security which is highly improbable.

Purposeful Action: Rules the Actors follow

All agents move around the model in random directions in pursuit of their objective. When the setup command is initiated, all the agents will randomly disperse throughout the system with the cyberterrorists spawning on the four outer edges of the model. Any agent that appears within the passive defense could be viewed as insiders, representing employees or operators of the node. The cyberterrorist goal is to breach the passive defense and physically hit the node. The passive defense will repel all actors within the system, however the level of protection will determine how many gaps are available that agents can pass through. This replicates the

vulnerabilities inherent to firewalls, network intrusion software and from relaxed security standards.

The detection agent actively searches for terrorists by interacting with all the agents in the system. When it encounters a cyberterrorist the detection agent has a 10% chance of correctly identifying the cyberterrorist and a 90% chance of misidentifying the cyberterrorist as a civilian. When it encounters a civilian the detection agent has a 99.8% chance of correctly identifying the civilian and a 0.2% chance of misidentifying the agent as a cyberterrorist. Agents identified by the detection agent as a cyberterrorist are painted white for 20 ticks, after which time the agents return to their original color. The low percentage of identification reflects the difficulty in positively identifying cyberterrorists and the time limit grants the cyberterrorist or civilian the ability to escape destruction. The small possibility of civilians being incorrectly identified as cyberterrorists introduces "false flagging," which models that fact that any cyberterrorist detection capability will not be perfect.

The cybercapability will kill any white agents (those flagged as cyberterrorists) that it encounters. The term "kill" means to remove the agent from cyberspace. This could represent a range of real world actions, from denial of service, loss of Internet access, incarceration, all the way up to assassination. Presumably, the less severe the physical effects of the offensive cyber capability are on the targeted agent, the more attractive the capability would be to governments, since the impact of incorrectly targeting civilians is reduced. If those agents removed from cyberspace could appeal the ban through a legal process, then bans due to mistaken identity could be reversed. However, this model is general enough to represent the full range offensive cyber options. The meaning of the number of civilian kills recorded in a model run may have a very different interpretation when the offensive capability is targeted assassination or a denial of service attack.

Findings

A total of nine experiments were conducted examining the relationships between different parameter settings. The number of cyberterrrorists, cybercapability, detection agents, civilians and passive defense could be adjusted from 0 to 100. The diameter of the passive defense could also be adjusted from 0 to 16. Throughout the experiments the four constant settings were the number of civilians (100), the number of cyberterrorists (5), the diameter of the passive defense (8) and the number of time ticks (1000). The number of offensive cybercapability and detection agents are jointly varied from 0 (None), to 10 (Medium), to 20 (High). The percentage of passive defense is varied from 50% (Low), to 80% (Medium), to 95% (High). The node violation mean represents the average number of times within the experiment-imposed 1000 time steps that the critical node was compromised. The top row of Table 1 depicts the level of passive defense for each experiment. The first column from top to bottom outlines the time steps, experiment number, the offensive cyber capability setting (none, medium, or high), the average number of times that the node was violated, and the average number of terrorists and civilians killed. The number in parenthesis is the standard deviation (the dispersion from the mean) for 20 replications of each experiment.

Table 1. Data Summary of the node violations, terrorist and civilian kills mean and standard deviation

TIME STEPS 1000	**50% Passive Defense**			**80% Passive Defense**			**95% Passive Defense**		
Experiment Number	**Ex 1**	**Ex 2**	**Ex 3**	**Ex 4**	**Ex 5**	**Ex 6**	**Ex 7**	**Ex 8**	**Ex9**
Cyber Capability Setting	**NONE (0)**	**MED (10)**	**HIGH (20)**	**NONE (0)**	**MED (10)**	**HIGH (20)**	**NONE (0)**	**MED (10)**	**HIGH (20)**
Node Violation ***Mean (STD DEV)***	3.85 (2.78)	3.20 (2.89)	3.85 (2.65)	5.20 (6.02)	3.20 (5.12)	2.15 (2.55)	1.45 (2.73)	2 (3.16)	1.35 (3.12)
Terrorist Kills ***Mean (STD DEV)***	0 (0)	2.05 (1.12)	3.55 (0.74)	0 (0)	1.95 (1.20)	4.15 (0.73)	0 (0)	2.20 (1.36)	3.90 (1.22)
Civilian Kills ***Mean (STD DEV)***	0 (0)	0.40 (0.58)	1.95 (1.20)	0 (0)	1 (0.71)	2.50 (1.57)	0 (0)	0.90 (0.83)	2.05 (1.75)

There were some major trends highlighted by the results of the experiments. Nodal violations decreased with both the increase of passive defensive and the increase of offensive cyber capability as shown in the node violation row. Vulnerabilities were reduced through better passive defensive measures, leaving fewer opportunities to successfully attack the node. However, increasing offensive cyber capabilities resulted in more kills, both civilian and cyberterrorist, evidenced by the terrorist kills and civilian kills rows. It is interesting to note that the mean nodal violations in experiment 4 runs counter to this trend. An explanation for this result is that the cyberterrorist may continue to exploit the vulnerability in the passive defense once breached. With 50% passive defense, terrorists have easy access to the critical node, but they move away from the node after their strike. With 95% passive defense, most terrorists do not find the small gaps in security. At 80% passive defense, node violations have both the highest average and the highest standard deviation. This indicates that on some runs of the simulation the passive defense restricts access to the critical node, but once they do breach the defense they continue to bounce around inside the defensive perimeter, scoring multiple attacks.

Even with the increase of passive defensive measures the data illustrates that an increase of offensive cyber capability contributes to a rise in civilian false flags, as indicated by the number of civilian kills. It is also important to note that the increase of the offensive cyber capability increases the likelihood of securing the node in the 80% passive defense case.

Table 2 focuses on the adjustment of the offensive cyber capability variable. The comparison was chosen to examine the relationship of the offensive cyber capability to a high passive defense setting. As outlined before it is clear that increasing the amount of cyber capability will contribute to a rise in terrorist and civilian kills. In order to accept the findings we must submit the data to a statistical test to ensure that the data is statistically significant. The first row identifies what we are measuring (terrorist or civilian kills). The second row outlines the experiment number followed by the passive defense level and then the offensive cyber capability level (the only variable to change in both experiments). The p value is used to calculate the

statistical significance of the data using the student's t-test. With a null hypothesis that there is no statistical difference in terrorist kills between the three levels of offensive cyber capability, the p values show that we can reject the null hypothesis at the 1% confidence level. Likewise, the null hypothesis that there is no statistical difference in civilian kills between the three levels of offensive cyber capability is rejected at the 1% confidence level.

Table 2. Student test of the significance of number of terrorist and civilian kills.

Terrorist Kills			
Experiment Number	**Ex 7**	**Ex 8**	**Ex 9**
Passive Defense Level	**95%**		
Cyber Capability Level	**NONE (0)**	**MED (10)**	**HIGH (20)**
Terrorist Kills *Mean*	0	2.20	3.90
	Ex 7 & 8	**Ex 8 & 9**	**Ex 7 & 9**
P Value	5.39E-07	8.49E-04	1.01E-11
Statistical Significance	99.99%	99.99%	99.99%

Civilian Kills			
Experiment Number	**Ex 7**	**Ex 8**	**Ex 9**
Passive Defense Level	**95%**		
Cyber Capability Level	**NONE (0)**	**MED (10)**	**HIGH (20)**
Civilian Kills *Mean*	0	0.90	2.05
	Ex 7 & 8	**Ex 8 & 9**	**Ex 7 & 9**
P Value	7.41E-05	2.48E-02	2.48E-02
Statistical Significance	99.99%	99.98%	99.98%

Table 3 focuses on the effects of passive defense and is set up similar to Table 2 but focused on the amount of nodal violations. The comparison was chosen to examine the relationship of a high offensive cyber capability to different settings of a passive defense. Again the student t-test rejects the null hypothesis that there is no statistical difference in the increase of passive defensive levels with a high offensive cyber capability with a 1% confidence level. Results of the tests were statistically significant supporting the observation that as passive defensive measures are increased, the likelihood of nodal violations decreased.

Table 3. Passive Defense Statistical Test

Effects of Passive Defense		
Experiment Number	**Ex 3**	**Ex 7**
Passive Defense Level	**50%**	**95%**
Cyber Capability Level	**HIGH (20)**	
Node Violation *Mean*	3.85	1.45
P Value		1.02E-02
Statistical Significance		99.99%

The most significant result from the agent based model is that an offensive cyber capability has demonstrated the ability to reduce acts of cyberterrorism, however risk of collateral damage rises with the increase of offensive cyber capability usage. An offensive cyber capability is a legitimate option, however there are many issues that the U.S. government struggles with that prevents the unrestricted use of an offensive cyber capability.

National Implications of Cyberterrorism

Cyberterrorism is not an easy threat for the U.S. government to address. The arguably successful strategy of nuclear deterrence does not apply well to the threat of cyberterrorism. The U.S. government does not have the capability to accurately attribute responsibility to an attacker, thereby limiting the option to retaliate. Considering cyberterrorism as an act of war would severely limit political options and may conflict with interests of other states. The cyberterrorist threat is not just limited to non-state actors. Other nations have expressed interest in using cyberspace as a means to gain a marked advantage over their adversary. There is nothing preventing these states from exploiting U.S. Internet vulnerabilities to satisfy their own interests. Currently, U.S. policy has placed increased attention to the protection of the cyberspace arena and

the formation of the CYBERCOM headquarters serves as indicators that the Internet is a critical asset that must be protected. In light of these issues, an offensive cyber capability can seem to be a significant risk reduction measure that can yield results.

One of the main questions that arises concerning cyberterrorism is can it be deterred? Lawrence Freedman defines deterrence as a coercive strategy that "involves the purposive use of overt threats of force to influence another's strategic choices. It presumes that the opponent will retain a capacity to make critical choices throughout the course of a conflict."[89] It is a defensive strategy that lets the potential attacker know that preparations have been made and the battle will inflict enough pain to deter aggression. A key example would be the nuclear standoff between the U.S. and the Union of Soviet Socialist Republics. Each side possessed enough of a nuclear stockpile that the concept of mutually assured destruction became the strategy. The concept relied on the perception that there was a sufficient second strike capability that it was not rational for the aggressor to initiate an attack. It is debatable whether deterrence prevented nuclear war; however the lack of war involving nuclear weapons after World War II provides the historical basis for the plausibility of deterrence theory. Throughout Freedman's book he limits his argument to state actors who are rational in thought. "Terrorists are not bound by traditional norms of political behavior between states," therefore their decisions may not be viewed as rational, counteracting the intended deterrence effect.[90]

Cyberterrorism highlights other issues that serve to prevent deterrence from working. Nuclear deterrence was based on overwhelming destructive power whereas cyberterrorism cannot be deterred in the same way. Cyber deterrence has many apparent flaws based on the answers to the following three questions. First, do we know who did it? Not only is it difficult to attribute a

---

[89] Lawrence Freedman, *Deterrence* (Cambridge UK: Polity Press, 2004). 26.

[90] Anthony H. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (Westport CT: Praeger Publishers, 2002), 28.

cyber attack to a state but also it is harder to convince third parties that the attacking state is indeed guilty. Computer systems and the packets they generate are very similar at a low level, making it hard to collect evidence necessary to attribute blame to anyone or a state. Also, computer systems and software are becoming more complex, making it easier for an offender to disguise their actions.

Second, can we hold their assets at risk? If the U.S. retaliates and does not cripple or destroy the attacker, credibility will be lost. If credibility is lost then deterrence cannot work. Even worse, it is possible that third parties may see our actions as offensive or disproportionate, spurring further cyber attacks.

Last, can we do so repeatedly?[91] What the author means by "do so repeatedly" is can the state continue to retaliate in the same manner if another cyberterrorist act happens? Although vulnerabilities in technology exist, that does not mean that the same vulnerability can be taken advantage of repeatedly. It is fair to assume that the targeted system will try to fix any vulnerability that is apparent and will continue to upgrade their network security, making it improbable that the same technique of cyber attack will continue to work. Cyber deterrence is problematic and has the potential to reduce credibility thereby reducing any intended deterrence effect.

According to Clausewitz, war is *"…an act of force to compel our enemy to do our will."*[92] War involves actors working to achieve a political purpose that compete over resources, ideologies or over power resulting in a stalemate, victory or loss. "International law does not define the term 'act of war.'"[93] International law views war and peace as distinctive forms of

---

[91] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica CA: The RAND Coorporation, 2009), 39.

[92] Carl V. Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1984), 75.

[93] Beidleman, Scott W. "Defining and Deterring Cyber War" (Research paper, U.S. Army War College, 2009), 11.

relations between states and that war (other than in self-defense) has been outlawed through international agreements and the Charter of the United Nations.[94] Currently, the U.S. has 11 formal declarations of war for reasons of "armed attacks on United States territory or its citizens and threats to United States rights or interests as a sovereign nation."[95] Of note, the joint resolution authorizing force against the terrorist attacks against the U.S. "authorizes military force against not only nations but also organizations and persons linked to the September 11, 2001, attacks on the United States."[96] This marks the first time in U.S. history that military force has been extended to cover organizations and persons linked to the terrorist actions of the 9/11 attacks. While the war on terror was based upon this authorization, cyberterrorism is different from the 9/11 attacks. Captain Kelli Kinley focused her research paper on the question of what would constitute an act of war in cyberspace. Kinley concludes that there is no definitive answer to the question.[97] The major implication of her study is that governments need to relook their cyber laws and treaties due to the fact that technological changes are not addressed in the various forms of policy.

Cyberterrorism cannot be considered an act of war according to current international rules. Any cyber attack would not conform to the definition of armed attack. According to The UN General Assembly's Resolution 3314, actions that would define armed attack would be "invasion or attack, bombardment, blockade of ports or coasts, and attacks on land, sea, or air forces of another state."[98] Each of the examples are limited to the battlespaces of land, sea and air without

---

[94] U.S. Congressional Research Service, "Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications, 2007," http://www.fas.org/sgp/crs/natsec/RL31133.pdf (accessed July 08, 2010), 22.

[95] Ibid., Summary.

[96] Ibid., 17.

[97] Kinley, Kelli, "What Constitutes an Act of War in Cyberspace?" (Research paper, Department of the Air Force Air University, 2008), 58.

[98] Beidleman, Scott W., "Defining and Deterring Cyber War" (Research paper, U.S. Army War College, 2009), 12.

any reference to cyberspace.

Currently, the UN does not have any resolution that covers the act of cyber warfare.[99] On April 27 2007, the country of Estonia suffered a massive cyber attack due to the movement of a Soviet memorial. Estonia has a robust telecommunications infrastructure with wide access to and heavy reliance on the Internet. The attack was allegedly sponsored by Russia and focused on denial of service to government, commercial and public infrastructure. Although this attack adversely affected the Estonian government and its people, NATO denied that the cyber attack was an act of war.[100]

Although cyberterrorism has the potential to inflict great harm on the U.S., treating it as an act of war would be problematic. The first reason is that the Internet is a pubic infrastructure, therefore there needs to be international consensus on what would constitute an act of war. While the U.S. can easily take the lead in cyber security, not every country is as concerned about the subject. There are many countries that are not as dependent on the Internet as the U.S. and cyberterrorism does not pose an immediate threat to these states. Declaring war due to a cyberterrorist act would possibly invite criticism from states that do not see cyberterrorism as a threat. "If the state responded to a cyberattack by retaliating, those skeptical of the claim might regard the response as illegitimate if it used a different modality from that of the attack itself."[101] Most important is the question of attribution. It is very difficult to attribute responsibility to any state or non-state actor that perpetrates hostile cyber activity. There is also the ability for a state or non-state actor to commit a hostile cyber act and blame it on someone else (false flag) or even worse, the possibility that the U.S. may retaliate against an innocent state. Based upon these reasons, it is not recommended to make a cyber attack an act of war. It risks losing U.S.

---

[99] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica CA: The RAND Coorporation, 2009), 179.

[100] Ibid., 179.

[101] Ibid., 180.

legitimacy and has the potential of limiting options of the political leadership by resorting directly to war.

State actors have the ability to actively sponsor terrorism. Countries are actively seeking advantage in the cyberspace domain by organizing offensive cyber capabilities. Cox argues "none of the thirteen international treaties on terrorism designate state actors as possible perpetrators of terrorism. Generally, there is a rich international legal tradition which defines only non-state actors as potential perpetrators of terrorism."[102] However, the Department of State (DOS) currently lists Iran, Sudan, Syria, and Cuba as state sponsors of terrorism. Based on the anonymity of cyberspace, these state entities can use the Internet without fear of reprisal or negative political effects. The April 2007 cyber attack on Estonia serves as an example of online state anonymity. Estonia had become one of Europe's most Internet dependent societies with the bulk of government and commercial services conducted over the medium. The removal of a Soviet WWII memorial incited a Denial of Service Attack (DoS) targeted towards government, news media, banking and communications firms. Russia was immediately suspected of the attacks, however, Russia's ambassador in Brussels, Vladimir Chizhov stated "I don't support such behavior, but one has to look where they [the attacks] came from and why."[103] NATO has acknowledged that the DoS attack is beyond the capability of individual players however both the EU and NATO did not place blame on Russia for the cyber attack. No conclusive evidence has linked Russia to the event, yet it is believed that the action could not occur without the consent of the Russian government.

There are three ways that a State can be involved in terrorism. First, they can support terrorist organizations, provide financial aid, ideological support, military or operational

---

[102] Dan G. Cox, John Falconer and Brian Stackhouse, *Terrorism, Instability, and Democracy in Asia and Africa* (Boston: Northeastern University Press, 2009), 16.

[103] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, 17 May, 2007.

assistance. Second, they can initiate, direct and perform terrorist activities through groups outside their own institutions. Last, they can perpetrate terrorist acts abroad by intentionally attacking noncombatants in other countries to achieve political aims.[104] Military planners in China believe that terrorism can be used to wage war against the United States. Their focus on computer hacking and asymmetric warfare will continue to drive their search for vulnerabilities that can be exploited.

> this kind of war means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It means that all weapons and technology can be superimposed at will, it means that all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed, and it also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten[105]

According to this work, military theorists in China are actively looking for any asymmetrical attacks to include network vulnerabilities that may be used to gain a marked advantage. Although this is a topic of ongoing debate, cyberspace provides the potential for states to commit cyberterrorist acts.

Conclusion

The continual growth of cyberspace and the increasing dependency by Americans on the cyber domain continues to set conditions for a cyberterrorist attack. As time progresses, methods of communication are continually converging through the network, creating additional vulnerabilities that can be leveraged. Cyberspace is an entity that is privately held and used for international commercial purposes, hindering any attempts made to secure cyberspace as a battle domain. The U.S. government's concern for security is in constant conflict with businesses'

---

[104] Ganor, Boaz, "Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?," http://www.understandterror.com/articles/Defining%20Terrorism%20by%20Dr%20Boaz%20Ganor.pdf (accessed July 05, 2010).

[105] Qiao Laing and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Panama: Pan American Publishing Company, 2006), 5.

desire for profits. Increased security measures incur costs and the sharing of network security lessons with competing business and government can run counter to the competitive edge that businesses seek. Disagreement on copyright and corporate espionage laws between different states further exacerbates this issue. The current policy of enhancing cooperation between government and industry is problematic, as the government cannot force international industry to increase its network security. Adding to the dilemma is the fact that businesses that invest heavily in Internet security can still be compromised by vulnerabilities elsewhere in the network, further detracting from the generation of profit. The Internet is also an international communications medium that does not fall under the control of any one state. Laws, regulation and practices that may forbid actions in one state may be legal in another. Taking offensive cyber action in another country can be seen as not only illegal but a violation of sovereignty. U.S. citizens desire freedom of the Internet, additional security measures run the risk of denying unrestricted access thereby infringing on their freedom.

Deterrence or the treatment of cyberterrorism as an act of war is highly problematic. The anonymity offered by the Internet grants the cyberterrorist the ability reduce the effectiveness of any counterstrike. Also, cyberterrorists are not restricted by the traditional norms of state behavior further complicating any effective deterrence policy. Cyberterrorism is not an act of war according to UN General Assembly Resolution 3314, U.S. policy does not address the topic and there is no international consensus that would define an act of war in the cyberspace realm. Further complicating matters is the likely negative international response to a declaration of war, following cyber attack due to the questions of attribution and varying state interests. Other states may find our actions too severe or question our motives, polarizing international relations. The basic loss of political options and possible loss of U.S. legitimacy may prevent a cyberterrorist attack from being immediately classified as an act of war.

There is a balance between an offensive cybercapability and passive defensive measures that must be achieved in order to attain an acceptable level of network security. Increased passive

defensive measures can reduce vulnerabilities, thereby mitigating the threat of cyberterrorist attack. However, public and industrial interests will continue to challenge the strength of the passive defensive measures, creating network vulnerabilities that can be taken advantage of. Offensive cyber capability also has the potential to reduce the threat of cyberterrorism. It is clear from the agent based model that the addition of this resource with passive defensive measures can lead to higher cyberterrorist kills and fewer nodal compromises.

Offensive cyber capabilities grant the state the ability to take direct action against a perceived threat, however the risk is high for attacking an innocent bystander. Civilians can lose the ability to access the Internet, be incarcerated or become physically harmed. This raises the issue of what actions must be taken to address this risk. It is possible to incorporate a legal process, similar to a warrant process, in which the government must prove an unlawful act at the risk of losing the advantage of surprise. Civilians that have been wrongly targeted may have a recourse system to restore their privileges and clear their name of all charges. Another major issue is that of state sovereignty. If activity is traced to foreign countries, the U.S. may not have the ability to act due to the status of diplomatic relations. Both these issues serve to illustrate the weaknesses of focusing on an offensive cyber capability to secure cyberspace.

Suggested Topics for Further Research

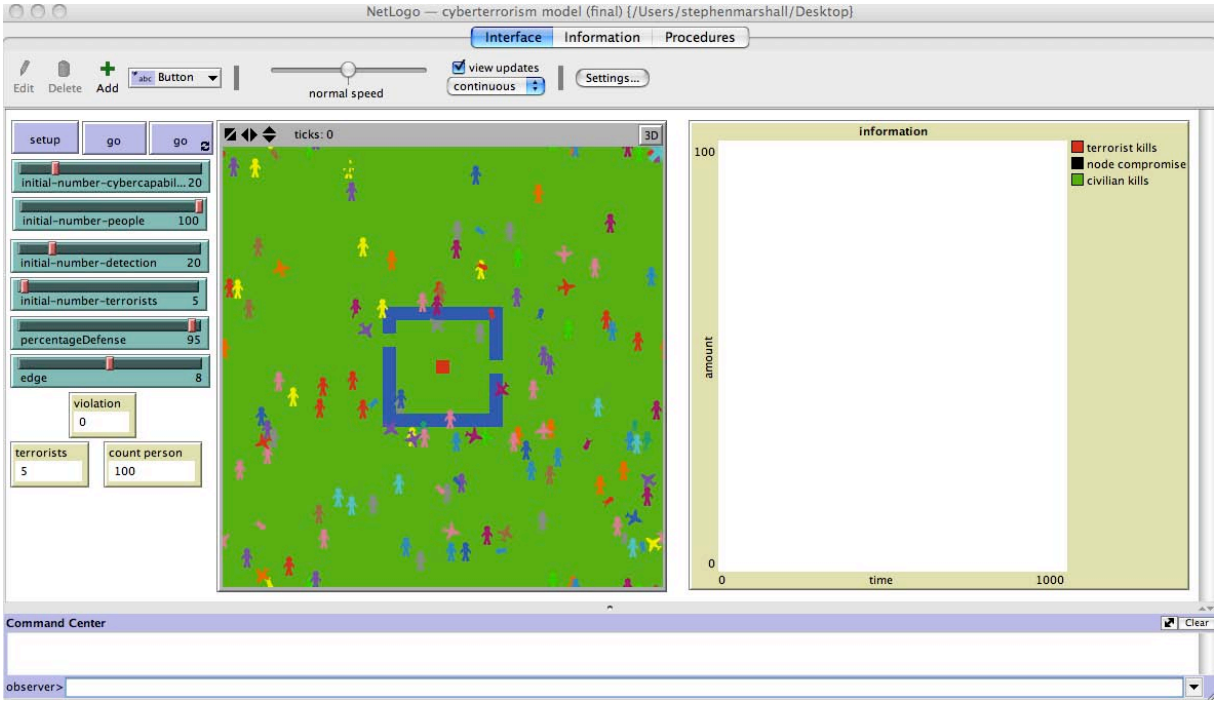
This monograph has explored the possibility of a cyberterrorist attack and the utility of the offensive cyber capability, however further research is needed in the following areas in order to expand the knowledge base of cyberterrorism. First, collection of more representative data would serve to make the model more useful. It would also be informative to have better resolution on who or what type of organization would conduct a cyberterrorist attack. This information can generate ideas to focus training for the offensive cyber capability. Who would be the lead agency identified to resource, plan and defend against a cyberterrorist attack? There are many different agencies that have jurisdiction within the U.S. and abroad and identification of

who is in charge of what actions can serve to reduce confusion. Finally, what is the optimal balance between passive defense and an offensive cyber capability? Research in the above topic areas will serve to widen the body of knowledge, adding to a deeper understanding of cyberterrorism.

Appendix (NetLogo)

The NetLogo Cyberterrorism source code can be copied and pasted into the procedures window of a new NetLogo program. The user must insert the control buttons, sliders, plots and monitors (as per the following example) in the interface window of the NetLogo program to avoid code errors. The errors result from the program trying to link commands with the corresponding controllers that are not immediately available when a new NetLogo program is opened. Users unfamiliar with NetLogo can download the user manual for further clarification on how to insert the required control buttons, sliders, plots and monitors.

Example of the Cyberterrorism Model Interface



Cyberterrorism Model Complete Source Code

```
breed [person]
breed [arrow]
breed [airplane]
breed [bug]
arrow-own [energy]
globals [halfedge needtobounce violation]
turtles-own [flagged flag-timer]

;;;;;;;;;;;;;;;;;;;;;;;;
;;; Setup procedures ;;;
;;;;;;;;;;;;;;;;;;;;;;;;

to setup
  clear-all
  set-default-shape person "person"
  create-person initial-number-people
    [ setxy random-xcor random-ycor
      set size 1.5
      set flagged false
      set flag-timer 0]
  set-default-shape arrow "arrow"
  create-arrow initial-number-terrorists
  ;;allows terrorists to randomly appear from all four corners preventing
  ;;terrorists from starting within the defensive peremeter
    [ setxy 16 16
      set size 1.5
      set flagged false
      set flag-timer 0]
  set-default-shape airplane "airplane"
  create-airplane initial-number-cybercapability
    [ setxy random-xcor random-ycor
      set size 1.5
      set flagged false
      set flag-timer 0]
  set-default-shape bug "bug"
  create-bug initial-number-detection
    [ setxy random-xcor random-ycor
      set size 1]
  setup-patches
  set violation 0
end

to setup-patches
  ask patches [ set pcolor green ]
  ask patches [
```

```
    ;;set position of node to center and color of node to red
    if pxcor = 0 and pycor = 0 [set pcolor red]
    ]
  ;;Defensive permeter settings
  set halfedge int (edge / 2)
  ask patches[
   if (pxcor = (- halfedge) and pycor >= (- halfedge) and pycor <= (0 + halfedge) )
    [if ( random 100 < percentageDefense ) [
    set pcolor blue] ]
   if ( pxcor = (0 + halfedge) and pycor >= (- halfedge) and pycor <= (0 + halfedge) )
    [if ( random 100 < percentageDefense ) [
    set pcolor blue] ]
   if ( pycor = (- halfedge) and pxcor >= (- halfedge) and pxcor <= (0 + halfedge) )
    [if ( random 100 < percentageDefense ) [
    set pcolor blue] ]
   if ( pycor = (0 + halfedge) and pxcor >= (- halfedge) and pxcor <= (0 + halfedge) )
    [if ( random 100 < percentageDefense ) [
    set pcolor blue] ]
   ]
end

to randomize
  setxy random-xcor random-ycor
  if pcolor = blue
    [ randomize ]
end

;;;;;;;;;;;;;;;;;;;;
;;; Go procedures ;;;
;;;;;;;;;;;;;;;;;;;;

to go
  ask patches [ if pcolor = black [
                      set pcolor red
                      set violation violation + 1]]
  ask turtles [ bounce
    fd 1
    if flagged = true [set flag-timer flag-timer + 1]
    if flag-timer > 20 [set flag-timer 0
                    set flagged false
                    set color orange]
    ]
  tick
  eat-node
  eat-terrorist
  grow-capacity
  find-terrorist
  update-plot
end

;;command to enable terrorists to attack node
```

```
to eat-node
  ask arrow [
    if pcolor = red [
    set pcolor black
    show count turtles
    set energy (energy + 10)
    ]
  ]
end

to-report absolute-value [number]
end

to eat-terrorist
  ask airplane [
    catch-arrow
    catch-person]
end

to grow-capacity
  ask arrow [
    if color = blue [hatch 0 [setxy random-xcor random-ycor
  set color black] ] ]
end

;;command to identify terrorists (from pool of civilians and terrorists)
to find-terrorist
  ask bug [ let suspect one-of arrow-here
           if suspect != nobody
           [
              if random-float 100 <= 10 [
                ask suspect [
                  set flagged true
                  set color white]]
           ]
]
   ask bug [ let suspect one-of person-here
            if suspect != nobody
            [
                  if random-float 500 <= 1 [
                  ask suspect [
                    set flagged true
                    set color white  ]]
            ]
]
end

to catch-person
  let prey one-of person-on neighbors
    if prey != nobody
    [ ask prey [ if flagged [die ]]
```

```
      ]
end

to catch-arrow
    let prey one-of arrow-on neighbors
  if prey != nobody [
     ask prey [ if flagged [die ]
     ]
   ]
end

to bounce
  set needtobounce false
  ask patch-ahead 0 [if pcolor = blue
    [set needtobounce true] ]
    if needtobounce
    [ set heading (heading + 170) ]
end

to move-turtles
  ask turtles [
    right random 360
    forward 1
    ]
end

to update-plot
  set-current-plot "information"
  set-current-plot-pen "terrorist kills"
  plot count arrow
  set-current-plot-pen "civilian kills"
  plot count person
  set-current-plot-pen "node compromise"
  plot violation
 end
```

Bibliography

Beidleman, Scott W. “Defining and Deterring Cyber War.” Research paper, U.S. Army War College, 2009.

Brown, Lawrence V. *Cyberterrorism and Computer Attacks*. New York: Novinka Books, 2006.

Caulkins, Bruce D. *Proactive Self-Defense in Cyberspace*. Virginia: The Land Warfare Papers, 2009.

Carafano, James J. and Mark A. Sauter. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. New York: McGraw-Hill, 2005.

Checkland, Peter and John Poulter. *Learning for Action: A Short Definitive Account of Soft Systems Methodology and its use for Practitioners, Teachers and Students*. England: John Wiley & Sons, Ltd, 2006.

Cilluffo, Frank J., Bruce D. Berkowitz and Stephanie Lanz eds,. *Cybercrime…Cyberterrorism…Cyberwarfare…:Averting An Electronic Waterloo*. Washington DC: The CSIS Press, 1998.

Clausewitz, Carl V. *On War*. New Jersey: Princeton University Press, 1984.

Collier, David, Fernando Daniel Hidlago and Andra Olivia Maciuceanu. “Essentially contested concepts: Debates and applications.” http://polisci.berkeley.edu/people/faculty/CollierD/Collier%20Gallie.pdf (accessed August 26, 2010).

Cordesman, Anthony H. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Connecticut: Praeger Publishers, 2002.

Corman, Steven R. and Jill S. Schiefelbein. “Communication and Media Strategy in the Jihadi War of Ideas.” http://comops.org/publications/CSC_report_0601-jihad_comm_media.pdf (accessed July 08, 2010).

Cox, Dan G., John Falconer and Brian Stackhouse. *Terrorism, Instability, and Democracy in Asia and Africa*. Boston: Northeastern University Press, 2009.

CSIS Task Force Report, *Cybercrime…Cyberterrorism…Cyberwarfare…: Averting an Electronic Warterloo*. Washington D.C.: The CSIS Press, 1998.

Denning, Dorothy E. “Special Oversight Panel on Terrorism Hearing on Terrorist Threats to the United States: Statement of Dorothy E. Denning.” http://armedservices.house.gov/comdocs/testimony/106thcongress/00-05-23denning.htm (accessed July 04, 2010).

Dunnigan James F. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press, 2003.

Dykman, Peter. “Terrorism and Cyberspace.” Research paper, Kansas State University, 2009.

Flynn, Stephen. *The Edge of Disaster*. New York: Random House Publishing Group. 2007.

Freedman, Lawrence. *Deterrence*. Cambridge UK: Polity Press, 2004.

Forest, James J. F. *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*. Connecticut: Praeger Security International, 2008.

Ganor, Boaz. "Defining Terrorism: Is one Man's Terrorist Another Man's Freedom Fighter?" http://www.understandterror.com/articles/Defining%20Terrorism%20by%20Dr%20Boaz%20Ganor.pdf (accessed July 05, 2010).

Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies—and What it Means to Be Human.* New York: Broadway Books, 2005.

Golumbic, Martin C. *Fighting Terror Online: The Convergence of Security, Technology, and the Law*. Israel: Springer Science and Business Media, 2008.

Janczewski, Lech, J. and Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism*. New York: Information Science Reference, 2008.

Kalyvas, Stathis N. *The Logic of Violence in Civil War*. New York: Cambridge University Press, 2008.

Kinley, Kelli. "What Constitutes an Act of War in Cyberspace?" Thesis, Department of the Air Force Air University, 2008.

Kramer, Granklin D., Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security*. Washington DC: Potamac Books, Inc., 2009.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America.* Panama: Pan American Publishing Company, 2006.

LeBaron, Wayne D. *Five Deadly Arrows of Terrorism: A Manual of Information and Protection.* New York: Nova Science Publishers, Inc., 2007.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. California: RAND Coorporation, 2009.

Lindgren, Mats and Hans Bandhold. *Scenario Planning: The link between future and strategy.* England: Palgrave Macmillan, 2003.

Newman, David. *Boundaries, Territory and Postmodernity*. New York: Frank Cass. 1999.

National Intelligence Council. Mapping the Global Future: Report of the National Intelligence Council's 2020 Project. http://www.foia.cia.gov/2020/2020.pdf (accessed July 03, 2010).

Pfaltzgraff, Robert L. and Richard H. Shultz. *War in the Information Age: New Challenges for U.S. Security Policy*. Washington: Brassey's, 1997.

Robertson, Ann E. *Terrorism and Global Security*. New York: Infobase Publishing, 2007.

Trinquier, Roger, *Modern Warfare: A French View of Counterinsurgency*. Kansas: Combat Studies Institute, 1985.

U.S. Army Training and Doctrine Command. *DCSINT Handbook No. 1.02. Cyber Operations and Cyber Terrorism*. Kansas: Government Printing Office, 2005.

U.S. Army Training and Doctrine Command. "Cyberspace Operations Concept Capability Plan 2016-2028." http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf (accessed July 03, 2010).

U.S. Congressional Research Service. "Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications, 2007." http://www.fas.org/sgp/crs/natsec/RL31133.pdf (accessed July 08, 2010).

U.S. Department of Homeland Security. "Department of Homeland Security." http://www.dhs.gov/files/programs/gc_1189168948944.shtm (accesed July 05, 2010).

U.S. Department of Homeland Security. "National Strategy For Homeland Security, 2007." http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed July 03, 2010).

U.S. Director of National Intelligence. "Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence, 2010." http://www.dni.gov/testimonies/20100202_testimony.pdf (accessed July 04, 2010).

U.S. President. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009." http://www.wired.com/images_blogs/threatlevel/2009/05/cyberspace_policy_review_final.pdf (accessed July 04, 2010).

U.S. President. "The National Security Strategy of the United States, 2006." http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/ (accessed July 03, 2010).

U.S. President. "The National Security Strategy of the United States, 2010." http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed July 03, 2010).

U.S. President. "The National Strategy to Secure Cyberspace, 2003." http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed July 03, 2010).

U.S. President. "The Comprehensive National Cybersecurity Initiative, 2009." http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed July 03, 2010).

U.S. Defense Department. "Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy. 2009." http://iase.disa.mil/policy-guidance/dasd_ciia__strategy_aug2009.pdf (accessed July 03, 2010).

U.S. Defense Department. "Joint Publication 1-02: The Department of Defense Dictionary of Military and Associated Terms, 2010." http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed July 04, 2010.)

U.S. Defense Department. "National Defense Strategy, 2008." http://www.defense.gov/pubs/2008NationalDefenseStrategy.pdf (accessed July 03, 2010).

U.S. Defense Department. "The National Military Strategy for Cyberspace Operations (U), 2006." http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed July 04, 2010).

U.S. Defense Department. "U.S. Cyber Command Fact Sheet May 25, 2010." http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf (accessed July 03, 2010).

Verton, Dan. *Black Ice: The Invisible Threat of Cyber-Terrorism*. New York: McGraw-Hill, 2003.

Weimann, Gabriel. *Terror on the Internet: The New Arena, The New Challenges*. Washington, DC: United States Institute of Peace Press, 2006.

Wilensky, U. NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling, Northwestern University. Illinois. 1999.