2007-12

Cyberterrorism cyber prevention vs cyber recovery

DiBiasi, Jeffrey R.

Monterey California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERTERRORISM: CYBER PREVENTION VS CYBER RECOVERY

by

Jeffrey R. DiBiasi

December 2007

Thesis Advisor:	Letitia Lawson
Second Reader:	Daniel Moran

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
December 2007

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE CyberTerrorism: Cyber Prevention Vs Cyber Recovery

5. FUNDING NUMBERS

6. AUTHOR(S) Jeffrey R. DiBiasi

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The technological age has forced the U.S. to engage a new set of national security challenges. Several potential adversaries have cyberspace capabilities comparable to those of the U.S., and are constantly conducting surveillance, gathering technical information, and mapping critical nodes that could be exploited in future conflicts. How can the U.S. government best defend against future cyber attacks? Recent policy documents set out a strategy for securing all of cyberspace, which experts argue is impossible to implement, but also unnecessary. This thesis seeks to move the discussion beyond this stalemate by undertaking an analysis of the vulnerability of cyberspace to terrorist attacks. The first analysis examines the Code Red Worm and the Slammer Worm. These two worms were selected because they were highly destructive and spread faster than normal worms, making them well suited for assessing the existing security of computers and networks. The next analysis examines a staged cyber attack on critical infrastructure, entitled Attack Aurora. In the staged Aurora attack, researchers from the Department of Energy's Idaho lab hacked into a replica of a power plant's control system. This attack is the most recent staged attack and facilitates an analysis of vulnerabilities of critical infrastructures to cyberterrorism.

14. SUBJECT TERMS
Cyberattacks, Cyberterrorism, Critical Infrastructure Protection (CIP) Computer Worms
CREVS Model, CARVER + Shock Model, Supervisory Control and Data Acquisition (SCADA)
Cyber Defense, Cyber Prevention, Firewalls, Food Safety and Inspection Service (FSIS)

15. NUMBER OF PAGES
65

16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

CYBERTERRORISM: CYBER PREVENTION VS CYBER RECOVERY

Jeffrey R. DiBiasi
Major, United States Air Force
B.S., Regis University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Author: Jeffrey R. DiBiasi

Approved by: Letitia Lawson
Thesis Advisor

Daniel Moran
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The technological age has forced the U.S. to engage a new set of national security challenges. Several potential adversaries have cyberspace capabilities comparable to those of the U.S., and are constantly conducting surveillance, gathering technical information, and mapping critical nodes that could be exploited in future conflicts. How can the U.S. government best defend against future cyber attacks? Recent policy documents set out a strategy for securing all of cyberspace, which experts argue is impossible to implement, but also unnecessary. This thesis seeks to move the discussion beyond this stalemate by undertaking an analysis of the vulnerability of cyberspace to terrorist attacks. The first analysis examines the Code Red Worm and the Slammer Worm. These two worms were selected because they were highly destructive and spread faster than normal worms, making them well suited for assessing the existing security of computers and networks. The next analysis examines a staged cyber attack on critical infrastructure, entitled Attack Aurora. In the staged Aurora attack, researchers from the Department of Energy’s Idaho lab hacked into a replica of a power plant’s control system. This attack is the most recent staged attack and facilitates an analysis of vulnerabilities of critical infrastructures to cyberterrorism.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to sincerely thank my wife, Michelle, and my son, Christopher, for their patience and love. This was truly a very challenging experience and at times, was quite stressful. I know that I would have never accomplished this rewarding milestone if it was not for their continuous love, support, and eagerness to help in anyway possible. A sincere thanks and gratitude goes to Professor Letitia Lawson. She was simply marvelous. She continually supported me and ensured I was always on the “right track.” Moreover, she tirelessly worked rewrite after rewrite with me and never showed any signs of frustration or aggravation. She was totally guiding me every step of the way. This is a key reason for my success. Above all, I would like to thank God for helping me with this thesis and my grad school experience at NPS. Without his love and guidance, I surely would have failed.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The information age has forced the U.S. to engage a new set of national security challenges. It now relies on the communication infrastructure to exchange information on strategic and tactical operations and provide services such as telecommunications, finance, aviation, transportation, electrical power, gas, and government/administration. Along with the rewards of an ubuquitous communication infrastructure comes new risks, including the threat of "cyberterrorism." This form of terrorism could cause havoc with critical infrastructures. Several potential adversaries have cyberspace capabilities comparable to those of the U.S., and are constantly conducting surveillance, gathering information, and mapping critical nodes that could be exploited in future conflicts. As a result, the U.S. can no longer rely on its geographical location in preventing an attack.

Denning describes cyberterrorism as "unlawful attacks and threats of attacks against computers, networks and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" and should "result in violence against persons or property, or at least cause enough harm to generate fear."[1] Cyberterrorism involves leveraging cyberspace as a primary weapon to generate political or social change. It is important to recognize that cyber-terrorism is a tactic that can be used to achieve broader strategic objectives.[2]

The cyberterror threat is exacerbated by the fact that the ability to network has far outpaced the ability to protect networks. The internet was designed as an

[1] Dorothy Denning, "Cyberterrorism," *Global Dialogue*, August 24, 2000, 1, http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc, accessed 7 September 2007. See also Paraphrased from Bruce Hoffman's *Inside Terrorism. NY:* Columbia University Press, 1998. 14-15.

[2] Concepts derived from Dorothy Denning, prepublication copy of "Cyberterrorism", *Global Dialogue,* August 24, 2000, 1. Accessed on-line at http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc on 7 September 2007.

open platform, lending accessibility to those who know how to access the platform. Furthermore, most information systems have been engineered in the most economically efficient manner, and are therefore dependent upon a small number of applications. This makes them exceptionally vulnerable to attack.[3] Internet connected computers or servers are broken into every 20 seconds by hackers, identity thieves, and other mischievous people who want to cause havoc to networks. Terrorist could easily copy the techniques of these groups, giving them the power to disrupt parts of the cyberspace network.[4]

Due to advanced adversary technology, enemies now can choose between military and commercial information operation infrastructures. Enemies know that the Department of Defense (DOD) has several networks within the Pentagon; however, they also know that all U.S. commerce is accomplished utilizing commercial systems and networks. As the U.S. government spends resources protecting one area, the other area is vulnerable to attack.[5]

Conversely, cyberterrorism conjures up images of vicious terrorists unleashing catastrophic attacks against computer networks, wreaking havoc, and paralyzing nations.[6] While the cyberterrorism threat has increased, the fears of many Americans are exaggerated.[7] Generic distrust of computer technology, overblown articles in the media, and a lack of understanding of government strategies and policies combine to generate panic.

How can the U.S. government best defend against future cyber attacks? Recent policy documents set out a strategy for securing all of cyberspace, which

[3] Russell Howard and James Forest. *Homeland Security and Terrorism* (New York, NY: Mcgraw-Hill, 2006), 116.

[4] Brian Krebs. “A Cybersecurity Role for Uncle Sam?” (April 2004); Russell Howard and James Forest. *Homeland Security and Terrorism* (New York, NY: Mcgraw-Hill, 2006), 126.

[5] Ibid., 3.

[6] Gabriel Weimann. “The Sum of All Fears?” *Studies in Conflicts and Terrorism* 28, no.3 (2005):5.

[7] Gabriel Weimann. *Terror on the Internet* (London: New York: USIP Press, 2006), 24-27; Gabriel Weimann. “The Sum of All Fears?” *Studies in Conflicts and Terrorism* 28, no.3 (2005):5.

experts argue is impossible to implement, but also unnecessary.[8] This thesis seeks to move the discussion beyond this stalemate by undertaking an analysis of the vulnerability of cyberspace to terrorist attacks, and then evaluating whether the potential costs and loses associated with such attacks are acceptable or indicate a need for improved cyberterrorism preparedness.

A. LITERATURE REVIEW AND THESIS ARGUMENT

There is a consensus in the literature on the nature of cyberterrorism threats. Because the internet was designed as an "open platform," adversaries can easily access vital information and disrupt information processing in critical areas.[9] Such attacks may come from individuals, non-state actors such as terrorist organizations, or states.[10] The largest potential threat in today's security environment is from terrorist organizations and this will therefore be the focus on this thesis. Organizations such as Al-Qaeda may seek to use information

[8] *Joint Publication (JP) 3-13*: *Information Operations,* Feb 13, 2006, Washington DC: Office of the Chairman, Joint Chiefs of Staff, 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jps_13.pdf Accessed (April 27, 2007); *Air Force Doctrine Document (AFDD) 2-5: Information Operations,* Jan 11, 2005, Washington DC: Air Force Publishing, 2005, http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5/afdd2-5.pdf Accessed (April 27, 2007). "The National Strategy to Secure Cyberspace" (February 2003) http://www.whitehouse.gov/pcipbl Accessed (December 5, 2006).

[9] Brian Lewis. "Information Warfare" http://www.fas.org/irp/eprint/syder/infowarfare.htm Accessed (December 5, 2006). Russell Howard, *Homeland Security and Terrorism* (New York: Mcgraw-Hill Companies, 2006), Chapter 10. "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructures" (February 2004) http://www.kantei.go.ip/foreign/it/security/2001/cyber_terror_sum.html Accessed (February 7, 2007). "Federal Bureau of Investigation, Congressional Testimony" http://www.fbi.gov/congress/congress02/nipc072402.htm Accessed (February 7, 2007)."Cyber Security" (February 2005) http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf Accessed (February 7, 2007).

[10] Frank Cilluffo and Nicholas Paul. "Cyberstrategy 2.0," (Spring 2006)http://www.securityaffair.org/issues/2006/10/cilluggo_nicholas.php Accessed (December 5, 2006). U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, *Cybersecurity Protection, testimony of Mr. George S. Forseman, 13 Sep 2006,* accessed via Lexis/Nexis on 1 Feb 07. *Report to Congressional Requestors on Internet Infrastructure,* Report number GAO-06-672, Washington, D.C., Government Accountability Office.

systems as "Weapons of Mass Effect" (WMEs) to gather information that will harm the U.S. communication infrastructure or significant portions of it.[11]

To confront the cyber threats to the Internet and portions of the communication infrastructure, the Joint Staff published Computer Network Operations (CNO), and the U.S. Air Force (AF) published the Network Warfare Operations doctrine in 2006.[12] These doctrines state that joint and AF forces will perform the mission of Computer Network Defense (CND) and Network Defense (NetD).[13] Several other government documents focus on cyberwarfare strategy and policy. Other government publications discuss policies aimed at reducing the vulnerabilities of critical infrastructure and information systems before cyber attacks occur.[14] The National Strategy to Secure Cyberspace seeks to protect all critical infrastructures, both public and private. Noting that cyberspace is comprised of a myriad of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work, the strategy provides direction to the federal government departments and agencies that have roles in cyberspace security and delineates steps that agencies, companies, and local governments can take to improve cyber security. In short, the strategy

[11]Frank Cilluffo and Nicholas Paul. "Cyberstrategy 2.0," (Spring 2006) http://www.securityaffair.org/issues/2006/10/cilluggo_nicholas.php Accessed (December 5, 2006). U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, *Cybersecurity Protection, testimony of Mr. George S. Forseman, 13 Sep 2006,* accessed via Lexis/Nexis on 1 Feb 07. *Report to Congressional Requestors on Internet Infrastructure,* Report number GAO-06-672, Washington, D.C., Government Accountability Office.

[12] *Joint Publication (JP) 3-13*: *Information Operations,* Feb 13, 2006, Washington DC: Office of the Chairman, Joint Chiefs of Staff, 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jps_13.pdf Accessed (April 27, 2007).

[13] *Air Force Doctrine Document (AFDD) 2-5: Information Operations,* Jan 11, 2005, Washington DC: Air Force Publishing, 2005, http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5/afdd2-5.pdf Accessed (April 27, 2007).

[14] *Information Operations Roadmap (DECLASSIFIED);* Gregory Rattray, *Strategic Warfare in Cyberspace,* Cambridge MA: The MIT Press, 2001. *Information Warfare – Defense (IW-D),* Washington DC: Office of the Under Secretary of Defense for Acquisition and Technology, 1996; a compendium of articles in Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden, eds. *Cyberwar: Security, Strategy, and Conflict in the Information Age,* Fairfax, VA: Armed Forces Communications Electronics Association International Press, 1996. Arthur F. Galpin, *Computer Network Defense for the United States of America,* Carlisle Barracks PA.

highlights the role of public-private engagement and provides a framework for contributions at all levels to secure various parts of cyberspace.[15]

The above policy documents clearly establish that the U.S. government believes it can and should secure all of cyberspace. However, many private experts argue that this is neither possible nor necessary. The National Strategy to Secure Cyberspace contains three strategic objectives: to prevent cyber attacks against America's critical infrastructures, to reduce national vulnerability to cyber attacks, and to minimize damage and recovery time from cyber attacks that could possibly occur. Critics argue that in order to secure all of cyberspace, it would be necessary to secure the "ephemeral space that exists only in relation to the medium of the internet," which is inherently chaotic and beyond the reach of any organized central control.[16] Thus, the U.S. government objective is simply unattainable. However, these experts also suggest that securing cyberspace in not necessary, noting that there is no recorded instance of a terrorist cyberattack on the Internet, networks, U.S. public facilities, transportation systems, nuclear power plants, power grids, or other key components of the national infrastructure.[17]

The U.S. government has not responded to the critics on the record. Instead, the National Strategy seems to have slipped in importance for both the Bush administration and the IT industry. There has been a dramatic decrease in the visibility of the strategy since its signing in February 2003. This has left the fundamental issues surrounding cyberterrorism and cyberdefense unresolved. This thesis therefore seeks to address them through analysis of the available

[15] "The National Strategy to Secure Cyberspace" (February 2003) http://www.whitehouse.gov/pcipbl Accessed (December 5, 2006). "Critical Infrastructure Protection" (January 2003) http://www.whitehouse.gov/news/releases/2001/10/20011016 Accessed (December 5, 2006).

[16] Michael Simmer. "The Tensions of Securing Cyberspace: The Internet, state power and the National Strategy to Secure Cyberspace" (March 2004):11. "The National Strategy to Secure Cyberspace" (February 2003) http://www.whitehouse.gov/pcipbl Accessed (December 5, 2006).

[17] Michael Simmer. "The Tensions of Securing Cyberspace: The Internet, state power and the National Strategy to Secure Cyberspace" (March 2004). "The National Strategy to Secure Cyberspace" (February 2003) http://www.whitehouse.gov/pcipbl Accessed (December 5, 2006).

evidence to determine if the current level of cybersecurity is sufficient or if additional investment in cyberdefense is required.

B. METHODOLOGY

In order to provide a grounded analysis of existing evidence, this thesis uses a within case analysis of non-terrorist cyber attacks on computers and web site servers, and a simulated terrorist attack on critical infrastructures in the United States. Cyber attacks on computers and servers are well known and straightforward. In such cases, terrorist attacks would generate economic and psychological costs to the individual and corporate owners and users of computers and networks, respectively. Cyber attacks on critical infrastructure pose a less widely recognized threat, and a potentially much more dangerous one. The federal government has identified eight important sectors of the economy that are critical to national security and the essential functioning of the U.S. economy: telecommunications, transportation, water supply, oil and gas production, banking and finance, electrical generation, emergency services, and essential government functions.[18] All of these systems have one item in common—their dependence on information systems that are susceptible to cyber attack.[19]

[18] Michael O'Neil "Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry," *Depaul Business Law Journal Vol 12, p. 97*, 1999/2000, http://www.cdt.org/publications/lawreview/2000depaul.shtml Accessed (December 5, 2006).

[19] Michael O'Neil "Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry," *Depaul Business Law Journal Vol 12, p. 97*, 1999/2000, http://www.cdt.org/publications/lawreview/2000depaul.shtml Accessed (December 5, 2006).The vulnerability of critical infrastructures and the unique risks associated with networked computing have been recognized for some time. However, the issue was given new urgency by the report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997, which highlighted the topic of critical infrastructures and made a series of specific recommendations for their protection. On May 22, 1998, the President approved Presidential Decision Directive 63 establishing a national critical infrastructure protection policy and a government framework to develop and implement infrastructure protection measures. Key organizations created in that directive were a National Infrastructure Protection Center (NIPC), located within the Federal Bureau of Investigation (FBI), with operational responsibilities, and a Critical Infrastructure Assurance Office (CIAO), administratively located in the Department of Commerce, which provides planning and coordination support to a National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, who is located in the National Security Council. On January 7, 2000, the Executive Branch issued its national plan for critical infrastructure protection. The document sets out a ten point program, focused on protection of the federal government's information systems.

The next chapter examines the Code Red Worm and the Slammer Worm. In laymen's terms, a worm is a form of a virus designed to copy itself by utilizing e-mail or other software applications. The main goal of using this technique is to permeate the network or portions of the Internet with malicious code that will affect the performance of certain software applications or will totally bring applications to a halt.[20] These two worms were selected because they were highly destructive and spread faster than normal worms, making them well suited for assessing the existing security of computers and networks. They were both attacks on computers, but the Slammer Worm also affected the network, and so can be used to assess the likely impact of a cyber terror attack on the network itself. The third chapter examines a staged cyber attack on critical infrastructure, entitled Attack Aurora. In the staged Aurora attack, researchers from the Department of Energy's Idaho lab hacked into a replica of a power plant's control system. This attack is the most recent staged attack and facilitates an analysis of vulnerabilities of critical infrastructures to cyberterrorism.

An adapted version of the CARVER + Shock model will be utilized for the analysis in each case. This model was originally developed by the military and later revised to assess possible vulnerabilities in the food industry looking at factors such as cost, impact, and recoverability within systems and infrastructures. The model breaks a potential target into segments and considers, per the acronym, its criticality, accessibility, recuperability, vulnerability, effect of loss, and recognizability elements. These elements are

[20] "The Menace of Worms" (October 2007) http://www.emisissoft.com/en/kb/articles/tec050629 Accessed (September 1, 2007). There are four types of worms: Instant messaging, Internet Relay Chat, File-sharing Network, and Internet. Instant messing worms infect websites to everyone on a local contact list. They have a minimal impact on software performance. Internet relay chat worms attack chat channels and spread malicious code by sending infected files or by sending links to infected websites. These type of worms can slow down network performance by 25%. File-sharing network worms copy themselves into a shared folder. This worm will place a copy of itself in a shared folder under a harmless name. Due to this fact, the worm would be ready for down load over any network and would spread malicious code throughout the entire network. These worms slow down network performance by 50%. Internet worms will scan all available network resources using local operating system services and scan the Internet for vulnerable machines. These worms slow down the network by 75%.

then analyzed to assess the shock, or psychological impact, of an attack, in addition to the economic impact.[21] Table 1 gives a short description of each CARVER + Shock element.

Figure 1 delineates the five point scales assigned to each of the elements of the original CARVER + Shock model. It also conveys the criteria for each of the assigned scales and shows how scores of 1 to 10 are assigned. The maximum total number of points in the original model is 70. Scores of 35 or higher warrant additional food system protection. This number is 50% of the total and is subjective, based on criteria set forth by the USDA.[22]

Element	Description
Criticality	**Considers the public health and economic impacts of a successful attack.**
Accessibility	**Relates to the attacker's physical access to the target. The target is accessible when the attacker has sufficient resources along with the physical ability to reach a specific location and achieve the desired effect.**
Recognizability	**The ease of identifying a target and is more significant for "outside" attackers.**
Vulnerability	**Evaluates whether the attacker has the means and resources accomplish an attack with the desired effect.**
Effect	**Relates to the actual, direct and immediate impact of the attack.**
Recuperability	**Ability to recover from an attack financially.**
Shock	**Focuses on the psychological effects of an attack and incorporates both the short and long-term behavioral changes that may be precipitated by an attack.**

Table 1. CARVER Definitions[23]

[21] "How to Effectively use the CARVER+Shock Method of Assessing Risk and Vulnerabilities" (April 2006) http://www.afdo.org/afdo/Conferences/upload/060617-0815-1-Rigby-AFDO%20CARVER%20training.pdf Accessed (July 29, 2007).

[22] *US FDA/CSFAN CARVER + Schock Testomonial,* web live video, directed by USD Accessed on line at http://www.cfsan.fda.gov/~dms/vltcarv.html Accessed (November 2007).

[23] *US FDA/CSFAN CARVER + Schock Testomonial,* web live video, directed by USD Accessed on line at http://www.cfsan.fda.gov/~dms/vltcarv.html Accessed (November 2007).

Criticality Scale

Criteria	Scale
Loss of over 10,000 lives or loss of more than $100 billion.	**9-10**
Loss of over 1000 -10,000 lives or loss of $10 billion - $100 billion.	**7-8**
Loss of 100 – 1000 lives or loss of $1 billion -$10 billion.	**5-6**
Loss of less than 100 lives or loss of less than $1 billion.	**3-4**
No Loss of live or loss of less than $100 million	**1-2**

Accessibility Scale

Criteria	Scale
Easily Accessible	**9-10**
Accessible	**7-8**
Partially Accessible	**5-6**
Hardly Accessible	**3-4**
Not Accessible	**1-2**

Recuperability Scale

Criteria	Scale
> 1 year	**9-10**
6 months to 1 year	**7-8**
3 – 6 months	**5-6**
1 – 3 months	**3-4**
< 1 month	**1-2**

Vulnerability Scale

Criteria	Scale
Target characteristics allow for easy introduction of sufficient agents to achieve aim.	**9-10**
Target characteristics almost always allow for easy introduction of sufficient agents to achieve aim.	**7-8**
Target characteristics allow 30 to 60% probability that sufficient agents can be added to achieve aim	**5-6**
Target characteristics allow 10 to 30% probability that sufficient agents can be added to achieve aim	**3-4**
Target characteristics allow low probability (less than 10%) sufficient agents can be added to achieve aim	**1-2**

Effect Scale

Criteria	Scale
Greater than 50% of the system's production impacted.	**9-10**
25 – 50% of the system's production impacted.	**7-8**
10 – 25 % of the system's production impacted.	**5-6**
1 – 10 % of the system's production impacted.	**3-4**
Less than 1% of the system's production impacted.	**1-2**

Recognizability Scale

Criteria	Scale
The target is cleary recognizable and requires little or no training for recognition.	**9-10**
The target is easily recognizable and requires only a small amount of training for recognition.	**7-8**
The target is difficult to recognize or might be countered with other targets or target components and requires some training for recognition.	**5-6**
The target is difficult to recognize. It is easily confused with other targets or components and requires extensive training for recognition	**3-4**
Less than 1% of the system's production impacted.	**1-2**

Shock Scale

Criteria	Scale
Target has major historical, cultural, religious, or other symbolic importance. Loss of over 10,000 lives. Major impact on sensitive subpopulations, e.g. children or elderly. National economic impact more than $100 billion.	**9-10**
Target has high historical, cultural, religious, or other symbolic importance. Loss of between 1,000 – 10,000 lives. Significant impact on sensitive subpopulations, e.g. children or elderly. National economic impact between $10 and $100 billion.	**7-8**
Target has high historical, cultural, religious, or other symbolic importance. Loss of between 100 – 1000 lives. Moderate impact on sensitive subpopulations, e.g. children or elderly. National economic impact between $1 and $10 billion.	**5-6**
Target has little historical, cultural, religious, or other symbolic importance. Loss of life less than 100. Small impact on sensitive subpopulations, e.g. children or elderly. National economic impact between $100 million and $1 billion.	**3-4**
Target has no historical, cultural, religious, or other symbolic importance. National economic impact less than $100 million	**1-2**

Figure 1. CARVER + SCHOCK MODEL[24]

[24] *US FDA/CSFAN CARVER + Schock Testomonial,* web live video, directed by USD Accessed on line at http://www.cfsan.fda.gov/~dms/vltcarv.html Accessed (November 2007).

I have revamped the CARVER + Shock model to make it relevant to an accurate analysis of cyberattacks. The elements of Accessibility and Recognizability were removed as these add little or no value in analyzing cyberattacks. In addition, it was necessary to change the criteria and scaling for the Criticality and Vulnerability portions of the model. Under Criticality, the original model looked at loss of lives and economic damage for the criteria and scaled them using data pertinent to the food industry. I have utilized the same equation as the original CARVER + Shock model (looked at nine years of data and then took the average for my median scale number) but replaced criteria data with cyber data from congressional economic reports.[25] Secondly, I have replaced the Vulnerability segment from the introduction of harmful food supply agents with security data taken from prevention and recovery documentation.[26] This information is critical to cyberattacks because the amount of security that a system has available and in place, impacts all of the other elements in the new model. Finally, the Effect element scale is based on an annual basis. To ensure numbers are not inflated, percentages have been recalculated accordingly. For example, if total restoration time for an attack is recorded as 60 days, and reports estimate and approximate percent of productivity loss,1/6 would be multiplied by the actual percent given to ensure numbers reflect an annual loss.[27]

[25] CRS Report For Congress, *The Economic Impact of Cyber-Attacks, 1 Apr 2004,* accessed via Lexis/Nexis on 1 Feb 07. *Information Security, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington, D.C., Government Accountability Office, 5-7. The information replaces original information under the Criticality segment of the Carver + Shock model. Just like in the original CARVER segment, an average was taken to accurately scale numbers from 1-10.

[26] "Detect, Deploy, and Defend Against Outside Threats," *Novell,* 2006 http://www.novell.com Accessed (July 27, 2007). Criteria from original CARVER Model: Target characteristics allow for easy introduction of sufficient agents to achieve aim. Target characteristics almost always allow for easy introduction of sufficient agents to achieve aim. Target characteristics allow 30 to 60% probability that sufficient agents can be added to achieve aim. All three of these are changed in the new model, respectively, to: No software security installed with no security procedures in place. Minimal software security installed with minimum security procedures in place. Medium software security installed with adequate security procedures in place.

[27] By changing the production loss to an annual figure gives a more realistic number for the model. For instance, if organizations lose 25% of their productivity for 60 days due to Internet performance, they are not losing the production for the whole year. This adjustment ensures the model captures the most accurate data to assess attacks.

The total cumulative points for the new CREVS (Criticality, Recovery, Effect, Vulnerability, Shock) model are 50. As in the CARVER model, 50% of the cumulative was taken to indicate a need for additional cyber security measures. Therefore, a score of 25 or higher would warrant an additional investment in cyber security. Just like the CARVER model, this number is subjective but is reasonable because the number is based on an increase in cyber vulnerabilities that would in turn cost more in system recovery. For example, at the 5-6 scoring level in the CREV model, systems affected by an attack incur more cost in time and recovery. These factors decrease system production and would therefore warrant additional cyber security for the attacked systems.

The new CREVS model (Figure 2) lends major advantages for analyzing cyberattacks. Not only are essential cyber elements presented, but this model allows them to be weighed with more accurate, documented cyberattack data. However, like all models, the CREVS model does have its shortcomings. Like the CARVER model, the CREVS model is simplistic and does not allow organizations to assign either an unknown likelihood or an unknown severity to a particular factor. For example, looking at the Shock element in the new model, the severity to subpopulations is unknown, so the impact is assumed. Nonetheless, the CARVER + Shock model is widely accepted in Federal agencies, such as the Food Safety and Inspection Service (FSIS) and the Food and Drug Administration (FDA). These agencies praise this method and recommend other agencies utilize the model to evaluate potential vulnerabilities within their respective computer systems or infrastructures.[28] Therefore, the adapted CREVS model represents the best framework available for analyzing cyber security.

[28] "Detect, Deploy, and Defend Against Outside Threats," *Novell,* 2006 http://www.novell.com Accessed (July 27, 2007). Criteria from original CARVER Model: Target characteristics allow for easy introduction of sufficient agents to achieve aim. Target characteristics almost always allow for easy introduction of sufficient agents to achieve aim. Target characteristics allow 30 to 60% probability that sufficient agents can be added to achieve aim. All three of these are changed in the new model, respectively, to: No software security installed with no security procedures in place. Minimal software security installed with minimum security procedures in place. Medium software security installed with adequate security procedures in place.

Criticality Scale
Definition: An attack is critical when the attack had significant recovery costs.

CRITERIA	SCALE
Recovery costs > $64 Billion	**9-10**
Recovery costs > $8 Billion -$64Billion	**7- 8**
Recover costs = $1 Billion – $8 Billion	**5-6**
Recovery costs = < $1 Billion	**3-4**
Recovery cost = < $ 100 Million	**1-2**

Recuperability Scale
Definition: Time it took to recover from the attack

CRITERIA	SCALE
> 1 year	**9-10**
6 months to one year	**7- 8**
> 3 – 6 months	**5-6**
1 -3 months	**3-4**
< 1 month	**1-2**

Effect Scale
Definition: System productivity damaged by the attack

CRITERIA	SCALE
> 50 of system's production was impacted	**9-10**
>25%-50 % of system's production was impacted	**7- 8**
>10%-25% of system's production was impacted	**5-6**
1%-10% of system's production was impacted	**3-4**
< 1% of system production was impacted	**1-2**

Vulnerability Scale
Definition: Level of software security installed on system/systems attacked.
Factors that Influence Security:

- Level of software security installed
- Level of enforcement of security procedures (i.e. security and password protection)

CRITERIA	SCALE
No software security installed with no security procedures in place	**9-10**
Minimal software security installed with minimum security procedures in place	**7- 8**
Medium software security installed with adequate security procedures in place	**5-6**
Medium software security installed with high level security procedures in place	**3-4**
Maximum software security installed with high level security procedures in place	**1-2**

Shock Scale

Definition: Combined measure of psychological and economic impacts of a successful attack on system/systems

Factors that Influence Shock:

- Loss of life
- Number of casualties
- Critical Infrastructure damage

CRITERIA	***SCALE***
Loss of over 10,000 lives. Major psychological impact on sensitive subpopulations, e.g., children or elderly. National economic impact > $100 billion.	**9-10**
Loss of life between 1,000 and 10,000. Significant psychological impact on sensitive subpopulations e.g., children or elderly. National economic impact between $10 and $100 Billion	**7- 8**
Loss of life between 100 and 1000. Moderate psychological impact on sensitive subpopulations e.g., children or elderly. National economic impact between $1 and $10 billion.	**5-6**
Loss of life less than 100. Small psychological impact on sensitive subpopulations e.g., children or elderly. National economic impact between $100 million and $1 billion.	**3-4**
No loss of life. National economic impact >$100 million.	**1-2**

Figure 2. CREVS MODEL

II. VULNERABILITY OF COMPUTERS AND NETWORKS TO CYBERTERRORISM

A. CODE RED AND SLAMMER WORM INTRODUCTION

The Code Red Worm was an Internet-based worm that was first reported at a university in Guangdong, China on July 17, 2001. This worm attacked numerous Web servers causing certain web pages to become inoperable. In addition, this propagating worm installed "backdoors" on the infected Web servers, making them vulnerable to hijacking by other cyber attackers who know how to exploit this type of vulnerability. The worm was particularly problematic because it spread much faster than other worms. Due to the speed and permeation of the worm, it was able to affect an estimated 250,000 systems in nine hours.[29] The reason why the worm spread so rapidly was due to its design. The Code Red worm's design was such that it could scan the Internet, identify vulnerable systems, and then infect those systems by installing itself. As each newly installed worm joined other previous installed Code Red worms, the rate of scanning increased rapidly, infecting other vulnerable systems. This was the most harmful aspect of the Code Red Worm. Not only did the worm have the ability to broadcast to the Internet information about other servers that were vulnerable to the malicious code it carried, it also left certain Web servers wide open to other attacks not related to the Code Red Worm.[30]

The Slammer Worm was the fastest computer Internet worm in history. It hit on 25 January 2003 and infected more than 90 percent of host computers within 10 minutes. The Slammer Worm "spread nearly two orders of magnitude

[29] *Information Security, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington, D.C., Government Accountability Office, 4-7.

[30]."Code Red Worm Propagation Modeling and Analysis" (November 2002) http://www-unix.ecs.umass.edu/~gong/papers/codered.pdf Accessed (September 1, 2007).

faster than Code Red."[31] As the worm spread throughout the Internet, "it doubled in size every 8.5 seconds."[32] The most harmful aspect of the Slammer Worm was the worm's capability to overload networks. Many sites lost connectivity due saturated bandwidth and there were several reports of Internet backbone disruption. This caused network outages, airline flight system failures, interference with the 2003 elections, and ATM failures. The worm also left some Web servers vulnerable to other possible attacks by different computer viruses and other diverse worms.[33]

B. IMPACT OF THE WORM ATTACKS

Table 2 illustrates the approximate speed of worm permeation, infected systems, infected servers, conveys recovery cost information, and shows the significant decrease of performance in the Internet for both worms.

Case	Speed of Worm Permeation	Infected Systems	Infected Servers	Recovery Costs	Decrease in Internet Performance
Code Red	**9 Hours**	**250,000**	**975, 000**	**$2.4 Billion**	**25%**
Slammer	**10 Minutes**	**70,000**	**N/A**	**$1 Billion**	**35%**

Table 2. Worm Analysis[34]

Together the worm attacks infected more than 300,000 systems and 975,000 servers in less than 10 hours.[35] In addition, the attacks disrupted both

[31] David Moore, "The Spread of the Sapphire/Slammer Worm," *CAIDA & USSD CSE,* 2003, http://www.caida.org/publications/papers/2003/sapphire/sapphire.html Accessed (September 1, 2007).

[32] Ibid., 2.

[33] Paul Boutin, "Slammed!," *WIRED,* July 2003, http://www.wired.com/wired/archive/11.07/slammer.html Accessed (September 1. 2007). "Robert Lemos, "Counting the cost of Slammer," *C/net News,* http://www.news.com/2100-1001-982955.html; "Inside the Slammer Worm," *Computer Society,* July/August 2003, http://computer.org/secuirty/ Accessed (September 1, 2007).

[34] *Information Security, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington, D.C., Government Accountability Office, 7-9.

government and business operations, by slowing Internet services down by more than 25% and forcing some organizations to disconnect themselves from the Internet. The estimated losses resulting from the worm attacks are $3.4 billion. These involve costs associated with cleaning infected systems and returning them to normal service, inspecting servers to determine the need for software patches, patching and testing services, and the negative impact on the productivity of system users and technical staff.[36]

The impacts of both attacks were contained by programmers spending time modeling the worms and finding their flaws. They found several programming errors by the hackers, which allowed them to design and configure a patch to eliminate the worm and repair defaced web pages the worms had compromised. The total time of patch preparation and installation on infected systems is estimated at 72 hours.[37] In addition to the patch, programmers were able to design an algorithm that when installed could make a detailed list of exact number of machines attacked and effected. This greatly facilitated the worm eradication process because programmers did not have to waste time on unaffected systems. Instead, they could look at additional vulnerabilities in the actual attacked networks and systems.[38]

[35] "Cisco Security Advisory: "Code Red" Worm – Customer Impact" (July 2001) http://www.cisco.com/warp/public/707/cisco-sa-20010720-code-red-worm.shtml Accessed (September 1, 2007). *Information Security, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington, D.C., Government Accountability Office, 9-10.

[36] Ibid., 2-5.

[37] David Moore, "The Spread of the Sapphire/Slammer Worm," *CAIDA & USSD CSE,* 2003, http://www.caida.org/publications/papers/2003/sapphire/sapphire.html Accessed (1 September 2007).

[38] "Code Red Worm Propagation Modeling and Analysis" (November 2002) http://www.cisco.com/warp/public/707/cisco-sa-20010720-code-red-worm.shtml Accessed (September 1, 2007). Cisco Security Advisory: "Code Red" Worm – Customer Impact" (July 2001) http://www.cisco.com/warp/public/707/cisco-sa-20010720-code-red-worm.shtml Accessed (September 1, 2007).

C. CREVS ANALYSIS

An analysis was conducted looking at five main factors presented in the model. Where the total score is 25 or greater, additional cyber measures should be invested in the prevention of future cyber attacks. A score of below 25 indicates that recovery costs are low enough that more security is not necessary. Tables 3 – 7 convey each individual score as it relates to the model in Figure 1.

1. Criticality Factor

This factor considers the total direct cost of recovery from the attack itself. In both cases, costs were mainly for labor. There were no reported costs in the areas of hardware or software[39]

Case	Case Data	Model Criteria and Score	Score
Code Red	**$2.4 Billion**	**Recovery costs = $1 Billion-$8 Billion**	**5**
Slammer	**$1 Billion**	**Recovery costs = $1 Billion-$8 Billion**	**5**

Table 3. CREVS Criticality Results

2. Recovery Factor

This factor considers the total restoration time it took to recover from the cyber attack.[40]

Case	Case Data	Model Criteria and Scale	Score
Code Red	**3 Months**	**1-3 months**	**3**
Slammer	**3 Months**	**1-3 months**	**3**

Table 4. CREVS Recovery Factor Results

[39] *Information Secuirty, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington D.C., Government Accountability Office, 4-5.

[40] Ibid., 2-4.

3. Effect Factor

This factor considers the percentage of productivity lost from the cyber attacks. Reports indicate the following loss in productivity:[41]

- Several federal agencies had to change the numeric Internet address that identified its Web Site to the public.
- The DOD was forced to briefly shut down its public web sites.
- The Treasury Department's Financial Management service had to disconnect from the Internet for approximately two weeks.
- Loss of Hotmail caused outages for users of Qwest's high-speed Internet services nationwide.
- Fedex had to delay package deliveries for up to 10 days.
- Networks across Asia, Europe, and the United States were effectively down.
- Bank of America customers could not withdraw funds from its 13,000 ATMs.
- Continental Airline agents had to revert to the old fashioned way of business, using phones, and pen and paper to record reservations and electronic tickets. This caused numerous flight delays and cancellations.

Reports state that all of the above productivity losses for the Code Red and Slammer worm account for 25% loss in Internet production. Since the total

[41] All Effect Factor bullets were taken from: "Cisco Security Advisory: "Code Red" Worm – Customer Impact" (July 2001) http://www.cisco.com/warp/public/707/cisco-sa-20010720-code-red-worm.shtml Accessed (September 1, 2007). *Information Security, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington, D.C., Government Accountability Office, 5.

restoration time in both cases was 3 months, this number has been refigured to meet an annual productions loss. Based on this, the total Internet production loss in both worm attacks were 6%[42]

Case	Case Data	Model Criteria and Scale	Score
Code Red	**6% of Internet production was impacted**	**1% - 10% of system's production was impacted**	**4**
Slammer	**6% of Internet production was impacted**	**1%-10% of system's production was impacted**	**4**

Table 5. CREVS Effect Factor Results

4. Vulnerability Factor

This factor measures the level of security installed on the system prior to the cyber attack. The level of software security installed and the level of enforcement are combined to formulate the actual score in this area. All systems affected by both worms had minimal software security installed with minimum security procedures in place. It was reported that on some computer systems the minimal level of spy ware and antivirus protection was installed, 60% of the employees that were operating infected systems did not properly change their passwords as outlined in their security procedures, and systems lacked the proper Intrusion Detection System (IDS) that is available for all systems.[43] These prevention methods are essential because they "harden" the system and prevent these types of attacks from occurring.[44] If an IDS is properly used and

[42] *Information Security, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington, D.C., Government Accountability Office, 5. By changing the production loss to an actual annual figure gives a more realistic number for the model. For instance, if organizations lose 25% of their productivity for 60 days due to Internet performance, they are not losing the production for the whole year. This adjustment ensures the model captures the most accurate data to assess attacks.

[43] *Information Secuirty, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington D.C., Government Accountability Office, 6. "Inside the Slammer Worm," *Computer Society,*July/August 2003, http://computer.org/security/ Accessed (September 1, 2007).

[44] Ibid., 3-5.

installed, it can catch worms with a similar design. The Slammer worm for instance, was a duplicate of a previously thwarted worm attack months earlier, but since attacked systems had no IDS installed, the worm was able to spread undetected.[45] In addition, in both worm attacks organizations failed to ensure they had a proper security model in place. The security model is absolutely necessary in dealing with cyber security because with this process, an organization, without an additional investment in cyber security, can develop a precise and unambiguous statement of cyber security policy that would facilitate in the prevention of cyber attacks. This is due to the fact that the model forms adequate policy, and conveys what security level users are authorized to access. This gives added protection to cyber security as it alleviates the number of individuals having access to sensitive files that could possible be sold to adversaries to infiltrate systems and networks.[46] Due to the above facts, a CREVS score of 7 was given in this area.[47]

Case	Case Data	Model Criteria and Scale	Score
Code Red	**Minimum software security installed with minimum security procedures in place**	**Minimum software security installed with minimum security procedures in place**	**8**
Slammer	**Minimum software security installed with minimum security procedures in place**	**Minimum software security installed with minimum security procedures in place**	**8**

Table 6. CREVS Vulnerability Factor Results

[45] Paul Boutin, "Slammed!," *Wired*, July 2003, http://www.wired.com/wired/archive/11.07/slammer.html. Accessed (1 September 2007).

[46] "Detect, Deploy, and Defend Against Outside Threats," *Novell,* 2006 http://www.novell.com Accessed (September 1, 2007).

[47] Ibid., 6.

5. Shock Factor

This factor focuses on loss of lives, the impact on subpopulations, and the National economic impact. Since no loss of lives occurred from this attack and there was no economic impact to the U.S. economy, the score in this area was 1.

Case	Case Data	Model Criteria and Scale	Score
Code Red	**No loss of life and zero Worldwide economic impact**	**No loss of life and Wordwide economic impact > $100 million**	**1**
Slammer	**No loss of life and zero Worldwide economic impact**	**No loss of life and Wordwide economic impact > $100 million**	**1**

Table 7. CREVS Shock Factor Results

D. CONCLUSION

The cumulative total for both cases using the analysis model was 21. Since this score is below the number identified in the model as an indicator to spend additional funds on cyber defense, this case, as presented, suggests that recovery is more cost effective than additional investment security for cyber defense.

How might the effects of the attacks have been different had they been undertaken by terrorists rather than hackers? The attack as presented, was performed by individuals who saw it as a “challenge” to write programmable malicious worms and introduce them into the governmental, critical infrastructure, and private information systems sectors. These individuals were not attempting to cause national economic loss or fear. They simply looked at proposed targets as a challenging game where the goal of the game was to slow down system performance while causing a huge annoyance for system administrators.

Terrorist organizations are after maximum economic damage and fear with low attack costs. Worms are very simple to create at minimal cost. Although the exact costs of the worms are unknown, some are so simplistic that they could be written within a very short amount of time. With this stated, a terrorist worm would produce the same economic loss as one produced by hackers, but could produce significantly more fear. If a terrorist organization used the same technology but announced across affected computer screens, “Al Qaeda has taken over all computer systems,” the psychological effect would be quite different from a hacker attack. In fact, this could push the Shock score to the 5-6 range, which would produce a total score higher than the 25 tipping point. Thus, this case assessment suggests that terrorists could be interested in this type of cyber attack, and the total costs of such an attack would indicate a need for improve security rather than simply recover.

However, it would be rather simple to reduce the scores for future worm attacks significantly. In both worm attacks, costs and recovery time would have been substantially lower had the proper security software been installed, had security personnel developed more in-depth procedures for thwarting attacks, and/or had the proper network tools and techniques for combating attacks been employed. These three defense tactics are already available and in most cases, are free with the purchase of necessary operating systems.[48] Although it is not apparent how the worms were introduced to computer systems or to the Internet, it is assumed that introduction was through web servers. In this method, the attacker breaks password protection on the server, gaining full access to install malicious code. In both cases, security guidance lacked the necessary content on password preparation and administration. Many passwords were not prepared to withstand possible intrusion: 40% of users’ passwords were the name of a pet, spouse, or sport.[49] These passwords can be easily discovered by

[48] “Virulent Worm Calls into Doubt Ability to Protect the Net” (July 2001) http://www.news.com/2009-1001-270471.html Accessed (September 1, 2007).

[49] Ibid., 2.

free password breaking software that is available on the Intranet or by advanced computer programmers who know how to write algorithms to crack carelessly chosen passwords. Alternatively, the worms may have been introduced through individual computer systems. In this method, the attacker looks for an unattended system, on which the user has not logged out and/or the system are not properly locked, and then installs the malicious code through the unattended system. In both worm attacks, software security that could have preempted this method of introduction were set at the minimal level, and thus failed to do so. This allows unattended systems "free reign" for potential hackers that work within a company. Setting security settings to the maximum level prevents unattended systems from being hacked into as they are locked out and can only be unlocked by the authorized user of the respective system. Finally, the worms could have been introduced by personnel with access to government, public, or private computers.[50] In this case, prevention would have fallen back on the same security software that could have limited introduction via web servers.

Thus, another lesson of the case is that existing prevention measures can substantially reduce the costs of an attack, if they are actually in place. If attacked systems were properly maintained with the firewall security and anti-virus software that was purchased with server operating systems, there would have been a minimal loss of production because the worm would have been detected and eradicated before it reached certain portions of the Internet. To correct this problem, the government should take the "high road" and establish stricter standards for maintaining cyber security. Moreover, they need to share their new standards with the private and public sector and convince these sectors that cyber security is a team effort. It would not be probable for the government to mandate stricter security standards, but it can certainly offer these sectors incentives to do so or educate them on what they would be saving on recovery

[50] "A Computing Can Of Worms" (July 2004) http://www.cbc.ca/news/background/internet/worms.html Accessed (September 1, 2007). "The Menace of Worms" (October 2007) http://www.emisissoft.com/en/kb/articles/tec050629 Accessed (September 1, 2007).

and productions costs if they were to adopt the stricter standards and use the prevention tools available. This team effort would have reduced the scores in the Code Red and Slammer worm incidents to the 1-2 level in all elements, reducing the overall score from 23 to between 5 and 10. (The exact score would depend not strictly predicable because even with the strictest standards, error can occur.)

The analysis also showed that in general, available network tools and techniques are not properly utilized. Security personnel fail to use the available hardware that scans systems for worm vulnerabilities.[51] Network administrators fail to use the available password cracking software tools to assess the password strength of assigned users, utilize effective network monitoring tools available that would identify suspicious network activity, or develop the suggested distribution lists of the most common types of vulnerabilities and their respective corrective actions. If these available tools and techniques were utilized fully, malicious worms like the Code Red and Slammer would cause much less damage, or no damage at all, and the threat of cyberterror attacks against computers and networks would be negligible.

[51] A Computing Can Of Worms" (July 2004) http://www.cbc.ca/news/background/internet/worms.html Accessed (September 1, 2007). "The Menace of Worms" (October 2007) http://www.emisissoft.com/en/kb/articles/tec050629 Accessed (September 1, 2007).

THIS PAGE INTENTIONALLY LEFT BLANK

III. VULNERABILITY OF CRITICAL INFRASTRUCTURES TO CYBERTERRORISM

A. INTRODUCTION

This chapter will assess the vulnerability of critical infrastructures to cyberterrorism, evaluate the impact this type of attack would likely have on the national economy, and consider whether existing prevention measures are adequate or increased investment in network security is required. The case examined here is simulated, since there have been no cyber attacks on critical infrastructures to date. The assessment first looks at the simulated Attack Aurora, using CREVS to assess the likely impact of an actual replication of the simulated attack. .Because those involved with the simulation concluded that it demonstrated the plausibility of a large scale attack using the same strategy, this chapter will also utilize CREVS to assess the likely impact of a larger scale version of the simulated attack. Although the data generated by the simulation, and especially the large scale attack modeled on the simulation, are less certain than in the previous case, the fact that this was a simulated terrorist attack allows us to have more confidence that the contours of the case capture those of an actual terrorist, as opposed to a mischievous, attack.

B. STAGED CYBERATTACK AURORA BACKGROUND

"The electrical power system in U.S. has more than 16,770 individual power-generating units installed in 2,880 plants, with a combined capacity exceeding 1,000 million kilowatts."[52] In September 2007, researchers from the Department of Energy's Idaho lab conducted a staged cyber attack, hacking into a replica of a single power plant's control system. Once access was achieved, attackers were able to change the operating cycle of one of the power-generating

[52] Jay Apt, M. Granger Morgan, and Lester B. Lave, "Electricity: Protecting Eseential Services," in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006), 164.

units, sending it out of control.[53] Sources familiar with the experiment concluded that the Aurora attack scenario illustrated that "very large critical pieces of equipment can be controlled with this type of attack" and that once adversaries gain control of critical components, they can make the components do whatever they want.[54]

1. Altering Attack Parameters

Since the security hardware in the electrical power systems' infrastructure is the same in every electrical plant, the biggest concern arising from the simulated attack was that individuals, groups, or cyber-terrorists using the same attack strategy could easily coordinate larger attacks that would cause widespread damage to the electric infrastructure.[55] Therefore, this chapter considers both an attack on a single plant and an attack, using the same technical expertise and strategy, on (an arbitrary) one third of the 16,770 power generating units simultaneously.[56]

C. CREVS ANALYSIS

The following results reports results for an Aurora-style attack on one and then 5534 power-generation units (one third of the 16,770 units in the U.S). Estimates are based on simulation parameters as discussed in the case study.[57] As in the previous chapter, where the total score is 25 or greater, additional cyber measures should be invested in the prevention of future cyber attacks. A score

[53] Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN,* September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

[54] Ibid.

[55] Ibid.

[56] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007).

[57] Ibid.

below 25 indicates that recovery costs are low enough that more security is not necessary. Tables 8 -12 convey each individual score as it relates to the model in Figure 2.

1. Criticality Factor

This factor considers the total amount of funds needed to recover from the attack itself. Table 8 lists the scores for both attacks. In the original simulated attack, the total recovery costs were minimal. Assumed recovery costs of an attack based on the simulated parameters of one power-generated unit would equal $100 million.[58] Costs are caused mainly by labor expenditures and machinery replacement.[59] Assumed recovery costs for 5534 power-generation units is estimated at $5.5 billion. Due to the fact that so many power-generation units are affected, costs would include not only labor expenditures and machinery replacement, but lost income to workers and investors, and losses due to food and commodity spoilage.[60]

Case	Case Data	Model Criteria and Score	Score
Aurora	**$100 Million**	**Recovery costs < $ Billion**	**3**
Altered Aurora	**$5.5 Billion**	**Recovery costs = $1 Billion-$8 Billion**	**4**

Table 8. CREVS Criticality Results

[58] Jay Apt, M. Granger Morgan, and Lester B. Lave, “Electricity: Protecting Essential Services,” in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006), 165.

[59] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007).

[60] Jay Apt, M. Granger Morgan, and Lester B. Lave, “Electricity: Protecting Eseential Services,” in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006), 175.

2. Recuperability Factor

This factor considers the time it took to recover from the cyber attack. Table 9 lists the scores for both attacks. For an attack of one power-generated unit, recovery time would be approximately one week.[61] Estimated recovery time for 5534 power-generation units is three months.[62]

Case	Case Data	Model Criteria and Scale	Score
Aurora	**One Week**	**< 1 month**	**1**
Altered Aurora	**Three months**	**1-3 months**	**5**

Table 9. CREVS Recuperability Results

3. Effect Factor

This factor considers the percentage of productivity lost as a result of the cyber attack. Since the electric power system extends to other critical national infrastructures, critical productivity would be lost in the following critical areas:[63]

- Information Technology
- Telecommunications
- Banking
- Transportation
- Emergency Services

Table 10 lists the scores for both attacks. An attack of one power-generated unit would result in no production loss.[64] An emergency generator

[61] Jay Apt, M. Granger Morgan, and Lester B. Lave, "Electricity: Protecting Eseential Services," in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006), 175.

[62] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007).

[63] 13. Michael Kormos and Thomas Bowe. "Coordinated and Uncoordinated Crisis Responses By The Electrical Industry," in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006), 162.

[64] Ibid.

would initiate and could run for 24 hours. Since only one-power generated unit is affected, services would not be affected, so additional fuel would be available to keep the generator operating until replacement of the power-generated unit (1 week). Production loss with an attack on 5534 power-generation units is estimated at 37%. Since the total restoration time is 3 months, this number has been refigured to meet an annual production loss. Based on this, total loss in production of electrical power would be 9%.[65] Taking out so many units simultaneously increases recovery time, which affects production. Also, other critical infrastructures would be affected (these losses are included in the shock factor below) making fuel harder to acquire for backup generators.[66]

Case	Case Data	Model Criteria and Scale	Score
Aurora	**0**	**< 1% of systems production in electrical power sector**	**0**
Altered Aurora	**9%**	**1%-10% production in electrical power sector**	**4**

Table 10. CREVS Effect Results

4. Vulnerability Factor

This factor focuses on the level of security installed on the system prior to the cyber attack. Table 11 lists the scores for both attacks. The level of software security installed and the level of enforcement are combined to formulate the actual score in this area. All systems affected by the simulated Aurora attack had medium software security installed with adequate security procedures in place. However, commercially available security hardware focuses on

[65] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007). Number recalculated as discussed on pg 11 of this thesis. The report indicated that 37% of electrical power production would be impacted. Based on the total restoration time of three months, the annual percentage impact would be 9%.

[66] Ibid

"traditional Internet and corporate application layer protocols," which cannot analyze or filter Supervisory Control and Data Acquisition (SCADA) packets at the level needed for increased system security.[67] ("SCADA refers to a system that collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data.")[68] Technologically advanced terrorist groups could use this vulnerability to access certain software applications and thereby gain operating system control over critical infrastructure components. This is exactly what happened in the simulated Aurora attack.[69] Because security hardware in the electrical power systems' infrastructure is the same in every electrical plant, changing the parameters of the attack does not change the CREVS score on this element.

Case	Case Data	Model Criteria and Scale	Score
Aurora	**Medium software installed with adequate security procedures in place**	**Medium software installed with adequate security procedures in place**	**5**
Altered Aurora	**Medium software installed with adequate security procedures in place**	**Medium software installed with adequate security procedures in place**	**5**

Table 11. CREVS Vulnerability Results

[67] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007).

[68] "What is SCADA?" http://www.tech-faq.com/scada.shtml Accessed (September 1, 2007)

[69] Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN,* September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.htm.

5. Shock Factor

This factor focuses on loss of lives, the impact on subpopulations, and the national economic impact. An attack on only one power-generated unit would not cause any loss of life, would have no psychological impact, and would not impact the national economy.

In contrast an attack on 5534 power-generating units would have a much greater effect. Estimated economic damage is $700 billion dollars.[70] Some experts believe economic losses could be significantly higher than this, arguing that since the electrical infrastructure affects other critical infrastructures, a broad array of services would come to a halt. The CREVS model scores any loss over $100 billion as a 10, so debates about the likely overall losses do not affect my results.

Case	Case Data	Model Criteria and Scale	Score
Aurora	**No pschological impact on sensitive subpopulations and no economic impact**	**No loss of life and no economic impact**	**0**
Altered Aurora	**Major psychological impact on sensitive subpopulations. $700 Billion in national economic damage**	**Major psychological impact on sensitive subpopulations. National economic impact > $100 Billion**	**10**

Table 12. CREVS Shock Results

[70] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007).

D. CONCLUSION

The total CREVS score for the Aurora case with one power-generated unit successfully attacked is 9. Since this score is far below the number identified in the model as an indicator to spend additional funds on cyber defense, this simulated case suggests that recovery is sufficient, and no additional investment for cyber defense is needed. However, for Altered Aurora case with 5535 power-generated units being affected simultaneously the CREVS score to 28. Since this number is above the tipping point of 25, this suggests that additional investment for cyber defense is in fact needed in securing the electrical critical infrastructure against cyber attacks.

The Altered Aurora analysis suggests that the potential damage from a cyber attack on the electrical critical infrastructure is sufficiently large to make it appealing for terrorists to invest in this type of attack.[71] Today's terrorist leaders know that the main benefit of attacks on critical infrastructures is not the immediate damage they inflict, but the erosion of public confidence and impact on the national economy. The loss of public confidence in critical infrastructures could cause panic, instilling fear that could cause citizens to lose trust in systems that are used to manage daily transactions. For instance, an attack of the Altered Aurora magnitude would likely cause individuals to doubt the security of commercial applications that are used in personal banking and on-line sales, exacerbating the impact of the attack. Al Qaeda spent $500,000 on the September 11 attacks, while the U.S. spent $500 billion to recover.[72] For every dollar Al Qaeda spent to attack, the U.S. spent $1 million to recover.[73] The

[71] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007).

[72] 3. Stephen E. Flynn. "The Brittle Superpower" in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006), 4-6.

[73] Ibid., 4-7.

Altered Aurora attack would cost terrorists an estimated $5 million to engineer,[74] and would produce a recovery price tag of $700 billion.[75] While almost an order of magnitude lower than the return on 9/11, this is still a more than adequate return on the investment.

Therefore, additional security is necessary. Although there has not been a cyber attack to date, the Aurora simulation shows that the electrical critical infrastructure is vulnerable, and existing security measures are insufficient to prevent massive economic, and probably psychological, damage.[76] Although the nation's electrical infrastructure is resilient, it is dependent upon other critical infrastructures, which are more vulnerable. Information services in particular are crucial in the performance of the electrical infrastructure.[77] "[V]irtually all of the command-and-control systems used by operators to manage the electrical grid depend on computer systems and networks."[78] In turn, these systems depend upon software applications to run accurately and effectively. In the past, these applications were designed in a highly customized standalone manner. However, budget constraints have led infrastructure managers to shift from a reliance on propriety control systems to the use of "open" systems and industry standard protocols.[79] In fact, many of the open source systems are manufactured overseas.[80] This adds to the vulnerability of critical infrastructures

[74] *Staged cyber attack reveals vulnerability in power grid,* web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007).

[75] Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN,* September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

[76] Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN,* September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

[77] 3. Stephen E. Flynn. "The Brittle Superpower" in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006), 135.

[78] 2. National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks,* prepared by National Infrastructure Security Co-ordination Centre, http://www.cpni.gov.uk/docs/re-20050223-00157.pdf.

[79] Ibid.

[80] Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN,* September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

like electricity as personnel at the overseas locations have access to control system schematics and the programmable source code that manages system capability and performance.[81] If terrorist groups purchased valuable schematic and source application code, they would have full access to control power sources as the simulated Aurora attack did; thus, a real attack of this nature is possible.[82]

The Altered Aurora scenario suggests the need for investments in improved system security specifically. Although information systems had adequate security software installed in the Aurora simulation, they lacked the security hardware (i.e., firewalls, routers, switches) necessary to thwart the attack.[83] As in the worm cases, security processes lacked the necessary guidance on attack prevention and recovery.[84] System security checklists in some instances were outdated, or simply were not prepared.[85]

To significantly reduce all of the above vulnerabilities to cyber terror attacks, the U.S. would need to invest only several million dollars in the development of new security hardware and advanced security.[86] In the hardware area, new security hardware has to be configured and installed to give additional intrusion detection to information systems that control critical infrastructures. This new security hardware would communicate over a secure channel that would give additional protection to operating systems that control

[81] Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN,* September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

[82] Ibid.

[83] 2. National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks,* prepared by National Infrastructure Security Co-ordination Centre, http://www.cpni.gov.uk/docs/re-20050223-00157.pdf.

[84] Ibid.

[85] Ibid.

[86] 2. National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks,* prepared by National Infrastructure Security Co-ordination Centre, http://www.cpni.gov.uk/docs/re-20050223-00157.pdf.

crucial infrastructures.[87] In regards to advanced security procedures, security checklists need to be revised and in some cases created to reflect the most current procedures to prevent and recover from cyber attacks.88 These investments would offer again offer a significant second layer of defense, protecting critical devices from an external or internal attack.

[87] 2. National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks,* prepared by National Infrastructure Security Co-ordination Centre, http://www.cpni.gov.uk/docs/re-20050223-00157.pdf.

[88] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

This thesis uses a case analysis approach to determine whether the current level of cybersecurity is sufficient or new investments in security are needed, in relation to computers, networks, and/or critical infrastructures.

A. LESSONS LEARNED FROM CODE RED AND SLAMMER WORM

The cases studied lend some credence to critics who argue that it is not necessary to secure all of cyberspace. In these attacks enough prevention was established to limit the attacks and facilitate robust recovery without securing the ephemeral space of the Internet. However, the score on the CREVS model was just below the tipping point of 25 for mischievous attacks on computers and networks, and it is possible that the additional shock associated with a similar attack by a terrorist organization would raise the score above the tipping point. However, the analysis also suggests that additional investments in computer and/or network security would still be unnecessary if organizations employed security tools, methods, and solutions that already are in place, and were vigilance in implementing existing security procedures.

This finding indicates that organizations need to go further in implementing the National Strategy to Secure Cyperspace, which outlines the importance of reducing vulnerabilities of cyber attacks and minimizing damage and recovery times. Improved cyber security awareness would go a long way toward preventing cyber attacks. A study conducted by the Network Reliability and Interoperability Council affirms this conclusion, that organizations that follow appropriate available security measures (i.e. appropriate level of spy ware, IDS, and antivirus protection software installed) are unaffected by worm attacks.[89]

[89] “NRIC Best Practices for ISP Security” (August 2004) http://www.cbc.ca/news/background/internet/worms.html Accessed (November 1, 2007).

B. LESSONS LEARNED FROM ATTACK AURORA

Unlike the worm attacks, the Altered Aurora analysis shows that when it comes to cyber protection, the electrical critical infrastructure is in need of additional investment. Although there has not been an attack to date, the simulation indicates that these infrastructures are vulnerable, which suggests that in this area criticisms of government efforts to increase cyber security need to be re-accessed. The Aurora simulation suggests the strategy and technical expertise are available for this type of cyber attack, and could easily be utilized to attack thousands of power facilities simultaneously, potentially leading to a cascade of effects across the national economy. In addition, the electrical generation infrastructure is dependent upon other critical infrastructures. Information services, for example, are crucial in the performance of the electrical infrastructure. These systems depend upon software applications to run accurately and effectively. Because of budgetary constraints, program managers have shifted from more customized and secure stand alone methodology to utilizing open systems and standard protocols. The fact that many of these open systems are manufactured overseas, compounds the problem, making the current status of current critical infrastructures susceptible to cyber attack.

Overall the conclusions of this analysis fall between those of the government and its critics. The government is right that cyber security needs to be improved, while the critics are right that it is not necessary to secure all of cyberspace. The analysis here shows that it is feasible to improve cyber security with simple, cheap methods, tools, and procedures. This suggests that the government does not need a strategy that is all encompassing, but a strategy that encourages the private and public sectors to be vigilant about cyber security.

Finally, assuming that terrorist make decisions based on a cost-benefit analysis, the Aurora study suggests that this type of attack is quite appealing for today’s terrorists: it is inexpensive to carry out and could have very significant economic and psychological effects.

C. CONCLUSION

While the solution to improving cyber security appears to be both simple and inexpensive, implementing it will require significant public-private cooperation. Such cooperation might be achieved through the formation of a joint “Federal Cybersecurity Reserve System,” as suggested by Stephen Flynn in his book Beyond Fear.[90] Flynn’s solution to managing the cumbersome Department of Homeland Security is to organize it along the lines of the Federal Reserve System, making it into a “Federal Security Reserve System.” In the area of cybersecurity, a “Federal Cybersecurity Prevention and Protection System” could address the specific vulnerabilities identified in this thesis, ensuring that security measures are discussed in an open forum between the government, private, and public sectors. Such a bold effort would support improved communication between the government, public, and private sectors. This in turn would facilitate public and private investments in cyber security needed to secure the nation’s critical structures.

[90] Stephen Flynn. *America the Vulnerable* (New York, HarperCollins Publisher, 2003, 65.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"A Computing Can Of Worms" (July 2004) http://www.cbc.ca/news/background/internet/worms.html accessed 1 September 2007

Adams, James. "Virtual Defense." Foreign Affairs (2001) 98-112

Advanced Network Defense Research. Santa Monica, CA: RAND, 2000.*Air Force Doctrine Document (AFDD) 2-5: Information Operations*. Jan 11, 2005. Washington, DC: Air Force Publishing, 2005. http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5/afdd2-5.pdf. accessed February 6, 2007.

AFI 33-202: Network and Computer Security. February 3, 2006. Washington, DC: Air Force Publishing, 2006. http://www.e-publishing.af.mil/pubfiles/af/33/afi33-202v1/afi33-202v1.pdf. accessed February 6, 2007.

Air Force Instruction (AFI) 33-115 Volume 1: Network Operations (NetOps). May 24, 2006. Washington, DC: Air Force Publishing, 2006. http://www.e-publishing.af.mil/pubfiles/af/33/afi33-115v1/afi33-115v1.pdf. accessed February 6, 2007.

Anderson, Robert H.; Phillip M. Feldman; Scott Gerwehr; Brian Houghton; Richard Mesic; John Pinder; Jeff Rothenberg; and James Chiesa. *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*. Santa Monica, CA: RAND, 2003. http://www.rand.org/pubs/monograph_reports/MR993/. accessed February 20, 2007.

Apt, Jay. M. Granger Morgan, and Lester B. Lave, "Electricity: Protecting Essential Services," in *Seeds of Disaster, Roots of Repsonse* ed. New York, NY:Cambridge University Press, 2006

Boutin, Paul, "Slammed!," *Wired*, July 2003, http://www.wired.com/wired/archive/11.07/slammer.html. accessed February 20, 2007

Chairman of the Joint Chiefs of Staff (CJCS) Instruction (CJCSI) 3401.03: Information Assurance (IA) and Computer Network Defense (CND). July 15, 2003. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2003. http://www.dtic.mil/cjcs_directives/cdata/unlimit/3401_03.pdf. accessed February 16, 2007.

Cisco Security Advisory: “Code Red” Worm – Customer Impact” July 2001 http://www.cisco.com/warp/public/707/cisco-sa-20010720-code-red-worm.shtml accessed 1 September 2007.

CJCS Manual (CJCSM) 6510.01: Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND). Mar 25, 2003 (with changes 1-3 dated through Mar 8, 2006). Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2003. http://www.dtic.mil/cjcs_directives/cjcs/manuals.htm. accessed February 20, 2007.

CJCSI 6510.01 Series: Information Assurance (IA) and Computer Network Defense (CND). Jun 15, 2004. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2004. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf. accessed February 20, 2007.

“Code Red Worm Propagation Modeling and Analysis” (November 2002) http://www.cisco.com/warp/public/707/cisco-sa-20010720-code-red-worm.shtml accessed 1 September 2007

“Critical Infrastructure Protection,” January 2003,www.whitehouse.gov/news/releases/2001/10/20011016, accessed 7 February 2007

CRS Report For Congress, *The Economic Impact of Cyber-Attacks,* 1 Apr 2004, accessed via Lexis/Nexis on 1 Feb 07; *Information Security, testimony of Mr Keith A. Rhodes,* Report number GAO-01-1073T, Washington, D.C., Government Accountability Office.

“Cyber Security: A Crisis of Prioritization,” February 2005, www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf, accessed 7 February 2007

“Cyberstrategy 2.0,” Spring 2006 http://www.securityaffairs.org/issues/2006/10/cilluggo_nicholas.php, accessed 5 December 2006

Denning, Dorothy “Cyberterrorism,” *Global Dialogue*, August 24, 2000, 1, http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc, accessed 7 September 2007.

“Detect, Deploy, and Defend Against Outside Threats,” *Novell,* 2006 http://www.novell.com accessed 1 June 2007

“Federal Bureau of Investigation, Congressional Testimony,” http:///www.fbi.gov/congress/congress02/nipc072402.htm,accessed 7 February 2007

Flynn, Stephen. “The Brittle Superpower” in *Seeds of Disaster, Roots of Repsonse* (New York, NY:Cambridge University Press, 2006)

Hoffman Bruce, *Inside Terrorism. NY:* Columbia University Press, 1998.

“How to Effectively use the CARVER+Shock Method of Assessing Risk and Vulnerabilities” (April 2006) http://www.afdo.org/afdo/Conferences/upload/060617-0815-1-Rigby-AFDO%20CARVER%20training.pdf accessed 29 July 2007.

Howard Russell and Forest James. *Homeland Security and Terrorism* New York, NY: Mcgraw-Hill, 2006

Information Secuirty, testimony of Mr Keith A. Rhodes, Report number GAO-01-1073T, Washington D.C., Government Accountability Office

“Information Warfare,” http://www.fas.org/irp/eprint/snyder/infowarfare.htm, accessed 5 December 2006

“Inside the Slammer Worm,” *Computer Society,*July/August 2003, http://computer.org/security accessed 15 July 2007

Kormos. Michael, and Bowe Thomas. *Coordinated and Uncoordinated Crisis Responses By The Electrical Industry,* in *Seeds of Disaster, Roots of Repsonse* ed. New York, NY:Cambridge University Press, 2006

Krebs, Brian “A Cybersecurity Role for Uncle Sam?” (April 2004) http://www.stanford.edu/class/msande91si/www-spr04/readings/week2/washpost.html accessed 15 July 2007

Meserve, Jeanne “Sources: Staged cyber attack reveals vulnerability in power grid,” *CNN* 26 September, 2007http://www.cnn.com/2007/US/09/26/power.at.risk/index.html accessed 1 September 2007

Moore, David. “The Spread of the Sapphire/Slammer Worm,” *CAIDA & USSD CSE,* 2003, http://www.caida.org/publications/papers/2003/sapphire/sapphire.html accessed 1 September 2007.

National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks,* prepared by National Infrastructure Security Co-ordination Centre, http://www.cpni.gov.uk/docs/re-20050223-00157.pdf accessed 15 July 2007.

NRIC Best Practices for ISP Security" August 2004 http://www.cbc.ca/news/background/internet/worms.html accessed 1 November 2007.

O'Neil, Michael "Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry," *Depaul Business Law Journal Vol 12, 97*, 1999/2000, http://www.cdt.org/publications/lawreview/2000depaul.shtml accessed 1 September 2007

Report to Congressional Requestors on Internet Infrastructure, GAO-06-672, Washington, D.C., Government Accountability Office, 2006.

Russell, Howard, *Homeland Security and Terrorism*. New York, Mcgraw-Hill Companies, 2006.

Simmer, Michael. "The Tensions of Securing Cyberspace: The Internet, state power and the National Strategy to Secure Cyberspace" March 2004 http://www.firstmonday.org/issues/issue9_3/zimmer/index.html accessed 1 July 2007

"Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructures," February 2004. http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html, accessed 7 February 2007.

Staged cyber attack reveals vulnerability in power grid, web live video, directed by CNN Accessed on line at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (September 2007)

"The Menace of Worms" (October 2007) http://www.emisissoft.com/en/kb/articles/tec050629 accessed 1 September 2007

"The National Strategy to Secure Cyperspace," February 2003, http://www.whitehouse.gov/pcipbl, Last accessed 5 December 2006.

"The Tensions of Securing Cyberspace: The Internet, State Power and The National Strategy to Secure Cyberspace," January 2004, http://www.firstmonday.dk/issues/issues9_3/zimmer, accessed 1 June 2007

U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, *Cybersecurity Protection, testimony of Mr. George S. Forseman, 13 September 2006,* accessed via Lexis/Nexis on 16 Nov 2006.

U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, *Cybersecurity Protection, Testimony of Mr. Vincent Weafer, 13 September 2006,* accessed via Lexis/Nexis on 16 November 2006.

US FDA/CSFAN CARVER + Schock Testomonial, web live video, directed by November 2007 USD Accessed on line at http://www.cfsan.fda.gov/~dms/vltcarv.html accessed 1 August 2007

"Virulent Worm Calls into Doubt Ability to Protect the Net," July 2001 http://www.news.com/2009-1001-270471.html accessed 1 September 2007 accessed 1 August 2007

Weimann, Gabriel. *Cyberterrorism: The Sum of All Fears?* London, Taylor and Francis, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California