NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COMMUNICATION BREAKDOWN: DHS OPERATIONS DURING A CYBER ATTACK

by

Larry M. Corzine

December 2010

Thesis Co-Advisors: Dorothy Denning
Eric J. Dahl

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 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Communication Breakdown: DHS Operations During a Cyber Attack		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Larry M. Corzine			
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 United States Government. IRB Protocol number _____N.A._____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The Department of Homeland Security (DHS) leverages information technology to increase the effectiveness of first responders during disaster recovery. At the same time, cyber attacks against these information technologies have significantly increased. Unfortunately, cyber attacks have grown faster than the technologies used to defend them. The reliance on technology coupled with the difficulty of defending it makes it unrealistic to assume that communications will always be available when needed. Therefore, it is critical that first responders are prepared to operate when one or some of their communications abilities are lost.

Alarmingly, DHS has the responsibility to prepare first responders to operate during disasters; however, they lack the authority to enforce programs to ensure this happens. This lack of authority affects how first responders communicate and provides gaps in DHS efforts to prepare for disasters. Until DHS has the authority to enforce change across all levels of government, communications will not be guaranteed during disaster recovery operations. However, DHS could leverage communication outages during operational exercises to better prepare first responders. This thesis explores DHS exercises on the federal, state and local levels and how they are preparing first responders to operate through cyber attacks.

14. SUBJECT TERMS CERTS, DHS, ENISA, FEMA, P25, NLE, TOPOFF, Critical Infrastructure, Cyber Attack, First Responders, Department of Homeland Security, Disaster Recovery, Emergency Support Function, European Network and Information Security Agency, Federal Emergency Management Agency, Homeland Security Presidential Directive, Malware, National Exercise, Quadrennial Homeland Security Review, Trusted Internet Connections, Zero-Day Exploits			**15. NUMBER OF PAGES** 93 **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

COMMUNICATION BREAKDOWN:
DHS OPERATIONS DURING A CYBER ATTACK

Larry M. Corzine
Major, United States Air Force
B.S., Wayland Baptist University, 1995
M.B.A., Bellevue University, 2002

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 2010

Author: Larry M. Corzine

Approved by: Dorothy Denning
Thesis Co-Advisor

Eric J. Dahl
Thesis Co-Advisor

Harold Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Homeland Security (DHS) leverages information technology to increase the effectiveness of first responders during disaster recovery. At the same time, cyber attacks against these information technologies have significantly increased. Unfortunately, cyber attacks have grown faster than the technologies used to defend them. The reliance on technology coupled with the difficulty of defending it makes it unrealistic to assume that communications will always be available when needed. Therefore, it is critical that first responders are prepared to operate when one or some of their communications abilities are lost.

Alarmingly, DHS has the responsibility to prepare first responders to operate during disasters; however, they lack the authority to enforce programs to ensure this happens. This lack of authority affects how first responders communicate and provides gaps in DHS efforts to prepare for disasters. Until DHS has the authority to enforce change across all levels of government, communications will not be guaranteed during disaster recovery operations. However, DHS could leverage communication outages during operational exercises to better prepare first responders. This thesis explores DHS exercises on the federal, state and local levels and how they are preparing first responders to operate through cyber attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEMS AND HYPOTHESES....2
B. DHS DISASTER PREPARDNESS....6
C. METHODS AND SOURCES....7

II. CYBER ATTACK....9
A. INTRODUCTION....9
B. CYBER ATTACK TOOLS....9
C. VIRUSES AND WORMS....11
D. ESPIONAGE....13
1. Moonlight Maze....14
2. Titan Rain....15
3. Operation Aurora....15
E. TARGETED ATTACKS....16
1. Israel Attacks Syria....16
2. Stuxnet Worm....18
F. FUTURE SCENARIO....19
1. Phase I....20
2. Phase II....22
3. Phase III....23
4. Phase IV....25
5. Phase V....27
G. CONCLUSION....27

III. PREVENT, PROTECT, RESPOND, AND RECOVERY AGAINST CYBER ATTACKS....29
A. INTRODUCTION....29
B. PREVENT....30
C. PROTECT....34
D. RESPOND....39
E. RECOVERY....40
F. CONCLUSION....43

IV. NATIONAL EXCERCISE PROGRAM FOR FIRST RESPONDERS....45
A. INTRODUCTION....45
B. TIER IV....46
C. TIER III....48
D. TIER II....51
E. TIER I....52
F. RADIO INTEROPERABILITY....54
G. CONCLUSION....58

V. CONCLUSION....61
A. SUMMARY....61

BIBLIOGRAPHY **63**
INITIAL DISTRIBUTION LIST **75**

LIST OF FIGURES

Figure 1. Cyber Attack Phases 20
Figure 2. First Responder Radio Network Example 57

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. National Exercise Plan (NEP) Communication Findings.....60

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CERTS	Computer Emergency Response Teams
CIKR	Critical Infrastructure and Key Resources
Comm-out	Communication Outage
DHS	Department of Homeland Security
DoD	Department of Defense
ENISA	European Network and Information Security Agency
ESF	Emergency Support Function
EU	European Union
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
HAZMAT	Hazardous Material
HSPD 8	Homeland Security Presidential Directive 8
IDS	Intrusion Detection System
IG	Inspector General
IP	Internet Protocol
MHz	Megahertz
NEP	National Exercise Plan
NIST	National Institute of Standards and Technology
NPD	National Preparedness Directorate
NSA	National Security Agency
NSC	National Security Council
P25	Project 25
PLE	Principle Level Exercise
QHSR	Quadrennial Homeland Security Review
SONS	Spill of National Significance Exercise
TIC	Trusted Internet Connections
TOPOFF	Top Officials Exercise
USSTRATCOM	United States Strategic Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my wife, for her love, support and understanding

Theresa J. Corzine

To my co-advisors, for their guidance, mentoring, patience, and pragmatism

Professor Dorothy Denning (Defense Analysis Department)
Professor Eric J. Dahl (National Security Affairs Department)

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Department of Homeland Security (DHS) leverages and directs the resources of federal, state, and local governments to protect the American people in their homeland. This is a massive undertaking and covers more than 87,000 different jurisdictions across the United States.[1] DHS prepares for man-made and natural disasters by conducting scenario- based exercises across federal, state, and local governments and more recently has added in nongovernmental participants. First responders conduct exercises at all levels of government in accordance with the National Exercise Plan (NEP). The NEP is designed to take the lessons learned at the state and local government-level exercises and then roll them up to the larger national-level exercises. What is common in these first responder exercises is the fact that cyber and physical have been kept split into separate exercises. This has not allowed the first responders on the front lines to understand how to operate when the communications they are using are attacked or simply go down for periods of time. This thesis explores DHS exercises on the federal, state and local levels, and how they are preparing first responders to operate through communication outages.

An examination of these exercises suggests areas where DHS operations could be strengthened. DHS first responder operational exercises have assumed all communication systems will be operating at 100-percent capability and will be available for all disasters. Ardent Sentry, a large-scale first responder operational exercise, was even cancelled early in 2006 because basic communications could not be brought on-line. DHS's Cyber Storm exercise is specifically designed to test how critical infrastructures can operate while under cyber attack. However, even that exercise fails to take into account the potential for attacks against DHS's own communications networks. The 2008 Cyber Storm final report points out the interdependency of the physical and cyber saying, "Cyber events have consequences outside the cyber response community, and

[1] Kay Bailey Hutchison, "Kay Bayley Hutchison United States Senator," http://hutchison.senate.gov/govsites.html, (accessed 23 May 2010). Senator Hutchinson's website provides links and discriptions of federal agencies. Her site pulls this data from other federal websites.

non-cyber events can impact cyber functionality."[2] This presents a gap in how first responders prepare for an emergency or disaster recovery operation. By not testing the effects of attacks against its own first responder communications systems, DHS is not preparing the nation's first responders to operate through a communications outage.

DHS could better prepare by using the lessons learned in cyber and operational functional exercises, and using them in cross functional exercises combining cyber and physical scenarios. By doing this, DHS could introduce "communication systems outages" during portions of the exercise. This would allow DHS to see the effects of a cyber attack on a physical operation and provide training for the first responders to operate through communication outages. DHS is preparing for events similar to this now; however, they are missing the simple fact that the preparation needs to combine both physical and cyber scenarios to provide the best training and ensure first responders are prepared to operate without all communications available.

A. PROBLEMS AND HYPOTHESES

During disaster recovery operations, DHS and first responders communicate across multiple types of communication systems. Communicating across multiple systems strengthens the possibility that critical information will reach the agencies when needed. Even with multiple systems, there are challenges when communicating across government and nongovernment agencies. Different agencies deploy different communication systems and software that are not always compatible with other agencies in a disaster recovery operation.[3] This makes it difficult to compare what a cyber attack could present to the different agencies. Some agencies will have multiple communication lines that an attacker will have to bring down to slow the operation, while others will have a single point of failure. This is relevant to DHS operating through a cyber attack

[2] Department of Homeland Security, "Cyber Storm II Final Report," July 2009, http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf, (accessed 10 April 2010), 3.

[3] Currently, radio frequencies between first responders are not compatible and first responders have to carry multiple radios in order to communicate. When commercial phones are taken out in a disaster the systems that DHS deploys cannot legally hook up to commercial cell phones. Currently, DHS first responders hand out cell phones that work on their system; however, the number available is limited and distribution takes time—and time is one of the factors that determine the success of the operation.

because it reduces the number of systems first responders can use in a disaster recovery effort. Limiting the number of systems used, by first responders, provides a more specific target for a cyber attack and amplifies the effects an attack can have on an operation. One of the best ways to operate through a cyber attack is for agencies to have the ability to communicate across multiple systems.

Across government and nongovernment agencies, communication is crucial before and during homeland defense operations; it affects the speed at which the recovery takes place and the overall outcome of the operation. However, if DHS's communications systems are taken down by an adversary, then the department's reliance on complex computer systems to communicate across government and nongovernment agencies will become a choke point that can tremendously affect the success of a disaster recovery operation. My research indicates that DHS is not planning sufficiently for a cyber attack scenario that could take out communications needed for first responder operations. There are several reasons why this is being overlooked at the present time. There is a lack of technical communications systems experts at all levels of government, positions are going unfilled, DHS is responsible for areas they do not own, and DHS lacks the authority to enforce any changes.

Based on the lack of authority to enforce follow up actions, it appears DHS has not explored what losing communications during an attack would do to its disaster recovery response. This raises the question of the effects of losing communications would have on a homeland security operation. Currently, there are no numbers or statistics that provide expectations of how specific communications outages would affect a disaster recovery effort. I am not suggesting that all communications systems are likely to be disrupted at one time for an extended period. I am advocating that specific systems used to communicate during DHS disaster recovery operations could be the target of an adversary, and that if brought down, would significantly slow recovery operations.

Government agencies have repeatedly demonstrated that communications between agencies and within agencies are crucial before and during homeland defense operations. Both the Australian Government's Security and Critical Infrastructure

Division and the United States Department of Homeland Security have echoed how critical communication is before and during a major homeland defense operation.[4] Reliance on automated computer systems to conduct daily operations within the United States is growing at a fast pace within agencies at all levels. This rapid growth is alarming the experts in two ways. First, defense of these networks has not kept up with the growth of the networks. Second, there have been poor communications across government agencies due to lack of shared information and interoperability problems between the automated systems.[5] At the same time, some experts believe that since the Internet was created as an "open platform," any system attached to the Internet can be accessed by anyone, from anywhere, and at anytime.

With the rise of Internet attack tools and the ease of availability, other states, non-state actors, terrorist groups, and even individuals can attack networks. The CIA released a report, "Preserving National Security in an Increasingly Borderless World," which discusses how United States adversaries will use cyber attacks such as denial-of-service attacks to inflict "Weapons of Mass Effect (WME)" against the United States.[6] Historically, most United States government agencies have not placed defense of their communications systems as a top priority. It was not until the United States began seeing other nation-state agencies infiltrating their automated communications systems that the priority began to change.

The United States government put cyber modernization on the back burner until recently when they identified the exploitation and defense of automated communications systems as being the battlefield of the future. Clarke and Knake identify several studies that have been conducted that point out the growing threat of cyber attacks on the United States:

---

[4] Australian Attorney General, "Cyber Storm II final report and Findings," August 2008, pp. 13–18. See also United States Department of Homeland Security, "Cyber Storm II Final Report," July 2009, 3.

[5] Peter Buxbaum, "Air Force Explores the Next Frontier," 17 Febuary 2007, http://gcn.com/articles/2007/02/17/air-force-explores-the-next-frontier.aspx, (accessed 23 May 2010).

[6] Lawrence K. Gershwin, "Statement for the Record: Cyber Threat Trends," 21 June 2001, https://www.cia.gov/news-information/speeches-testimony/2001/gershwin_speech_06222001.html, (accessed 9 June 2010).

> Part of the reason we are so unprepared today is "the boy who cried wolf too soon" phenomenon. Sometimes the boy who cries wolf can see the wolf coming from a lot farther away than everyone else. The Joint Security Commission of 1994, the Marsh Commission of 1997, the Center for Strategic and International Studies commission of 2008, the National Academy of Science commission of 2009, and many more in between have all spoken of a major cyber security or cyber war risk.[7]

Military professionals have used the slogan, "To kill people and break things," as the purpose of war, when in fact, the purpose of war is to modify your opponent's behavior and inflict your will upon him.[8] This type of thinking is not new to warfare and was pointed out 2,500 years ago when Sun Tzu pronounced, "Supreme excellence consists of breaking the enemy's resistance without fighting."[9] During the 1990s and through the early 2000s, there was debate among United States government policy makers on how to classify government automated communications systems.[10] During that time, many policy makers only viewed automated communications systems as enablers for physical operations.[11] This is interesting since historically signal intercept operations have been used in defensive efforts. The Western alliance used message interceptions to understand German and Japanese actions and took counter actions based on this information to defeat them in WWII. Further, the Israeli government destroyed a Syrian facility thought to be related to weapons of mass destruction. What is interesting about this attack is how the Syrian air defense system never reacted to the Israeli fighter jets entering their air space. The Israelis had hacked into the Syrian system and what appeared on the Syrians' screen was what the Israelis had put there that night: a virtual

---

[7] Richard Clarke and Rob Knake, *Cyber War The Next Threat to National Security and What To Do About It*, New York: Harper Collins, 2010, 135.

[8] Douglas H. Dearth, "Rethinking the Application of Power in the 21st Century," n.d., http://www.fas.org/irp/agency/army/mipb/1997-1/dearth.htm, (accessed 30 May 2010).

[9] Alan Campen, Douglas H. Dearth, and R. Thomas Gooden, *Cyber war Security, Stategy and Conflict in the Information Age*, Fairfax Virginia: AFCEA International Press, May 1996, 251.

[10] Classify from a perspective of a center of gravity for war and a weapon system. This becomes more evident when the United States Air Force changed the tier and structure of all its communications career fields in May 2010. They are now considered Cyber Operators vs. Communications Managers.

[11] United States Department of Defense, "Information Operations Roadmap," 30 October 2003, 2.

clear sky.[12] These are just two examples, but they clearly show that adversaries are willing to exploit communication systems to defeat an enemy, and will be discussed in later chapters.

B. DHS DISASTER PREPARDNESS

In response to 9/11, the United States created DHS, and since then the Department of Defense has added two major commands that defend United States automated communications systems. In 2002, the Department of Defense activated the United States Northern Command (USNORTHCOM), and in 2009, the United States Cyber Command (US Cyber Command) was created.

The focus of these agencies has been to prevent adversaries from getting into automated communications systems, to ensure interoperability across agencies, and to assist in recovery of the systems, once they fail. If United States automated systems were deliberately attacked by an adversary during a disaster recovery effort what effects would this have on their success? Would first responders simply be "neutralized" as Campen pointed out back in 1996?[13]

In the last Cyber Storm exercise, there were eight major findings by DHS and all revolved around failures in communications.[14] This should highlight to DHS that there is a growing concern that all communication systems might not be available or work properly during a disaster recovery effort if attacked by an adversary. There have also been exercises for first responder operations that have assumed they will have all automated systems, at all times, running at full capacity. From lessons learned at Ardent Sentry and Cyber Storm, it is not likely this will be the case in a real-world event. With the increasing threat of cyber attacks, this thesis argues that DHS needs to be prepared to operate without full communications capability.

---

[12] Richard Clarke and Rob Knake, *Cyber War The Next Threat to National Security and What To Do About It*, New York: Harper Collins, 2010, 1–5.

[13] Douglas H. Dearth, "Rethinking the Application of Power in the 21st Century," n.d., http://www.fas.org/irp/agency/army/mipb/1997-1/dearth.htm, (accessed 30 May 2010).

[14] Department of Homeland Security, "Cyber Storm II Final Report," July 2009, http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf, (accessed 10 April 2010), 3.

DHS exercises that build scenarios on the effects of operations if specific communications systems were down or not operating for periods of time during a real-world disaster response, will help first responders prepare for future disaster operations. At a meeting in July 2009, Air Force General Arthur Lichte, Commander of Air Mobility Command (AMC), echoed this concern, by inquiring how AMC could move people and cargo if their communications systems were under attack.[15] The concern of operating through a cyber attack is being voiced; however, the preparation for operating through an attack is not being done.

Historically, government agencies conducted communication systems outage or "comm-out" exercises, where they tested how to operate in the event that electronic communications systems were lost. Yet, despite the growing reliance on electronic communications, "comm-out" exercises have disappeared. This thesis explores why "comm-out" exercises are not being used to prepare first responders and argues that they should be included in the general exercises.

C. METHODS AND SOURCES

The thesis used reports available through open sources, including reports of lessons learned, Inspector General reports, and United States Government of Accountability (GAO) reports. Further, the research compared how the European Union is preparing their first responders versus the United States in the event of a cyber attack. DHS was unable to provide any information during this research; therefore, all the information included in this thesis was obtained through open source documents posted on the Internet. The nature of this research does expose first responder vulnerabilities to cyber attacks during a disaster recovery effort; however, these vulnerabilities are available to anyone with Internet access. DHS could use this research to synergize their exercises and become better prepared to operate through a major cyber attack.

[15] Air Mobility Command (AMC) is responsible for getting supplies, troops and weapons to the physical domain of war. AMC flies 900 sorties per day and a plane takes off every 90 seconds. This is how the U.S. is able to react to and sustain large-scale operations. This effort is controlled by about 100 personnel on duty at any given time across the globe and relies heavily on automated communications systems to make it happen.

Chapter II will focus on the growing threat of cyber attacks. It outlines what attack tools are being used in cyber space, how these tools emerged, and how current defenses are not stopping the attacks. Further, it highlights how nations are willing to use cyber attacks in conjunction with physical attacks. In addition, this chapter will point out that cyber attacks have the ability to be targeted. Last, it will outline what a future cyber attack on critical infrastructure could look like, and the fact that the tools are available today to conduct such an attack. Chapter III will explain the four DHS mission areas and how they relate to first responder communications. In addition, it points out there are communication problems in each of the four DHS mission areas that are not currently being addressed. Further, these problems are significant enough to enable communication outages from cyber attack, if not addressed. Chapter IV will highlight the lessons learned from first responder exercises at local, state, and the national level. It does not encompass the lessons learned from every first responder exercise because after action reports and lessons learned are usually kept close hold by the agency conducting the exercises. However, there were enough sources on the open Internet to highlight common findings that need DHS attention with respect to their first responder communications. Chapter IV includes a table with common findings across all levels of first responder communications. Chapter V will use the observations from chapters II, III, and IV in order to build a base proposal for "comm-out" first responder operational exercises. Chapter V will conclude with key findings, and suggest areas for future research.

II. CYBER ATTACK

> *If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere.*
>
> —Carl von Clausewitz

A. INTRODUCTION

Historically, cyber attackers have found creative ways to thwart cyber defenses. We live in a time and age where a majority of our society relies heavily on digital communications to conduct daily business and their personal lives. Just the thought of any of our digital communications not being available on demand is becoming unthinkable. This chapter will take the first step in presenting the case that digital communications may not be available when needed by DHS in disaster recovery operations. It will show that attackers have continued to find creative ways to conduct cyber attacks. In addition, the cases presented will show that the technology exists to conduct cyber attacks against United States assets. These attacks may be against United States companies, critical infrastructure, and DHS first responders. The objective of these attackers may be to support military action against the United States, or further an organizations' political agenda. The last section of this chapter will outline a possible future cyber attack that could cripple a major hospital, which first responders depend on during disaster recovery. This scenario describes how an attack against one of the United States' critical infrastructures could happen.

B. CYBER ATTACK TOOLS

Cyber attacks employ malicious software called "malware" to conduct harmful activities on electronic communications. Malware is a term used to identify computer software designed to damage or produce other unwanted actions without the consent of the systems' owner. It is a generic term that covers all types of destructive software to include computer viruses, worms, trojan horses, spyware, logic bombs, key loggers,

scareware, backdoors, botnet code, sniffers, and rootkits.[16][17] When discussing and understanding malware, these ten categories are not independent of each other and are often blended together to achieve a desired objective. Further, each of these types of malware can carry different types of payload depending on the desired objective of the cyber attack. Payloads can serve a variety of objectives, including sabotage, espionage, fraud, control, amusement, protest, denial of service, extortion, and even physical destruction.

Cyber attacks can be classified in four categories: penetration attacks, bandwidth flooding attacks, cyber infrastructure attacks, and electronic warfare attacks. Penetration attacks seek to gain access to an automated system and then elevate privileges, often with the help of rootkits. Rootkits allow attackers to mask intrusion and gain elevated privileges to a computer or network.[18] Bandwidth flooding attacks are normally used to conduct denial of service attacks, and involve overwhelming a network with large amounts of traffic. Cyber infrastructure attacks focus on vulnerabilities found in Internet services, such as Domain Name Systems (DNS), and seek to hijack the service or otherwise interfere with its normal operation. Electronic warfare attacks seek to jam communication signals or inject signals into a communications transfer that changes the information.[19]

Known cyber attacks can often be blocked by firewalls, intrusion detection tools, and malware scanning software; however, there is a growing number of unique forms of malware that severely stress current defenses. Most current defenses rely on known signature files to block malware; however, these usually fail against new forms.

---

16 NOTE: Definition of Malware came from, "The Tech Terms Computer Dictionary," and can be found online at http://www.techterms.com/definition/malware.

17 NOTE: Types of Malware source was from a lecture by Dorothy Denning on 19 July 2010 given at the Naval Postgraduate School in Monterey California.

18 Shon Harris, *All in One CISSP Exam Guide: Fifth Edition*,2010, 649.

19 NOTE: Lecture given by Dorothy Denning on 19 July 2010 at the Naval Postgraduate School in Monterey California.

Blocking these requires more sophisticated defenses based on behavioral analysis. Many systems are not adequately protected with such defenses, making new malware an especially serious threat.

McAfee, a software security company which writes anti-malware software tools to detect and remove malware from a computer or network, began collecting a database of unique malware in 1986. While it took them 22 years, from 1986 through 2008, to collect the first 10 million unique samples of malware, it only took another year for that number to double to over 20 million, and in early 2010 the number had jumped to over 44 million.[20][21] We are now seeing over 54,000 new malware samples on the Internet every day.[22] This exponential growth of malware is making it very difficult to ensure communications will always be available when needed. If an adversary were to use this type of malware against first responders, it could significantly slow a recovery effort.

C. VIRUSES AND WORMS

Viruses were among the earliest forms of malware, and a ninth grader named Richard Skrenta used his 1982 Apple II computer to create the first.[23] Since computer viruses must have a host application to replicate, and early Apple computers stored their operating systems on floppy disk, it was easy for Skrenta to spread his virus via floppy disk through computer labs at his high school. By 1986, the most popular home computer in the world was built on an IBM platform, and that same year, the first virus for IBM computers was developed and released into the wild.[24, 25] Through the late

---

20 Francois Paget, "Malware at Midyear: a Summary," McAfee Labs, 7 July 2010, https://www.afit.edu/cip/index.cfm, (accessed 20 October 2010).

21 Francois Paget, "Malware at Midyear: a Summary," McAfee Labs, 7 July 2010, https://www.afit.edu/cip/index.cfm, (accessed 20 October 2010).

22 NOTE: Malware writers build off each others' code and it does not require much skill to create new malware.

23 Paquette, "A History of Viruses," Symantec, 16 July 2000, http://www.symantec.com/connect/articles/history-viruses, (accessed 18 September 2010).

24 NOTE: the phrase, "In the wild," is a computer term that means outside a testing environment or on the Internet with no controls.

25 Paquette, "A History of Viruses," Symantec, 16 July 2000, http://www.symantec.com/connect/articles/history-viruses, (accessed 18 September 2010).

1980s, viruses spread primarily through the boot sector and executable files on a floppy disk. Today, viruses spread through online media such as file sharing and e-mail, as well as portable media such as Universal Serial Bus (USB) memory sticks. The viruses of the late 1980s also transformed from harmless pranks into malicious attacks destroying digital information.

The late 1980s also brought about the launch of the first computer worms. Worms are similar to viruses, except they can spread on their own, without users taking explicit actions or the execution of a host application. They are self-contained programs that, once released, look for known vulnerabilities in computer systems and reproduce by exploiting these vulnerabilities.[26] Because worms can replicate on their own, they are able to spread across the Internet at much greater speeds than viruses.

Although not the first worms to be introduced into the wild, the "Code-Red" worm and the "Slammer" worm provide a good comparison on how fast worms can spread on their own. When Code-Red was launched on the morning of July 19, 2001, it was designed to exploit a known vulnerability in Microsoft's IIS (Internet Information Services) Web server. At the peak of Code-Red's growth, it was infecting over two thousand systems per minute and, in just 14 hours, it infected 359,000 machines across the globe.[27]

In comparison to Code-Red, when the Slammer worm was launched just two years later in 2003, it was two orders of magnitude faster than Code-Red. With Slammer, the number of systems infected doubled every 8.5 seconds in comparison to 37 minutes with Code-Red. This never before seen rate of growth allowed the Slammer worm to infect 90 percent of the systems in the world that were vulnerable to this attack in only 10 minutes.[28] It only took this single packet worm 30 minutes to spread to over 200,000

---

[26] Shon Harris, *All in One CISSP Exam Guide: Fifth Edition*,2010, 1020.

[27] David Moore, "The Spread of the Code-Red Worm," The Cooperative Association for Internet Data Analysis, 24 July 2001, http://www.caida.org/research/security/code-red/#background, (accessed 1 October 2010).

[28] David Moore, "The Spread of the Slammer Worm," The Cooperative Association for Internet Data Analysis, 2003, http://www.caida.org/publications/papers/2003/sapphire/, (accessed 1 October 2010).

systems around the globe. The Slammer worm was faster than previously launched worms because it used far less bandwidth and employed a better strategy for propagation. It was comprised of a single 404-byte User Datagram Protocol (UDP) packet compared to Code-Red's 4 Kbyte payload.[29]

It is important to note that both of these worms had a negative impact on society. Code-Red caused an estimated $2.62 Billion in global economic impact and was able to shut down a Japanese airline-ticketing counter, delaying 15,000 passengers for 2 hours.[30] The Slammer worm shut down ATMs in South Korea, emergency 911 systems, airline booking systems, and a monitoring system for a nuclear plant in Ohio; it also impacted control systems on electrical and water utilities.[31][32][33] In both cases, a known vulnerability for which patches existed was exploited. However, it is evident with the global spread of these two worms that systems administrators around the world were not updating their systems. These two cases are representative of the increase threat of cyber attacks. In just a few short years, malware grew from simple pranks in high schools to malicious attacks that affected electrical power grids, nuclear power plant networks, and emergency response communication systems.

D. ESPIONAGE

Espionage is a normal occurrence between companies and states; however, prior to the Internet and cyber attacks, it had to be conducted manually. Before the Internet, a

---

29 David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, "Inside the Slammer Worm," IEEE Computer Society, 2003, http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf, (accessed 17 October 2010).

30 Computer Economics, "Malicious Code Attacks Had $13.2 Billion Economic Impact in 2001," Computer Economics: Metrics for managers September 2002, http://www.computereconomics.com/article.cfm?id=133, (accessed 18 Spetember 2010).

31 Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," Security Focus, 19 August 2003, http://www.securityfocus.com/news/6767, (accessed 7 May 2010).

32 A. Creery, "Industrial Cybersecurity for Power System and SCADA Networks," Andritz Automation, n.d., http://www.andritzautomation.com/documents/industrialcybersecurity.pdf, (accessed 10 August 2010).

33 Peter Abraham, "The Slammer Worm Attack: The worst attack to date, probably not the last," Dynamic Net, 14 February 2003, http://www.dynamicnet.net/news/articles/slammer.html, (accessed 10 August 2010).

spy had to have insider access to classified data relating to United States national security; now they simply have to hack into a computer system and download the information. In the true-life movie, the Falcon and the Snowman set in the late 1970s, it takes thousands of dollars, an insider with a security clearance and lots of time to steal a very small amount of information.[34] Conversely, with cyber infiltration, terabytes of information can be downloaded with little cost to the spy or spying agencies in very a short amount time.

Cyber espionage has targeted highly protected government networks, as well as major corporations. The next three cases, Moonlight Maze, Titan Rain, and Operation Aurora will make the point that even protected networks can be penetrated. In each of these three cases, network security departments were defending the targeted networks, but their electronic defenses were defeated.

1. Moonlight Maze

An early example of cyber espionage to steal mass amounts of data was coded "Moonlight Maze". Moonlight Maze was an ongoing FBI case that uncovered that data was being stolen from United States critical networks. The intrusions conducted during Moonlight Maze began in 1998 and continued for several years.[35] Two significant aspects displayed the growing sophistication associated with cyber attacks. First, they were sustained for over a three-year period. This level of a continued intrusion had never been seen prior to Moonlight Maze, and proved that it is possible to conduct a sustained cyber attack. Second, when United States computer security specialists attempted to fight the attack, they were defeated. The intrusions consistently went around defenses, and at times, became stealth to United States defenders.[36] By the time they were noticed, they

---

[34] Bonnie Sayer, "The Falcon and The Snowman," Epinions, 30 September 2001, http://www99.epinions.com/review/mvie_mu-1007016/content_42021654148, (accessed 1 October 2010).

[35] CNN Tech, "Epic Cyber Attack Reveals Cracks in United States Defense," CNN Tech, 10 May 2001, http://articles.cnn.com/2001-05-10/tech/3.year.cyberattack.idg_1_moonlight-maze-hackers-russian-Internet-addresses?_s=PM:TECH, (accessed 17 March 2010).

[36] Richard A. Clarke, and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it,* 2010,111.

had been going on for over two years. Investigators determined that the source was a mainframe computer in Russia, and that the targets included the Pentagon, NASA, the Energy Department, universities, and research labs. When the United States government asked Russia if they were sponsoring the intrusions, the Russian government denied any involvement.

2. Titan Rain

Another well-known case of cyber espionage happened in 2004, and was given the code name Titan Rain.[37] Titian Rain was an FBI investigation that determined classified data was being stolen electronically through the Internet from Sandia Labs, Army Research Labs, Lockheed Martin, NASA, and the World Bank. The investigation determined that Chinese hackers had infiltrated Sandia Labs, United States government agencies, United States military installations, and defense contractors, and had electronically stolen critical information protecting United States national security.

3. Operation Aurora

A more recent and highly sophisticated case of cyber espionage against United States companies was code named "Operation Aurora" by the computer security company McAfee.[38] Interestingly, Operation Aurora involved coordinated attacks against 20 major corporations with large computer security departments.[39] According to the vice president of McAfee's threat research, Dmitri Alperovitch, this type of attack has never been seen outside of the defense industry and stated, "We have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack, it's totally changing the threat model." Alperovitch goes on to point

---

[37] Richard Stiennon, *Surviving Cyber War*, The Scarecrow Press 2010, 1–10.

[38] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora/, (accessed 22 October 2010).

[39] McAfee, "Operation Aurora," McAfee, 14 January 2010, http://www.mcafee.com/us/threat_center/operation_aurora.html, (accessed 22 october 2010).

out that a zero-day exploit was used to employ a dozen pieces of malware, and the attack was encrypted at a level McAfee had never seen.[40]

Although espionage in the above cases did not cause communication failure in the governments and companies attacked, the cases illustrated three significant issues. First, they showed that cyber intrusions could be sustained over time. Second, they proved that even if an organization is using sound network security technology and employs a knowledgeable network security department, their defenses could still be subverted. Third, these cases show that cyber intrusions can be specifically targeted. Moreover, and perhaps most importantly, many of the tools employed in cyber espionage can be employed to conduct cyber attacks. Once a network has been penetrated, an intruder can tamper with or delete data, and cause systems to fail.

E. TARGETED ATTACKS

The previous section showed that cyber attackers have the ability to surgically hit specific targets within their attacks. The two cases that follow show that surgical and/or targeted cyber attacks can be used for purposes other than espionage. By outlining these cases, this section will illustrate that cyber attacks are another weapon that can be used to gain an advantage.

1. Israel Attacks Syria

The first case is the attack of the Israeli Air Force against Syria on the night of September 6, 2007. Although the attacks were not sustained over time, their surgical precision proved powerful and demonstrated that cyber attacks can be used effectively in conflict. As a result of the attack, the Israeli Air Force was able to fly non-stealthy fighter aircraft 75 miles into Syria and destroy a building under construction, which was thought to house nuclear materials shipped from North Korea.[41]

---

[40] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora/, (accessed 22 October 2010).

[41] Sarah Baxter, Michael Sheridan, and Uzi Mahnaimi, "Israelis Blew Apart Syrian Nuclear Cache," The Times Online, 16 September 2007, http://www.timesonline.co.uk/tol/news/world/middle_east/article2461421.ece, (accessed 5 October 2010).

Syria has an extensive air defense system along its border that is designed to identify any aircraft that enters its air space; however, on the night of the bombings, the system showed Syrian operators that the air space remained clear.[42] In this case, United States analysts claim that brute-force electronic jamming, centralized Syrian air defense command and control, air to ground electronic attack, and computer-to-computer links were used to penetrate and disarm Syrian defenses. According to an article in Aviation Week, the Israeli military and government admitted they used cyber attacks as part of their defense capabilities.[43]

> Despite being hobbled by the restrictions of secrecy and diplomacy, Israeli military and government officials confirm that network invasion, information warfare and electronic attack are part of Israel's defense capabilities.
>
> They've been embraced operationally by key military units, but their development, use and the techniques employed are still a mystery even to other defense and government organizations. It remains "a shadowy world," says an Israeli Air Force general.

The Syrian facility was completely destroyed, the Israeli non-stealthy aircraft were never detected, and via electronic means, the air warning radars and surface to air missiles defense systems employed by Syria failed to react to the attack.[44] This marks a giant milestone in the evolution of cyber attacks because it is the first time a nation state has admitted to using cyber attacks in concert with a physical attack, by demonstrating actual nation state cyber capabilities.

---

[42] Clarke, Richard and Robert K. Knake, *Cyber War, The Next Threat to National Security and What To Do About it*, 2010, 1–9.

[43] David A. Fulghum, Robert Wall and Amy Butler, "Israel Shows Electronic Prowess," Aviation Week, 25 November 2007, http://www.aviationweek.com/aw/generic/story.jsp?id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess&channel=defense, (accessed 10 August 2010).

[44] Richard B. Gasparre, "The Israeli 'E-tack' on Syria," Air Force Technology, 10 March 2008, http://www.airforce-technology.com/features/feature1625/, (accessed 5 October 2010).

2. Stuxnet Worm

While this chapter was being written, the world witnessed a leap in cyber attack technology. The Stuxnet worm appears to only target Siemens' Industrial Control System's (ICS) which are used, among other places, to control nuclear power plants, electrical grids, and other critical infrastructure.[45] The worm infected over 45,000 industrial networks around the globe; however, it appears to only be malicious against certain types of systems.[46] Michael Assante, former chief of industrial control systems cyber security research at the United States Department of Energy's Idaho National Laboratory was quoted saying, "This is the first direct example of weaponized software, highly customized and designed to find a particular target."[47] Since this case is still under investigation, this thesis will not go into detail, and simply point out the fact that if the initial findings of this worm are true, then cyber attacks against specific targets are gaining sophistication. If a worm can be designed to hit only ICSs used in critical infrastructure, then the possibility exists that a worm can be designed to hit any specific target.

There are numerous other examples of targeted attacks, including denial of service attacks that have shut down particular websites and communication servers. These attacks often leverage "botnets" (networks of compromised computers under the control of the attacker through a command and control infrastructure) to amplify effects, but considerable damage is also possible from a single attacking machine. Such attacks could disrupt or disable first responder communication networks.

This chapter has shown the beginning of cyber attacks "in the wild," pointing out that attacks have evolved and can penetrate networks that are heavily defended. We do not know what attacks will surface next, what individuals or even nation states have in

---

[45] Paul Marks, "Why the Stuxnet Worm is Like Nothing Seen Before," News Science, 12 October 2010, http://www.newscientist.com/article/dn19504-why-the-stuxnet-worm-is-like-nothing-seen-before.html, (accessed 22 October 2010).

[46] Fox News, "Is a Cyber Attack Targeting Iran's Nuclear Plant," Fox News, 23 September 2010, (accessed 23 September 2010).

[47] Fox News, "Is a Cyber Attack Targeting Iran's Nuclear Plant," Fox News, 23 September 2010, (accessed 23 September 2010).

their secret arsenal, or when the next evolution in cyber attacks will take place. The last section of this chapter will lay out how the next evolution in cyber attacks might occur using a cyber attack scenario against United States critical infrastructure, in this case the infrastructure of a major hospital. However, the fundamentals of the attack could be conducted against any critical infrastructure that is controlled digitally through cyberspace and any computer network attached to the Internet.

F. FUTURE SCENARIO

First responders are dependent on hospitals in most disaster recovery efforts. They have to communicate with hospitals and other first responders before transporting patients. This section will outline a possible scenario that an attacker might use to penetrate a major hospital in the United States. The objective of the attacker will be to erode trust in the data systems and information used in the hospital to the point that the employees of the hospital can no longer can use it. Once trust has been eroded, the hospital will fall back on manual methods of records and equipment, thus, making it impossible to keep pace with the operations tempo during a disaster. It is important to note that the tools used in the following scenario are available today, easy to find, and defenses such as anti-viral software, intrusion detection systems and firewalls may not stop attackers from conducting similar cyber attacks.[48]

This scenario will outline five phases an attacker could employ to conduct a successful penetration attack on a hospital or any United States critical infrastructure that is attached and dependent upon the Internet. The five phases are: footprinting, scanning, gaining access, maintaining access, and if possible, covering their tracks.[49] Through each of these phases, the scenario will provide an understanding of the phases and what an attacker would hope to achieve in each phase of the attack. Once an attacker has gone

---

[48] NOTE: Information was presented in a presentation given by the CEO of HB Gary Inc., Gary Hoglund at a cyber crime conference at UC Davis on 5 August 2010. HB Gary is a computer security company that works with the FBI, DHS, DoD, and civilian companies to secure their networks.

[49] Andrew Landsman, "The Five Phase Approach of Malicious Hackers," Network Security Blog, 8 May 2009, http://blog.emagined.com/2009/05/08/the-five-phase-approach-of-malicious-hackers/, (accessed 8 May 2010).

through the five phases, they normally leave a door open in the system to allow for future access. Figure 1 illustrates the five phases of a cyber attack and how the phases are an ongoing and continuous cycle of events when deployed by a knowledgeable attacker.

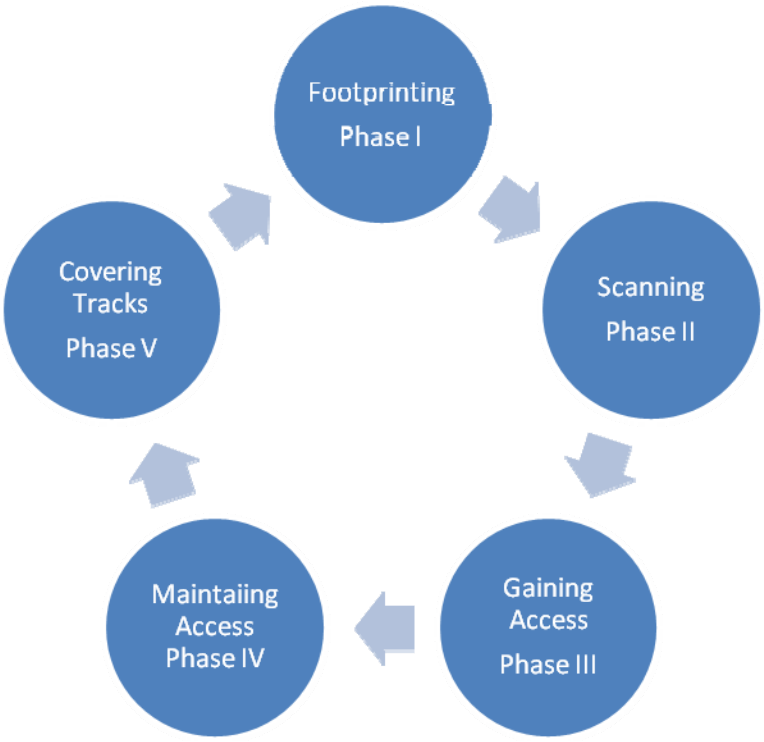

Figure 1. Cyber Attack Phases

1. Phase I

Footprinting of a cyber system is part of the reconnaissance portion of a cyber attack, and the first step an attacker takes when preparing to conduct cyber attacks on a system or network. In this phase, the attacker builds a blueprint of the target and includes details such as the domain name, network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, access control mechanisms and related lists, phone numbers, contact addresses, authentication

mechanisms, and system enumeration.[50, 51] This information can be found in many ways, including dumpster diving, social engineering, Google searching and Google hacking, and even by scanning the target's help wanted ads, which often list what systems a prospective employee should have experience with.[52] There are numerous software programs on the Internet that can be downloaded to help an attacker footprint a target. Just a few of the literally hundreds of tools used to footprint are: Whois, Nslookup, ARIN, Neo Trace, VisualRoute Trace, Smart Whois, eMailTrackerPro, Website Watcher, Google, Google Earth, Geo Spider, HTTrack Web Copier, and E-mail Spider.[53] These footprinting tools exist on the open Internet and can be employed by anyone who wants to use them. Attackers spend 90 percent of their time and energy in the footprinting phase of a cyber attack, and during this phase, targets usually suspect nothing is happening to their cyber systems.[54] The footprinting phase can go on for weeks, months and even years if the target is worthwhile.

During phase I of this scenario, the attacker goes through the hospital's job ads, looking for the types of software and hardware deployed at the hospital. The attacker also conducts Google searches to find specific e-mail addresses of the hospital's employees and what other organizations the hospitals employees are members. A good example of how Google can be used to find e-mail addresses is the Google string, (+@XYZ.com -www.XYZ.com) where the attacker replaces the XYZ with the targets name. This Google string will return a list of hospital employees' e-mail addresses and

---

[50] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 1, 220.

[51] NOTE: Systems enumeration is a catalog or lists that groups information used by hackers. Some examples of systems enumeration include list of network resources and shares, users and groups, applications and banners, and auditing settings. Source: EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 2, 687.

[52] Andrew Landsman, "The Five Phase Approach of Malicious Hackers," Network Security Blog, 8 May 2009, http://blog.emagined.com/2009/05/08/the-five-phase-approach-of-malicious-hackers/, (accessed 8 May 2010).

[53] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 1, 257.

[54] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 1, 220.

organizational website that the hospital's employees may be associated with and access using their hospital e-mail addresses. This information helps an attacker craft very specific phishing e-mails that can be used in Phase III, gaining access, later in the cyber attack.

2. Phase II

The second phase in a cyber attack, scanning, is still part of the reconnaissance portion of a cyber attack; however, in this phase, the attacker uses more aggressive tools that find specific vulnerabilities in the network or systems. Three types of scanning that an attacker might use include port scanning, network scanning, and vulnerability scanning.[55] This section will explain each and provide examples of how an attacker would use scanning in the hospital cyber attack scenario.

Network scanning is used to identify active host systems on a network and map the network structure. Attackers use tools such as ping sweeps to return information about IP addresses that correspond to live host systems on the Internet. This allows an attacker to get a clear picture of what host systems are running on a targeted network.[56]

Port scanning looks for open ports on a network's host computers, which indicate what services a system or network is running. Many software programs conduct port scanning. These programs target a system or network by sending a sequence of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets to determine if the services running on the targeted system or network are in a "listening state".[57] Sometimes, an attacker can gain unauthorized access to systems and networks through open ports if the service software is misconfigured or has vulnerabilities[58]

---

[55] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 2, 451.

[56] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 2, 452.

[57] NOTE: Refers to the port being open and ready to establish communications to a system or network outside the system the port is on.

[58] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 2, 452.

The third type of scanning, vulnerability scanning, is an automated method used to identify known vulnerabilities in a system or network. Vulnerability scanning is comprised of a scanning engine and a catalog that includes a list of common files with known vulnerabilities and common exploits. Just like the previous two types of scanning, vulnerability scanning helps an attacker gain unauthorized access to a targeted system or network.[59]

Scanning serves seven objectives for an attacker. First, to detect any live systems running on the network. Second, to discover which ports are open on the live systems, and therefore, candidates for entry. Third, to discover the operating system being used on the targeted system. Fourth, to discover the services running and specifically which ones are listening on the targeted system. Fifth, to discover the IP addresses on a targeted system and network. Sixth, to identify the applications and even what versions of the applications are running on the targeted system. Last, to identify all vulnerabilities that exist on any system across the network.[60] The goal of this phase is to find an opening and use it to exploit a given target and gain access to the system or network.

In the hospital scenario, the attacker uses the information found in the footprinting phase and applies scanning tools downloaded free from the Internet. With these tools, the attacker finds several openings in the hospitals network and systems. The attacker then makes a map of the hospital's network and lists each vulnerability on each system within the network that will be used later to gain access to the network. Next, the attacker writes, purchases, or downloads free malware and malware generators that will be used in phase III of the attack to gain access to the targeted system or network.

3. Phase III

During phase III, the attacker employs several techniques to gain access to the targeted systems or network. Using the information collected in phases I and II of the

---

[59] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 2, 452.

[60] EC-Council, "Ethical Hacking and Countermeasures training Course," EC-Council, 2010, Version 6.1, Vol. 2, 452.

attack, an attacker can conduct phishing and spear-phishing scams, SQL injections, and a variety of other attacks. To accomplish this, the attacker can create or acquire literally thousands of attack tools. This section will discuss several methods an attacker could use to gain access and show how they could be employed in the hospital scenario.

Phishing is a mechanism that uses social engineering and subterfuge to gain personal information and access credentials of people on a system or network.[61][62] Phishing targets a large number of people, while spear-phishing targets specific individuals or organizations. Both forms typically use spoofed e-mails claiming to be legitimate businesses or trusted organizations in an attempt to lead their targets to counterfeit websites, where they are tricked into divulging personal data or access credentials for legitimate systems and networks.[63] Phishing may also employ methods of subterfuge, such as planting software on a network that intercepts a user's access credentials to a particular system. Currently, most phishing scams are used to extract account credentials for financial services; however, these methods can be used for other purposes such as getting passwords to government systems.

Attackers can create, purchase, or download free programs that exploit weaknesses in systems and networks to attack their targets. There are many malware generating programs on the Internet, such as Eleanor, Tornado, Napoleon, and Zeus. These programs allow an attacker to enter the information collected in the footprinting and scanning phases, and then generate thousands of attacks that can be used on the specific targeted system or network depending on its configuration.

In the hospital scenario, the attacker uses the information collected in the footprinting and scanning phases to launch a phishing scam against the hospital's employees. The attacker tailors the spoofed e-mails to look like they come from a medical employee's life insurance company, hoping that at least one employee bites and

---

61 Shon Harris, All in One CISSP Exam Guide: Fifth Edition, 2010, 263.

62 Ronnie Manning, "Phishing Activity Trends," Antiphishing, 1st Quarter 2010, http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf , (accessed October 2010).

63 Ronnie Manning, "Phishing Activity Trends," Antiphishing, 1st Quarter 2010, http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf , (accessed October 2010).

divulges account information. The attacker also creates a spear-phishing e-mail that targets the hospital's president and two top doctors. The attacker pretends to be a trusted person in an organization the three belong to, hoping that if one bites, the attacker will gain elevated privileges within the hospital's systems and network. Simultaneously, the attacker employs the botnet building software Zeus and builds a botnet to decrease the chances of later being exposed by an investigation. Further, the attacker downloads Tornado, a Russian malware program, loads information about the hospital's network and systems into the program and generates 11,000 pieces of malware that can be used in this phase of the attack.

At this point, the attacker has footprinted and scanned the hospitals systems and networks, mapped and outlined vulnerabilities, and now purchased and developed the tools to gain access. The next step is to use these tools to gain access to the hospital's systems and network, and then sit back and wait for a month. After a month, the attacker uses the gained access to deploy multiple rootkits to as many systems in the network as possible. Rootkits are malware that gain administrator access to a system or network and use multiple techniques to avoid detection.[64, 65] Once rootkits are installed on a system, an attacker can use them and other malware to destroy, alter, and steal data; intercept or alter transmissions; and even change the behavior of a system. Rootkits can be installed in the systems "operating systems kernel" and when done correctly, this code is very difficult and sometimes impossible to find and remove.

4. Phase IV

During phase IV, the attacker employs installed rootkits and other malware to maintain access and begin the execution portion of the attack. At this stage, the target may notice changes to data or software that indicate they are under cyber attack. This section discusses how an attacker could maintain access once the target realizes they are

[64] Shon Harris, *All in One CISSP Exam Guide: Fifth Edition*, 2010, 649.

[65] Peter H. Gregory, and Lawrence Miller, *CISSP for Dummies*, Wiley, 2010, pp.118-119.

under attack, and using the hospital scenario, shows how employees could reach a state where they no longer trust the hospital's systems and network.

The hospital computer systems administrators begin to notice strange things happening in their network and notify management that they may have a possible virus or cyber attack taking place in parts of the network. The administrators advise management that they will work to remove the malware from the network. Management agrees and work in the hospital continues. The hospital's system administrators find the malware that is causing the problems and remove it from the network. They then report to management that the system is back to normal. In the meantime, employees of the hospital are reporting that some of the data in the system does not seem to be correct and several errors have been found in patient records. The hospital leadership announces that the network had a virus; however, the systems administration branch has found the infected files and removed them. The attacker waits another month, and then uses a second rootkit to launch more malware, which begins to erase data, and again changes existing data. Again, the systems administrators begin receiving calls that something is wrong with several systems across the network and they report to leadership that there might be another virus in the hospital's network. Leadership again sends them back to work to remove the malware from the hospital's network; however, this time they are unable to find the malware and it continues to delete and change data. The hospital finally decides to reload their systems and fall back on a backup they took eight days earlier when they believed their network was not infected. The problem is that the backup tapes now incorporate the rootkits and the attacker still maintains access.

The attacker then uses a third rootkit to launch another phase of malware, deleting data, changing records, and infects equipment used for patient care. The attack has been happening for over a month now, and each phase is getting worse. The employees of the hospital lose trust in the digital information and equipment used to run the hospital and employ their emergency contingency plan. The plan is to use paper records and manual equipment for patient care. The hospital's employees have lost confidence in their data systems and the attacker has achieved their objective. At this point, the hospital might

call in the FBI to assist in an investigation. They may also call in outside computer security companies to help find any malware that still resides on their systems and to help install better defenses against future attacks.

5. Phase V

While the hospital scrambles to defend these attacks, wondering when the next phase will be employed, the attacker notices evidence of an investigation and decides to cover their tracks and back out of the network. To make tracing more difficult, the attacker entered the hospital's network via compromised computers belonging to a botnet.[66] In addition, the attacker's rootkit shuts down the logging and detection methods deployed on the network, making it difficult to track down the source of the attack.

G. CONCLUSION

This chapter showed that cyber attackers have continually found creative ways to conduct cyber attacks, using cases to illustrate how cyber attacks have grown from mere high school pranks to deliberate attacks against civilian companies, government, and critical infrastructure. With the growing threat of cyber attack and the evolving technology used to conduct them, it is becoming evident that corporations and government agencies will not always have 100 percent of their digital communications available. During times of crises, organizations and states may employ cyber attacks to disrupt the confidentiality, availability and integrity of their adversary's data and electronic communications. This chapter demonstrated that cyber attacks can and have produced mass affects, and they are likely to continue. It pointed out that the tools needed to disrupt the availability of electronic communications are available. If these tools exist to disrupt electrical communications, then what would keep a United States adversary from deploying cyber attacks against United States critical infrastructure or even against first responders in a disaster recovery effort? Cyber attacks could be used to slow a United States military response, as an extension of an adversary's military

[66] NOTE: A botnet is a network of computers that have been taken over by an attacker and used to send out spam or launch cyber attacks.

response against the United States, or as an extension of an adversary's political agenda. Since this threat is real, and has been displayed in several cases, DHS can no longer expect that they will have all communications methods available during a contingency. It is time that DHS understands what a cyber attack could do to a major disaster recovery effort and exercise how they would operate through a cyber attack.

III. PREVENT, PROTECT, RESPOND, AND RECOVERY AGAINST CYBER ATTACKS

There is no security on this earth; there is only opportunity.

—Douglas MacArthur

A. INTRODUCTION

Homeland Security Presidential Directive 8 (HSPD 8) was established to strengthen emergency preparedness in the United States through prevention and response. HSPD 8 requires an all-hazards preparedness approach to improve delivery of federal assistance to state and local governments.[67] The term "all-hazards preparedness" is a conceptual and management approach that uses the same set of arrangements to manage all types of hazards with the belief that no one knows what disaster will happen next. According to DHS, the term "all-hazards preparedness" refers to the nation's preparedness for domestic terrorist attacks, major disasters, and other emergencies.[68] DHS has given the Federal Emergency Management Agency (FEMA) the operational management task of all-hazards preparedness for first responders. In order to manage this task, FEMA created the National Preparedness Directorate (NPD), which provides all-hazards preparedness guidance for first responders at federal, state, local and tribal government agencies. This guidance is built around DHS's four mission areas of prevention, protection, response, and recovery against terrorist attacks, natural disasters, and other emergency incidents that require involvement from first responders.[69] This

[67] Department of Homeland Security, "Homeland Security Directive 8: National Preparedness," Department of Homeland Security, 17 December 2003, http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm, (accessed 9 November 2010).

[68] Department of Homeland Security, "Homeland Security Directive 8: National Preparedness," Departement of Homeland Security, 17 December 2003, http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm, (accessed 9 November 2010).

[69] Federal Emergency Management Agency, "National Preparedness Directorate," Federal Emergency Management Agency, 11 August 2010, http://www.fema.gov/media/fact_sheets/npd.shtm, (accessed 9 November 2010).

chapter defines the four areas of DHS's all-hazards preparedness approach with respect to cyber attacks, and highlights why first responder communications may not be available during a cyber attack.

B. PREVENT

One way to ensure first responders communications systems will operate through a cyber attack is to avoid the attack completely or stop it from happening in the first place. DHS's mission area of prevention attempts to address this area and build mechanisms that would avoid or stop a cyber attack against critical infrastructure. This section will point out the efforts currently being employed to avoid and stop a cyber attack, and where they fall short. It will outline the National Security Agency's focus on a layered defense-in-depth approach to the prevention of cyber attacks. Second, it will look at the major mechanisms DHS is employing to create a defense-in-depth approach across government and critical infrastructure networks. More specifically, this section will look at DHS's Einstein Intrusion Detection System (IDS), the Trusted Internet Connections (TIC) initiative, and the Computer Emergency Response Teams (CERTS). Finally, this section will illustrate areas where these initiatives are currently failing in regard to preventing cyber attacks on the critical infrastructures that first responders are dependent upon during a major disaster.

The National Security Agency (NSA) refers to defense-in-depth as a "best practice" strategy that employs intelligent people, proper use of cutting-edge technologies, and smart daily operations.[70] The concept of defense-in-depth is widely accepted in the computer security industry as a means to resist and defend against cyber attacks; however, the industry also understands that the attackers have the upper hand. This section will point out that there are not enough resources or cooperation to employ an effective defense-in-depth strategy across all levels of governments, first responders, and critical infrastructure.

---

[70] National Security Agency, ""Defense in Depth,"" National Security Agency, 2000, http://www.nsa.gov/ia/_files/support/defenseindepth.pdf, (accessed 23 October 2010).

DHS's Einstein IDS was launched to protect federal executive agency information technology (IT) enterprises.[71] The system is currently deployed on a handful of federal agency's networks including DHS, the Department of Agriculture, the State Department, and the Department of Interior. All Internet traffic that flows through these agencies is monitored by Einstein and then analyzed by DHS's CERT.[72] What makes Einstein different from commercially available IDSs is that DHS has partnered with the Department of Defense (DoD), and is using malware signatures from specific attacks against the DoD and foreign allies.

Einstein is a good start; however, it is currently failing to prevent cyber attacks in three ways. First, it only detects known attacks, missing attacks that use new malware or that exploit zero-day (previously unknown) vulnerabilities.[73] With over 54,000 pieces of new malware every day, this may be leaving the critical infrastructure needed by first responders vulnerable to a cyber attack. Second, DHS cannot force other government agencies and civilian companies to use the system, and there are concerns that it infringes on civil liberties. DHS lacks any regulations that would give them the authority to require other government agencies and civilian companies to employ Einstein. The Senate is being very cautious in giving DHS any real backing to enforce the use of Einstein due to civil liberty concerns. The Senate is concerned that this level of intrusion detection could fall under the electronic surveillance laws, which would require a court order.[74] If a court order were needed to monitor an agency's network traffic, it would slow the process down significantly making it less effective in preventing cyber attacks. Last, DHS has

---

[71] Hugo Teufel, III, ""Privacy Impact Assessment for Einstein 2,"" 19 May 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf, (accessed 10 November 2010), 2.

[72] Carolyn Duffy Marsan,""Einstien 2: United States Government's 'Enlightening' New Cybersecurity Weapon,"" Network World, 11 February 2010, http://www.networkworld.com/news/2010/021110-cybersecurity-einstein-2.html (accessed 10 november 2010).

[73] Carolyn Duffy Marsan, ""Einstien 2: United States Government's 'Enlightening' New Cybersecurity Weapon,"" Network World, 11 February 2010, http://www.networkworld.com/news/2010/021110-cybersecurity-einstein-2.html (accessed 10 november 2010).

[74] Eric Chabrow, "Einstein 3 Privacy Concerns Voiced,"" Government Info Security, 17 november 2009, http://www.govinfosecurity.com/articles.php?art_id=1946, (accessed 10 November 2010).

been withholding data from other agencies that could have helped them address security breaches.[75] The accusation against DHS in regards to lack of sharing information may be explained by the fact that only 45 of the 98 positions that perform this function have been filled. In addition, the current Einstein system is said to be too slow to actually block a cyber attack.[76]

The second mechanism DHS is deploying through their CERTs is the Trusted Internet Connections (TIC) initiative. TIC is an effort to reduce the over 4,300 Internet connections to government systems to approximately 50.[77] The idea is to restrict the number of connections that need to be monitored in order to better capitalize on DHS's limited resources. Again, this initiative is not being deployed to critical infrastructures that first responders are dependent upon. DHS does not have regulatory teeth to actually force other agencies to comply. Further, reducing the number of connections to the Internet could create choke points for systems such as Einstein. If Einstein is too slow to block a cyber attack on smaller bandwidth connections, it is hard to see how it will handle more concentrated TIC choke points. Therefore, the TIC initiative could compound existing problems.[78]

The third mechanism DHS has employed to prevent cyber attacks are the CERTs. DHS employs the United States CERTs to provide cyber attack support for the federal civil executive branches of government. Further, these CERTs have been charged to share methods and information about cyber attacks to state and local governments, and

---

[75] Siobhan Gorman, "United States Hampered in Fighting Cyber Attacks, Report Says," Wall Street Journal, 16 June 2010, http://online.wsj.com/article/SB10001424052748703280004575309243039061152.html, (accessed 10 November 2010).

[76] Siobhan Gorman, "United States Hampered in Fighting Cyber Attacks, Report Says," Wall Street Journal, 16 June 2010, http://online.wsj.com/article/SB10001424052748703280004575309243039061152.html, (accessed 10 November 2010).

[77] United States Computer Emergency Response Team, "Trusted Internet Connections Initiative," Department of Homeland Security, 4 June 2008, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2008_TIC_SOC_EvaluationReport.pdf, (accessed 10 November 2010), 3–7.

[78] NOTE: TIC and Einstein are intended to work together to build layers of defense mechanisms between federal government networks and the Internet.

industry.[79] Although US-CERT was originally created to respond to cyber attacks, which will be discussed in a later section, it is now providing preventative services to governments and industry by distributing information on vulnerabilities, conducting site visits, and suggesting ways government and industry can better secure their cyber assets.[80] However, the preventative programs are struggling, because like the Einstein IDS program, they lack resources and regulatory teeth to get other government agencies and industry to take action on the information they provide and vulnerabilities they identify. In addition, there is the question of who pays to fix the identified problems. If a critical infrastructure is privately owned, should the government pay to secure it? If critical infrastructure owners continually spend significant amounts of money to prevent cyber attacks, can they retain competitive advantage? Last, there are no laws that mandate how industry should protect their property against cyber attacks.[81] Even if laws could be used to protect privately owned property against cyber attacks, it would be difficult at best to pass such laws in the United States because of the concern with civil liberties.

This section highlighted that although DHS is employing major initiatives to prevent cyber attacks, their programs are falling short. There is a lack of resources at all levels of government and in industry to address the vulnerabilities and provide a defense-in-depth strategy. There is no central authority to direct what measures must be taken to prevent cyber attacks on governments and industry. DHS is working hard to put measures in place to help prevent cyber attacks; however, their efforts fall short and lack any real teeth to ensure their measures are being followed. Further, DHS is finding it difficult to fill the positions they have created to address these issues. Until DHS is given

---

[79] United States Computer Emergency Response Team, "About Us," Department of Homeland Security, 8 October 2009, http://www.us-cert.gov/aboutus.html, (accessed 10 November 2010).

[80] United States Computer Emergency Response Team, "Industrial Control Systems Cyber Emergency Response Team," Departemnt of Homeland Security, n.d., http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Fact_Sheet_02c.pdf, (accessed 10 November 2010).

[81] Elizabeth Montalbano, "Cyberattack Drill Shows United States Unprepared," Information Week, 17 February 2010, http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=222900723, (accessed 10 November 2010).

the backing by Congress and cooperation from industry, they will continue to struggle in their attempts to provide true prevention of cyber attacks.

C. PROTECT

Another way to ensure first responders can communicate through a cyber attack on critical infrastructure is to reduce the likelihood of a cyber attack. In a recent cyber security conference held in Washington, D.C., Bruce Held, the intelligence chief for the Department of Energy, pointed out that you cannot stop a cyber attack; however, you might be able to use diplomacy to keep one from being launched:

> A static cyber defense can never win against an agile cyber offense in preventing a catastrophic cyber attacks. You beat me 99 times; I will come after you 100 times. Beat me 999 times, I will come after you 1000 times, and we will beat you. If you want to protect the nation's electricity grid, beefing up security for it, physical security, cyber security, etc., quickly becomes prohibitively expensive. You need a protection strategy, and that means you have to change the game.

Essentially, it is about making an adversarial foreign power reconsider launching an attack. If you wish to influence my behavior, you have to impose risks and consequences on me. It does not have to be perfect. You just have to impact my behavior.

Michael Chertoff, the former Secretary of DHS, backed this idea at a conference in Europe, sighting President Eisenhower's Project Solarium, which established the theory of deterrence. This theory of deterrence defined the "rules of the road" and made it clear that if an attack on the United States or its allies took place, the US would respond with overwhelming force.[82] Can the United States and other nations construct treaties, memorandums of understanding, and even international law that would have the power to deter cyber attacks? This section will show that the elements needed for deterrence of cyber attacks do not currently exist, and therefore will not stop cyber attacks against the critical infrastructure that first responders need in an emergency situation.

---

[82] Tom Espiner, "Chertoff Advocates Cyber Cold War," ZDNet UK, 14 October 2010, http://www.zdnet.co.uk/news/security-threats/2010/10/14/chertoff-advocates-cyber-cold-war-40090538/, (accessed 10 November 2010).

It is difficult to find an authoritative statement in the United States government that defines deterrence with regard to defense policy.[83] This thesis will use United States Strategic Command's (USSTRATCOM) definition of deterrence. USSTRATCOM is the combatant command that governs the sub-unified and newly organized (as of 21 May 2010), United States Cyber Command.[84, 85] USSTRATCOM's definition of deterrence is as follows:

> Deterrence seeks to convince adversaries not to take actions that threaten United States vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and / or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome.[86]

This definition of deterrence has a classical Clausewitzian character about it; basically, it involves compelling your enemy to act in the way you want them to act without using violence. This way of thinking about deterrence can also be found in Air Force Doctrine 2-12 that covers Nuclear Operations, yet has no joint doctrine counterpart.[87] Based on these facts, it is safe to argue that this definition of deterrence is deeply rooted in Nuclear Operations and Air Force Doctrine.

In order for deterrence to work, certain elements must be present. First, all opponents in the game must be rational thinkers, meaning they are able to calculate the cost of their actions and understand that these costs outweigh the gains they will achieve

---

83 John D. Steinbruner, "Information Strategies and Developing Options for United States Policy," Letter Report from the Committee on Deterring Cyberattacks, March 2010, 302.

84 William Jackson, "DoD Creates Cyber Command as United States Strategic Command Subunit," *Federal Computer Week.* June 24, 2009. http://fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx (accessed August 30, 2010).

85 USSTRATCOM. "United States Cyber Command Fact Sheet," *United States Stategic Command.* May 2010. http://www.stratcom.mil/factsheets/cc/ (accessed August 30, 2010).

86 USSTRATCOM, "Future Joint War ConceptsVersion 2.0," Defense Technical Inforation Center, December 2010, (accessed 30 August 2010).

87 Stephen J. Miller, Maj Gen., USAF, Le May Center Commander, "Air Force Doctrine 2-12," May 2009, (accessed 30 August 2010), 3–43.

by taking the action.[88] Second, there must be a clear threat present that is understood by each of the opponents. This known threat is the rationale to build defenses and key to each opponent refraining from initial attack.[89] Finally, opponents must have the ability to launch a clear counter attack after they have been attacked.[90] These three elements needed for a successful deterrence strategy worked well for the United States during the Cold War.

During the Cold War, the United States and the Soviet Union displayed signs that they were rational thinkers and understood the cost of launching a nuclear missile at their opponents, meaning they understood what would happen in return to their respective nations. Therefore, they signed Strategic Arms Reduction Treaties and developed multination agreements like the Limited Test Ban Treaty, which was ratified by 94 nations.[91] In addition, both the United States and the Soviet Union demonstrated, through test or real-world use, that they had the ability to launch a devastating nuclear attack on their opponents. This element provided the threat and rationale that the costs could outweigh the benefits. Finally, through intelligence gathering and open sources, each country understood that they could not destroy all nuclear forces of their opponent through an initial strike. The advent of the nuclear submarine made it impossible for either country to guarantee that their opponent could not strike back. This remains a credible threat, even today, around the globe.[92]

All three elements needed to make deterrence a successful strategy were present during the Cold War. There were rational opponents, a real demonstrated threat, and the

---

[88] John D. Steinbruner, "Information Strategies and Developing Options for United States Policy," Letter Report from the Committee on Deterring Cyberattacks, March 2010, 303.

[89] Steinbruner, John D., "Information Strategies and Developing Options for United States Policy," Letter Report from the Committee on Deterring Cyberattacks, March 2010, 303.

[90] Libicki, Martin, C. Dr., "Deterrence in Cyberspace," High Frontier, Volume 5, Number 3, 15 February 2010, 16–20.

[91] John D. Steinbruner, "Information Strategies and Developing Options for United States Policy," Letter Report from the Committee on Deterring Cyberattacks, March 2010, 319.

[92] Mike Burleson, "Submarine Threat Worse Than You Think," Worldpress, http://newwars.wordpress.com/2010/05/27/submarine-threat-worse-than-you-think/ 27 May 2010, (accessed 30 August 2010).

ability of both opponents to launch a devastating counter attack. Can these three elements be applied to cyber attacks with the strength they had during the Cold War to deter a nation from striking first?

In order to explore if DoD's nuclear deterrence strategy could be applied successfully to a cyber attack aimed at first responder communications and United States critical infrastructure, this section will apply the three elements discussed above and how they relate to cyber. First, are the attackers in a future cyber attack rational? Second, does anyone really understand the full threat from cyber at this time? Finally, is it clear who to target in a counter attack, and if so, how effective would your counter attack be at costing the attacker more than what it is costing you?

Currently, only 14 nation states possess nuclear weapons. Of those, only the United States, Russia, and China have the ability to deliver them around the globe.[93] In contrast, most nations, hacking groups and individuals, including radical terrorists, have the ability to launch a cyber attack. These attacks can be delivered from anywhere at any time, and it is difficult at best to figure out their origin.[94] This makes the argument that if the origins of the attack are not known, and anyone can launch an attack, then how can a counter attack be conducted in all cases? Second, cyber attacks are in their infancy. There have been somewhat successful denial of service attacks on the countries of Georgia and Estonia; however, these types of attacks are basic and have not been claimed by a nation state. Until a nation state or very organized group launches a full spectrum cyber attack and admits to the attack, it will be difficult to understand the effects of a full-scale cyber attack. Even if a full-scale cyber attack is carried out, the chances that an attacker will use the same attack next time are very low. At this point in history, there is no common understanding of what cyber attacks could be in the future, and therefore, it will be very difficult for nations to grasp what a successful deterrence strategy needs to look like. Last, since it is difficult to figure out where an attack is coming from, and no

93 Tom Collins, "Nuclear Weapons: Who Has What at a Glance," Arms Control Association, http://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat (accessed 30 August 2010).

94 Thomas, C. Wingfield, "International Law and Information Operations," *Cyberpower and Natioanl Security*, Potomac Books, Inc., 2009. 525.

nation has admitted to conducting an attack at this time, how can the United States or any other major nation launch a devastating counter attack? Further, the United States, Russia, and China keep their cyber capabilities secret. Without the other countries knowing if their opponent can conduct a devastating counter attack, the element of counter attack in deterrence is lost.

If deterrence is to be successful for cyber weapons as it was for nuclear weapons, we must first develop the three elements around cyber attacks that have guided success during the Cold War. With the vast opponents in cyber space, it is not possible at this time to assume that everyone is a rational thinker and understands the cost. Second, the threat in cyber is not understood as well as the nuclear threat was during the Cold War. The atomic bomb dropped on Hiroshima by the United States in 1945 demonstrated the consequences of using nuclear weapons to the world. The devastation it produced made it very clear to the world what happens when nuclear weapons are deployed. However, there has not been an equivocal demonstration in cyber to date. Without a clear understanding that cyber attacks can produce devastating effects, this element of deterrence will not be fulfilled. Further, when the Wall Street Journal announced in April 2009 that the United States power grid was planted with Chinese logic bombs, the United States did nothing.[95] This action makes it difficult for our opponents to know if we really have ways to counter an attack when needed. Last, without knowing quickly and clearly who is launching an attack on the affected computer system or network, there is no way to launch a successful counter attack.

The three elements present during the Cold War that have made deterrence possible are not present in relation to cyber attacks. At this time, deterrence is simply not a viable solution for cyber attacks. However, the United States and other nations will continue to develop cyber attack capabilities and defenses in the future. As they mature, we might be in a better position to develop successful cyber deterrence strategies. Until then, cyber deterrence is improbable.

---

[95] Richard Clarke, and Robert K. Knake, *Cyber War, The Next Threat to National Security and What To Do About it*, 2010, 198.

D. RESPOND

DHS prepares for a comprehensive, swift and effective response to large-scale emergencies. FEMA, under DHS, is responsible for providing the guiding principles to enable first responders to conduct a unified national response to disasters and emergencies. These key principles are defined in the National Response Framework (NRF) and describe how communities, tribes, states, the federal government, and industry are to apply them for a coordinated, effective response.[96] Specific guidelines are provided in the NRF's Emergency Support Function Annexes (ESFs). For the purpose of this thesis, this section will focus on the cyber incident ESF, and specifically four areas that present challenges for a response effort to a significant cyber attack.

The first area that the guidelines ignore is the availability of expertise and surge capacity to address cyber attacks. As stated earlier, there are not enough technical experts to address the wide range of ongoing cyber attacks, so what is going to happen in an emergency response effort when there is a sophisticated cyber attack? DHS is finding it difficult to fill the cyber expert positions they have created, much less bring in extra help after a significant attack has occurred.

The second area that the guidelines fail to prioritize is how multiple cyber events will be managed. The cyber incident ESF focuses on what agencies and departments will be stood up, and how they have "established communication procedures" with the other agencies. What is does not consider is how multiple attacks at once would be managed. Are there certain infrastructures that have a higher priority than others? Does it matter if the cyber attack is causing physical damage to parts of critical infrastructure? These questions need to be considered prior to a cyber attack and added to the response plan.

The third area that the cyber incident ESF is overlooking is the fact that "established communication" lines between agencies could be affected by the cyber

96 Federal Emergency Managemnt Agency, "Overview: ESF and Support Annexes Coordinating Federal Assistnace In Support of the National Response Framework," Department of Homeland Security, January 2008, http://www.fema.gov/pdf/emergency/nrf/nrf-overview.pdf, (accessed 10 November 2010), 1.

attack they are responding to. If a cyber attack disabled the infrastructure that the response agencies rely on to communicate, it would seriously undermine any response coordination.

The last area that the cyber incident ESF does not address is how to exert any control over the response to a cyber attack that targets private industry. Cyberspace and critical infrastructure are largely owned and operated by private industry. This again highlights that the federal government and the agencies that will respond to a cyber incident have limited authority over the targets they are trying to protect.[97]

DHS's ESF for cyber incidents is a great start to providing a response effort in the event of a cyber attack. However, until these four areas are addressed with real solutions, there remains a possibility that first responders will not have the communications they need in a disaster recovery effort.

E. RECOVERY

DHS recovery efforts focus on how fast operations can be returned to normal following a disaster. This section will look at DHS communications systems resiliency efforts and compare them to programs and efforts being conducted in the European Union (EU). DHS is focusing on the idea of resilience to protect physical and cyber infrastructure from a destructive attack, a pandemic, or a natural catastrophe, according to the National Security Council (NSC) Directorate for Resilience.[98] In the European Union (EU), resiliency is focused on how to protect public electronic communications from cyber attack and disruptions. Both the United States and the EU have adopted the idea that resilience is the best defense in the future for critical assets. This section will show that the operational effectiveness of DHS's resilience guidelines could be improved by developing methods more applicable at the state and local levels. Additionally, the EU's

---

[97] Federal Emergency Management Agency, "Cyber Incident Annex," Department of Homeland Security, December 2004, http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf, (accessed 10 November 2010), 3.

[98] Spencer S. Hsu, "Obama Integrates Security Councils, Adds New Offices," The Washington Post, 27 May 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052603148.html, (accessed 26 October 2010).

different perspective on resilience is opening avenues and allowing their policies on resilience to become operational at the local and state levels.

DHS conducted a three-phase study in order to build a definition of what resilience will mean to the United States in the future. Phase one, which studied over 100 documents and interviewed 30 plus subject-matter experts, provided the following working definition of critical infrastructure resilience:

> Infrastructure resilience is the ability to reduce the magnitude and /or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon the ability to anticipate, absorb, adapt to, and/or rapidly recover from a potential disruptive event.[99]

DHS identified three objectives within resilience: resistance, absorption, and restoration, and, eight principles of resilience: robustness, threat and hazard limitation, consequences mitigation, adaptability, risk-informed planning and readiness, risk informed investment, harmonization of purpose, and comprehensiveness of scope.[100] These principles provide a comprehensive perspective at the national level; however, they fall short of addressing resilience at the state and local level for their first responder agencies. DHS's top down approach is overlooking areas that subject matter experts in the EU are saying is most important.

Instead of a top down approach, the EU commissioned the European Network and Information Security Agency (ENISA) to enhance the capability of the civilian and government community in order to prevent, address, and respond to network and information security problems.[101] ENISA has six areas of activity: awareness raising, computer emergency response teams, identity and trust, risk management, stakeholder relations, and resilience of local and state public networks and electronic

---

[99] National Infrastructure Advisory Council, "Critical Infrastructure Resilience Final Report and Reccomendations," Natioanl Infrastructure Advisory Council, 8 September 2008. 7–8.

[100] Kahan Jerome, Andrew Allen, Justin George, and George Thompson, "An Operational Framework for Resilience," Journal of Homeland Security and Emergency Management, Vol 6 (1), article 83, 2009, 1–4.

[101] European National Security Agency, "What Does ENSIA Do," ENISA Europe, 2010, http://www.enisa.europa.eu/media/faq-on-enisa/general-faqs-on-enisa, (accessed 26 October 2010).

communications. ENISA's resilience division developed a multi-year program aimed at improving the resilience of public electronic communications networks, which would be used during disaster recovery, from both physical and cyber attacks. They analyzed the 27 member state regulatory policies and how they relate to providing resiliency across the public electronic communication systems used in disaster recovery. ENISA found that the states with specific requirements to secure electronic communications, combined with strong public and private partnerships, have the strongest frameworks for resilience.[102]

The electronic communications resiliency programs working in the EU could meet challenges if adopted in the United States. They all involve high levels of regulation of the providers of electronic communications, audits to ensure compliance, and sectarian and cross-sectarian exercises to evaluate how various providers function during emergencies.[103] Of the 27 states in the EU that belong to ENISA, the three states credited with the most comprehensive best practices are Sweden, Finland, and the Netherlands. These three countries also rank among the top six in the world for perceived level of trust people have for the public sector.[104] There may be a correlation between trust in the public sector and the best practices of detailed regulations, enforced audits, and government led exercises. The same study that placed Sweden, Finland, and the Netherlands in the top 6 placed the United States at 19. In the United States, strict regulations on private-sector electronic communications and periodic audits to enforce these regulations might not be as easily accepted. However, by taking the lessons learned in functional area exercises and applying them to cross-functional exercises, DHS could vastly improve the preparation of the United States first responders, communication outages during disaster recovery efforts.

---

[102] Vangelis Ouzounis "Policy Recommendations Report," European Network and Information Security Agency," 20 February 2009, http://www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations, pp. 99-105, (accessed 26 October 2010).

[103] Vangelis Ouzounis, "Policy Recommendations Report," European Network and Information Security Agency," 20 February 2009, http://www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations, pp. 101-106, (accessed 26 October 2010).

[104] Transparency International, "Corruption Perceptions Index," Transparency International, 2009, http://www.transparency.org/policy_research/surveys_indices/cpi/2009/cpi_2009_table, (accessed 36 October 2010).

F. CONCLUSION

This chapter highlighted DHS's four mission areas of prevent, protect, respond, and recovery with respect to communication systems. Further, it pointed out problems in these areas that could jeopardize the availability of first responder communications during a disaster recovery effort. At all levels of the defense-in-depth strategy being employed by DHS, it does not appear there is enough work force to execute the programs being fielded. There is no centralized authority with regulatory backing across government agencies or buy-in from private industry. Across all mission areas, there are plans and programs that provide guidelines; however, DHS is lacking any tools to follow up on any of these programs. The full consequences and implications of cyber attacks are unknown at this time; therefore, the elements to create deterrence currently do not exist. With more transparency in the future, there would exist the opportunity for diplomatic measures that could reduce cyber attacks; however, it will take time and there are no guarantees. DHS has made improvements in how they respond to disasters; however, similar to the prevention problems, DHS is facing a lack of authority and must overcome private-sector trust issues to become an effective response force. DHS's lack of authority over the areas they are responsible for are hindering their ability to reduce the time it takes to recover from a disaster. Until DHS obtains the work force needed to operate their programs, the authority and cooperation of other government agencies to fully meet its mission requirements, first responder communication systems will likely be vulnerable to a cyber attack that could impair their availability during recovery operations.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NATIONAL EXCERCISE PROGRAM FOR FIRST RESPONDERS

Amateurs practice until they get it right; professionals practice until they can't get it wrong.

—Jeffrey Ramsey, Assistant Fire Chief

A. INTRODUCTION

In February 2010, the first ever Quadrennial Homeland Security Review (QHSR) was delivered to the United States Congress, and identified safeguarding and securing cyberspace as one of the top five homeland security missions.[105] To support this mission, DHS works with owners and operators of critical infrastructure and key resources (CIKR) in the private sector, states, and municipalities to increase their cyber security preparedness, risk assessment and mitigation and incident response capabilities.[106] One of its responsibilities is to lead the National Exercise Plan (NEP).[107] NEP exercises fall into four tiers, with Tier I being directed by the White House. Lessons learned from Tiers II through IV are rolled up to provide scenarios for Tier I exercises. The purpose of these exercises is to improve response capabilities.[108]

This chapter outlines and explains the exercise tier levels in the NEP, and analyzes communication and procedural barriers identified in NEP exercises. The information in this chapter was taken from open source documents on the Internet. For Official Use Only (FOUO) or classified materials were not used. The information that follows is intended to help first responders operate through communications outages

105 Department of Homeland Security, "Quadrennial Homeland Security Review," Department of Homeland Security, February 2010, 29–30.

106 Deparment of Homeland Security, "Cybersecurity: Our Shared Responsibility," Department of Homeland Defense, 29 October 2010, http://www.dhs.gov/files/programs/gc_1158611596104.shtm, (accessed 29 October 2010).

107 Federal Emergency Management Agency, "Preparedness," Federal Emergency Management Agency, 29 October 2010, http://www.fema.gov/prepared/index.shtm, (accessed 29 October 2010).

108 NOTE: Information provided in a DHS standard briefing first given on 8 March 2007 and can be found at, www.fas.org/irp/agency/dhs/nep.ppt, (accessed 29 October 2010).

more efficiently, obtain interoperable communications equipment for disaster recovery efforts, and highlight how current interoperability efforts are making them more vulnerable to cyber attacks.

B. TIER IV

The NEPs Tier IV exercises are focused on state, territorial, local, and tribal governments, and private sector entities.[109] DHS provides local first responders guidance for these exercises. Each year, one Tier IV exercise is elevated to the Tier I level.[110] However, a majority of these exercises are planned, coordinated, and executed at the local level, with little connection to the higher tiered exercises. It also appears these lower level exercises have limited after actions reports, and most are kept in house for local agency use only. While conducting research for this thesis, DHS was unable to provide any information concerning Tier IV exercises or any lessons learned from them. Although, DHS is providing guidance for the exercises, there does not appear to be an effort to consolidate lessons learned. Without such consolidation, first responders are missing the opportunity to share observed best practices, and elevate real-world concerns that need to be addressed at higher-level exercises.

The information that does exist concerning Tier IV exercises suggest there are problems with interagency cooperation, and as at higher levels, the communication equipment has interoperability problems. Michael Fagel, a former New York City firefighter who spent three months working at Ground Zero after 9/11, now works for the Justice Department observing Tier IV exercises around the country.[111] Fagel observed command and control being conducted in some of these exercises by parking the mobile communications base stations of various first responder agencies like fire, police, and

---

[109] R. Eric. Peterson, "Homeland Emergency Preparedness and the National Exercise Program," 10 November 2008, http://www.fas.org/sgp/crs/homesec/RL34737.pdf, 13.

[110] Department of Homeland Security, "National Exercise Program," Department of Homeland Security, 29 October 2010, http://www.dhs.gov/files/training/gc_1179350946764.shtm, (accessed 29 October 2010).

[111] Matthew Brzezinski, *Fortress America: On The Front Lines of Homeland Security* (New York, NY: Bantam Dell, 2005), 147-148.

emergency medical services (EMS) near each other.[112] This was an attempt to facilitate face-to face communication across agencies and highlighted the fact that cross agency communications systems were not interoperable. Fagel's observations were conducted over five years ago; however, there is plenty of evidence that interoperability problems still exist. On October 24, 2010, in Lancaster, Pennsylvania, police officers and firefighters responded to a real-world gas leak at Millersville University. The local news media ran an article the next day stating that first responders could not communicate because their equipment was non-compatible across agencies. The article further explained that this problem was identified 11 years earlier and that $14 million dollars had been spent to fix it.[113] The article pointed out that this is not unique to Millersville University, and in fact, occurs across the county.

In an exercise conducted by the city of Oakland, California, first responders explored how they would conduct recovery efforts to a simulated 6.7 magnitude earthquake.[114] This was the third exercise of its kind and focused primarily on the emergency communications that would be used in a recovery effort. In this scenario, first responders had to simulate that cell and land line telephone communications were unavailable, and use agency radios as the primary means of communication. The scenario split the city into 35 separate neighborhoods for the initial response. Out of the 35 neighborhoods, only 6 reported positive comments on radio communications within their neighborhoods, and all reported some type of radio communications problem.[115] It is important to note that this exercise was pre-planned and all agencies understood radios would be the primary form of communications; nevertheless, radio communications were

---

[112] Matthew Brzezinski, *Fortress America: On The Front Lines of Homeland Security* (New York, NY: Bantam Dell, 2005), 147–148.

[113] Jack, Brubaker, "Radio Static When Police and Firefighters Can't Commuincate,"" Fire Engineering, 24 October 2010, http://www.fireengineering.com/index/articles/Wire_News_Display/1289320962.html, (accessed 30 October 2010).

[114] City of Oakland Respond to Emergencies Program 2007, *City of Oakland Respond to Emergencies After Action Report*, (City of Oakland Mayors Office 2007), 13.

[115] City of Oakland Respond to Emergencies Program 2007, *City of Oakland Respond to Emergencies After Action Report*, (City of Oakland Mayors Office 2007), 18–79.

a problem in most neighborhoods and participants had to resort to runners in order to communicate the locations of fires, gas leaks, and other problems needing attention. This significantly slowed operations. In an actual crisis, such problems could escalate and lead to unnecessary deaths.

The interoperability problems experienced at Millersville University, in the exercises observed by Mr. Fagel, and in Oakland, illustrate a serious problem for first responder disaster recovery efforts. They stem from a lack of centralized coordination and concrete direction on what technologies will work in disaster recovery efforts. DHS publishes the guidance for Tier IV exercises; however, a mechanism to consolidate findings and make changes at higher levels that will eventually resolve some of the communications and other problems encountered is not being used. It appears the people executing these exercises are highly motivated and making progress, but lack the technical expertise and resources needed to establish seamless communications during disaster recovery efforts.

C. TIER III

Tier III NEP exercises appear to be more coordinated than Tier IV, and are scheduled and tracked on a five year basis by DHS. Tier III exercises are federal-level exercises that focus on regional plans, policies and procedures. They do not require broad-level interagency involvement, and participation by national-level assets is determined by each first responder agency. In the event of resource conflict with other exercises, Tier II exercises take precedence.[116] DHS is currently tracking five Tier III exercises; however, only the after-actions reports for two of these exercises were available through open source and only from some of the participating agencies. These two reports appeared professional and comprehensive from their respective agency perspectives.

[116] R. Eric Peterson, "Homeland Emergency Preparedness and the National Exercise Program," 10 November 2008, http://www.fas.org/sgp/crs/homesec/RL34737.pdf, 13.

The first report, titled The Spill of National Significance Exercise (SONS), was conducted in three phases starting June 19, 2007 and ending August 1, 2007.[117] The United States Coast Guard, in conjunction with the United States Environmental Protection Agency, published an after actions report in December 2008 outlining the exercise and key areas that needed to be corrected. SONS '07 tested national-level contingency plans and the nation's first responder's readiness to respond to an oil and hazardous material (HAZMAT) catastrophic event. One of the six objectives of the exercise was to evaluate the effectiveness of the individual agency's notification and communication systems, processes and procedures.[118] Seven of the 24 improvement areas were related to communications between agencies and equipment problems. These seven areas can be consolidated into established communication processes, and communications equipment.[119] The exercise determined that notification processes were not robust and that there was a lack of common procedures across agencies. The command and control function of the exercise, which employed unclassified websites to disseminate information across dispersed agencies, suffered from lack of timeliness and inaccuracies. Depending on the website, this type of communication introduces the vulnerability to cyber attack that could stop or corrupt the information being passed. When agencies experienced communications equipment problems or "comm-outs," no procedures were in place to identify what alternative equipment were to be used.

The second report was related to Golden Guardian. Golden Guardian was a major portion of the NEP's Tier III exercise Vigilant Shield.[120] Golden Guardian was conducted in California, and tested first responder recovery efforts to a simulated 7.8

---

117 Anthony S. Lloyd, *Spill of National Significance Exercise*, (United States Coast Gaurd 2008), ii.

118 Anthony S. Lloyd, *Spill of National Significance Exercise*, (United States Coast Gaurd 2008), ii.

119 Anthony S. Lloyd, *Spill of National Significance Exercise*, (United States Coast Gaurd 2008), 43–53.

120 Matthew Rothschild, "WhatIs NorthCom Up To?," Progressive, 12 November 2008, http://www.progressive.org/mag/wx111208.html, (accessed 30 October 2010).

magnitude earthquake along 270 kilometers of the San Andreas Fault.[121] Prior to this exercise, it was scientifically determined that an earthquake of this magnitude in southern California would produce the following:

> 1,800 fatalities, 48,000 injuries, 1,600 fires, immediate loss of utilities and drinking water in the region, significant infrastructure damage to roads, bridges, and the interstate highways system, 350,000 household displaced, and 213 Billion dollars in economic loss.[122]

The exercise established six objectives of which four were communications focused. The results of the exercise found three areas of communications needing improvement.[123] One report about Golden Guardian pointed out in clear detail that communications needed more work, specifically regarding the testing and additional deployment of land mobile radio systems. Exercise participants noted that cell phones in a catastrophic event will become useless and that interoperable radio systems are a key element in first responder disaster recovery efforts.[124, 125]

Both of the Tier III NEP exercises discussed above had communication procedure and equipment problems. They identified that in disaster recovery efforts it is crucial to establish what procedures and equipment will be used in advance of a disaster. These cases showed that interoperable radio communications will more than likely be used by first responders during a disaster recovery effort. Further, these two exercises highlighted that more radios are needed in some agencies and that alternative government and civilian radio communication systems need to be developed.

---

121 Matthew Bettenhausen, *Golden Guardian After Action Report*, (California Emergency Management Agency, 2008), 8.

122 Matthew Bettenhausen, *Golden Guardian After Action Report*, (California Emergency Management Agency, 2008), 7.

123 Matthew Bettenhausen, *Golden Guardian After Action Report*, (California Emergency Management Agency, 2008), 10.

124 American Red Cross, *Golden Guardian Statewide Disaster Exercise*, (American Red Cross, 13 November 2008), 3–7.

125 Larry Collins, "Ready to Shake?," Fire Rescue Magazine 2008, http://www.firerescuemagazine.com/bonus_content/frm_great_shakeout.html, (accessed 30 October 2010).

D. TIER II

Tier II exercises include executive agencies and focus on strategy, policy and procedural issues that merit priority national and regional federal interagency participation. They can utilize the National Simulation Center, if needed, and the lead executive agency is responsible for the coordination, planning, execution, and evaluation of participants. One Tier II exercise of particular relevance to this thesis is Cyber Storm. To date, DHS has conducted three Cyber Storm exercises.

In the lower two tiers, III and IV, the exercises encountered communication problems; however, in each case, the focus of the exercise was not to attack and take down communications, but simply to get them to work. In contrast, the Tier II exercise Cyber Storm addresses problems that can arise from intentional cyber attacks and how DHS and other agencies would respond to them. [126] One of the key findings in Cyber Storm II was the fact that the cyber and non-cyber communities were intertwined, creating a need to converge and integrate response procedures tailored for physical disasters with those developed for cyber attacks.[127] The report states that cyber attacks and physical attacks have interdependency in most cases.

> Physical and cyber attacks are rarely mutually exclusive. Physical attacks impact cyber infrastructure and cyber disruptions can have severe physical consequences. An "all hazards" approach to incident response could strengthen preparedness and mitigate efforts.[128]

Since Cyber Storm is a simulated exercise conducted in computer labs, there are no physical first responders; therefore, radios are not used in this exercise. During Cyber Storm, communications between agencies are kept on-line and cyber attacks and the

---

[126] Department of Homeland Security, *Cyber Storm II Final Report*, Department of Homland Security, July 2009, 2.

[127] Department of Homeland Security, *Cyber Storm II Final Report*, Department of Homland Security, July 2009, 11, Section 2.

[128] Department of Homeland Security, *Cyber Storm II Final Report*, Department of Homland Security, July 2009, 11, Section 2.3.

affects of those attacks are simulated. Other Tier II NEP exercises like Positive Force 07, Diablo Bravo 08 and Global Lightening 09 also do not employ physical first responders or use radio communications.

At Tier II, there appears to be two distinct disconnects in the NEP overall process and coordination. First, at the two lower levels, problems with established procedures and the interoperability of radios are highlighted repeatedly in the lessons learned. While Tier II exercises appear to address the procedural problems at a strategic level, they fail to address the radio interoperability issue highlighted at the two lower levels. There have been other attempts at the federal level to provide solutions and guidance for Tier III and IV first responder radios; however, because they were made outside the NEP, they will be discussed in a separate section later in this chapter. Second, the observations from Cyber Storm reveals a disconnect in NEPs overall exercise coordination. The NEP was developed with the idea of using lessons learned in one exercise to develop scenarios in other exercises that will help strengthen emergency response capabilities. The fact that Cyber Storm identified the need for integrated physical and cyber attack response procedures highlights the need for cyber attack scenarios to be integrated into operational exercises at all levels.

E. TIER I

Tier I exercises are White House directed, focused on national strategy and policy-related issues, and require federal executive agency participation. There are four quarterly Principle Level Exercises (PLE) and an annual National Level Exercise (NLE). The Federal Emergency Management Agency (FEMA) is the lead planning agency for NEP Tier I exercises, unless the Domestic Readiness Group directs otherwise.[129] The four PLEs are focused on coordination at the Cabinet level, involving principle-level officials in federal agencies and forum based discussions associated with a major disaster

[129] R. Eric. Peterson "Homeland Emergency Preparedness and the National Exercise Program," 10 November 2008, http://www.fas.org/sgp/crs/homesec/RL34737.pdf, 13.

recovery effort.[130] The annual NLE is designed to incorporate lessons learned at Tiers II and III, and is the top first responder exercise to help prepare for catastrophic crises.

The NLE was formerly known as the Top Officials exercise series and was assigned the code named TOPOFF from 2000 through 2008. In 2009, the exercise was re-designated as NLE. Originally, TOPOFF was the responsibility of the Department of Justice. In 2003, the Department of Justice and FEMA began to share the responsibility of sponsoring TOPOFF. By 2005, DHS had been established and TOPOFF sponsorship switched to them and assigned to FEMA for execution. TOPOFF, and now NLE, has been developed to increase the nation's capability to prepare for, prevent, respond to, and recover from large-scale terrorist attacks and natural disasters.[131] However, there appears to be problems in the corrective action process which have not been resolved. According to a recent DHS Inspector General (IG) report, TOPOFF did not have a corrective actions process until 2007.[132] Since 2007, reports from the Department's IG and FEMA have both indicated that the corrective actions program is not fully implemented, recurring themes identified in previous exercises and real-world problems have not been resolved, and top officials rarely participate. Further, these reports indicate that a cyber scenario has not been used in any NLE since TOPOFF II in May 2003.[133, 134] Since then, it appears that DHS has split all cyber scenarios off and they are only conducted during the Tier II Cyber Storm exercise.[135]

---

130 Federal Emergency Management Agency, "Homeland Security Excercise and Evaluation Program," 2008, https://hseep.dhs.gov/support/Newsletter-Winter-2008.pdf, (accessed 30 October 2010).

131 Federal Emergency Management Agency, *FEMA's Implementation of Recommendations from Top Officials,* (Department of Homeland Security September 2010), 1–4.

132 Department of Homeland Security, *DHS Efforts To Address Lessons Learned in the Aftermath of Top Officials,* (Department of Homeland SecurityApril 2009), 6–7.

133 Federal Emergency Management Agency, *FEMA's Implementation of Recommendations from Top Officials,* (Department of Homeland Security September 2010), 4.

134 Department of Homeland Security, *DHS Efforts To Address Lessons Learned in the Aftermath of Top Officials,* (Department of Homeland SecurityApril 2009), 6–14.

135 Department of Homeland Security, *National Cyber Security Division Cyber Exercise Program,* (US Computer Emergency Response Team 2010), (accessed 8 November 2010).

Until DHS finds a better method to roll-up the lessons learned at lower-level exercises into NLEs, and employs a comprehensive corrective actions program, progress to resolve first responders' problems will remain slow. It appears that DHS, FEMA and other first responders are working very hard to prepare for a disaster; however, there are still significant barriers hindering their progress. After 10 years of preparedness exercises, the system for corrective actions has no regulatory teeth and is being ignored. Although Congress requires top officials to fully participate in Tier I exercises, it is rarely done.

F. RADIO INTEROPERABILITY

At the highest level of the NEP exercises, there appears to be a lack of support and regulatory teeth behind the annual NLE. As a result, the same problems resurface in exercise and real-world events year after year. Since the focus of this thesis is on first responders operating through a cyber attack, it is necessary to understand the issues around radio interoperability and why after being identified in 9/11, and again in Hurricane Katrina, the problems have not been resolved.

When multiple agencies respond to a disaster recovery effort, interoperable communications systems have been and remain an issue of great concern.[136] In an article presented in *Government Security News*, David Boyd, the Director of Command, Control and Interoperability Division in DHS, points out that budgets and planning cycles are pushing the different emergency responders to have different legacy communications systems. [137]

136 Mark Protacio, "National Emergency Response Interoperability Framework and Resilient Commuincation System of Systems," Department of Homeland Security, February 2009, http://www.dhs.gov/xlibrary/assets/st_national_emergency_response_ord.pdf, (accessed 23 October 2010), 3.

137 Jacob Goodwin, "Experts Call for Wider Testing of P25 Land Mobile Radios," Government Security News, 30 May 2010, http://www.gsnmagazine.com/article/20809/experts_call_wider_testing_p25_land_mobile_radios, (accessed 23 October 2010).

> David Boyd, Director of the Command, Control and Interoperability Division of the Science and Technology Directorate within DHS, pointed out that there are more than 50,000 different emergency response agencies in the United States and that each one has its own legacy communication system and its own budgeting and planning cycles.

These communications range from databases of information that employ specialized software to operate, to basic radio communications first responders use to communicate during contingencies. The interoperability of databases and systems used are highly susceptible to cyber attack, but what about radio communications? Unfortunately, the solutions currently being deployed to provide radio networks interoperability lack specific technical specifications and increase the vulnerability of these communications to cyber attack.

The interoperability problems stem from two issues. First, the equipment first responders use is driven by funding and the upgrade life cycle of the equipment rather than a well-formulated standard and plan for deployment. There is a federal radio standard in place, the Project 25 (P25); however, experts are finding that it is actually hindering the progress of seamless interoperability.[138] Further, there are four areas where the new P25 standard is falling short, according to Derek Orr, program manager for public safety communications systems at the National Institute of Standards and Technology (NIST).[139] First, the standard is not clear about the eight interfaces needed to make radios interoperable. Second, only a portion of the P25 radios being manufactured are actually living up to the standard. Third, many of the first responder agencies do not have the technical expertise to understand the P25 standard requirements.

---

138 Jacob Goodwin, "Experts Call for Wider Testing of P25 Land Mobile Radios," Government Security News, 30 May 2010, http://www.gsnmagazine.com/article/20809/experts_call_wider_testing_p25_land_mobile_radios, (accessed 23 October 2010).

139 Jacob Goodwin, "Experts Call for Wider Testing of P25 Land Mobile Radios," Government Security News, 30 May 2010, http://www.gsnmagazine.com/article/20809/experts_call_wider_testing_p25_land_mobile_radios, (accessed 23 October 2010).

Last, the industry lacks a formal compliance assessment program to ensure radios are meeting the standard. Although these radios are proving to not be interoperable, first responders are mandated to spend federal funds to purchase them.

The second concern regarding first responders' radio interoperability issues is the fact that they use different frequencies. The warning from a New York City police helicopter during 9/11 that the second tower was about to collapse missed many of the emergency responder radios because they were on different frequencies, highlighting the problem with first responder communications.[140] Nine years after 9/11, first responders continue to experience the inability to talk across radio networks due to frequency differences.

The solution many state, local, and even federal first responders are using to solve the interoperability problems is to employ gateways and connect over Internet Protocol (IP) networks. In this way, first responders working the same disaster recovery effort with different radios can talk, assuming the gateways and patches are properly employed. Several companies produce and sell these gateways, allowing radios systems from different manufacturers running on different frequencies to talk. Figure 2 is a diagram of how first responders using radios from different manufacturers with different frequencies might communicate during a disaster recovery effort.

[140] Ed Timmis, and Tanya Eiserer, "Despite Technology, First Responders Operating on Different Frequencies," Police One, 4 July 2009, http://www.policeone.com/police-products/communications/articles/1852711-Despite-technology-first-responders-operating-on-different-frequencies/, (accessed 23 October 2010).

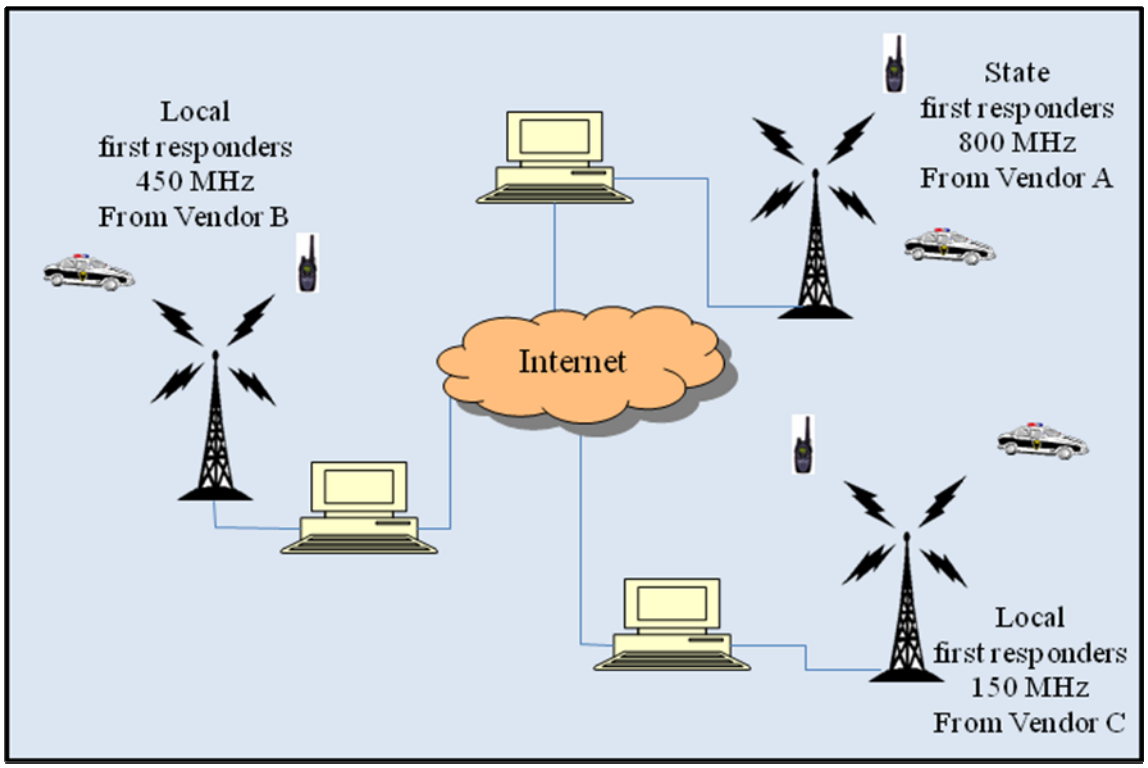

Figure 2. First Responder Radio Network Example

Local and state first responders are finding that these systems are technically challenging to install and configure, and need to be exercised prior to a disaster recovery effort. With many agencies involved in a first responder disaster recovery effort, it is near impossible to exercise all possible options prior to a recovery effort. Also, if the links to the dispatch centers are cut during the recovery effort or repeater towers are destroyed, first responders lose radio communications across different systems. Further, these solutions are providing an open door to cyber attacks. To connect the separate systems, they must be patched together through a dispatch center. Dispatch centers are connected to radio towers and other dispatch centers through the Internet, making these systems vulnerable to cyber attacks discussed earlier.

G. CONCLUSION

This chapter outlined how DHS uses the NEP to help meet its mission to build an integrated, interagency federal, state, territorial, local, and private sector capability to prevent terrorist attacks, and respond to and recover from terrorist attacks and major disasters.[141] Further, this chapter explained the four-tier approach DHS uses to coordinate, plan, and execute exercises across first responder agencies at all levels of government and the private sector. The cases discussed in this chapter identified that first responders at all levels are working hard to prepare for a disaster; however there are still many barriers to overcome and work to be done before these agencies are integrated seamlessly during operation-oriented exercises and real-world events.

[141] Federal Emergency Management Agency, *FEMA's Implementation of Recommendations from Top Officials,* (Department of Homeland Security September 2010), 4.

Table 1 highlights the findings from the cases studied at each of the tier levels in the NEP.

NEP Tier	Findings	Comments
I	Corrective actions program not implemented properly.	DHS has no mechanism to get first responder agencies to correct weaknesses found during exercises or real-world events. Problem identified in previous exercises are not being corrected and are recurring.
	Top officials rarely participate.	Congress mandates top officials participate in Tier I exercises; however, this is rare.
II	Radio interoperability problem not being looked at strategically in the NEP.	Radio interoperability was identified in Tier III and IV exercises. Tier II exercises could take a strategic look at this problem.
	Physical and cyber attacks are usually interdependent.	Cyber scenarios have only been included in operational based NLEs only once in ten years, in 2003.
III	More radios are needed at the state and local level for first responders.	More radios, and the training to use them needs to be considered. Interoperability is at Tier III as well.
	No backup or alternative systems identified when communications equipment fails.	Communication systems were expected to just work, and when they did not, agencies operated slower.
	Unclassified websites were employed to communicate with agencies.	This introduces the possibility of cyber attacks and assumes the Internet will be available.
IV	Lack of synchronization among agencies and other exercises.	Lessons learned and best practices are not readily shared across the United States

	Radio malfunctioning and interoperability problems.	Agencies operate radios on different frequencies and with incompatible equipment. Lack of technical expertise to program radios.
	Money being spent to provide radio interoperability is costly.	Agencies are throwing money at the problem without standards and guidance. Interoperability across first responders needs a strategic approach with concrete standards and methods.

Table 1. National Exercise Plan (NEP) Communication Findings

This chapter focused on the communications equipment and procedures problems that arose across tiers and agencies during NEP exercises. It highlighted in DHS's Cyber Storm scenarios that cyber attacks and physical attacks are rarely separate events and are normally interdependent. The NEP has conducted a cyber attack scenario only once in 10 years at an operational based NLE. With the lingering radio interoperability problem, and the increase in cyber attacks on communication systems, it is highly likely that first responders will experience failed communications during real-world operations. DHS's lack of authority to get first responders to follow up on corrective actions is providing a framework that is keeping the communications scenarios in major exercises from progressing. Even if first responders deploy gateways and dispatch radio networks together, it would be easy for an adversary to take these systems down with a cyber attack. This highlights the fact that communications could drop during real-world disaster recovery efforts. This problem will not be resolved in the near future, and practicing how operations would flow during "comm-outs" needs to become a reality. DHS should employ "comm-out" portions to their operational exercises to prepare first responders for recovery efforts. Further, employing cyber attack or "comm-out" scenarios would allow first responders to build contingency plans and understand how a "comm-out" could affect their operation. Current NEP exercises appear to make first responders look like they are practicing to get it right versus employing strategies and scenarios that will prepare them not to fail.

V. CONCLUSION

A. SUMMARY

Using a case study analysis, this thesis explored how prepared first responders are when communication systems are interrupted during a disaster recovery effort. It showed that cyber attacks used to disrupt communications systems are difficult at best to defend and even the best-defended systems are vulnerable to cyber attack. In addition, it highlighted that current efforts to improve first responder communication systems are actually making them more vulnerable to cyber attack. Moreover, current first responder exercises separate out the physical and cyber portions of operations, making it difficult for first responders to train and understand how they would operate if one of their communications systems was attacked and disrupted. By not practicing communication outages during operation exercises, first responders could be introducing confusion into a real-world disaster recovery effort.

Adding communication outages to first responder exercises would allow DHS to gain insight on the effects communication outages could have on a recovery operation. This insight would help develop better contingency plans for first responders that will yield improvements in DHS's four mission areas. Communication outages during exercises would create awareness for first responders that would help them prevent attacks, better protect the systems they use from attack, respond quicker when a system is lost, and recover faster in a real-world event. Currently, communications for first responder operations appear to be taken for granted, and the assumption is that there will be no disruptions. DHS does conduct cyber exercises; however, only the cyber personnel are involved, and the exercises overlook first responders who are operating on the front line of a disaster. Historical experience has shown that communications have been a problem during recovery efforts; however, DHS does not appear to involve

communication outage scenarios to their exercises. Further research is needed to look at the specific systems used across agencies and identify what agencies are most vulnerable to communication outages. This would help DHS prioritize their resources and help the areas most in need.

BIBLIOGRAPHY

Abraham, Peter. "The Slammer Worm Attack: The Worst Attack To Date, Probably Not The Last." *Dynamic Net.* February 14, 2003. http://www.dynamicnet.net/news/articles/slammer.html (accessed August 10, 2010).

Agence France-Press. "Inquirer." *Technology Inquirer.* December 5, 2007. http://technology.inquirer.net/infotech/infotech/view/20071205-105061/Saudi_forum_urges_global_cyber-terrorism_ban_ (accessed August 3, 2010).

Antidze, Margarita. "Door to NATO Still Open for Georgia." *Reuters.* October 1, 2010. http://in.reuters.com/article/idINIndia-51883420101001 (accessed October 5, 2010).

Arnold, Chloe. "Russian Group's Claims Reopen Debate On Estonian Cyber Attacks." *Radio Free Europe.* March 30, 2009. http://www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html (accessed October 5, 2010).

Arquilla, John, and David Ronfeldt. *Networks and Netwars: The future of terror, crime, and militancy.* Santa Monica: RAND, 2001.

Australian Attorney General. *Cyber Storm II Final Report.* Final Report and Findings, Security and Critical Infastructure Division, Australian Government, 2008.

Baxter, Sarah, Michael Sheridan, and Uzi Mahnaimi. "Israelis Blew Apart Syrian Nuclear Cache." *The Times Online.* September 16, 2007. http://www.timesonline.co.uk/tol/news/world/middle_east/article2461421.ece (accessed October 5, 2010).

BBC News. "Heavy Fighting in South Ossetia." *BBC News.* August 8, 2008. http://news.bbc.co.uk/2/hi/europe/7546639.stm (accessed October 22, 2010).

Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War?" *informaworld.* May 1, 2008. http://www.informaworld.com/smpp/section?content=a795001836&fulltext=713240928 (accessed August 17, 2010).

Brubaker, Jack. "Wire News Display." *Fire Engineering.* October 24, 2010. http://www.fireengineering.com/index/articles/Wire_News_Display/1289320962.html (accessed 2010 30, 2010).

Bureau of European and Eurasian Affairs. *United States Department of State.* March 17, 2010. http://www.state.gov/r/pa/ei/bgn/5377.htm (accessed August 17, 2010).

Buxbaum, Peter. "Air Force Explores the New Frontier." *Government Computer News.* Feburary 17, 2007. http://gcn.com/articles/2007/02/17/air-force-explores-the-next-frontier.aspx (accessed May 23, 2010).

Campman, Allen, Douglas Dearth and Thomas Goodden. *Cyberwar: Security, Strategy, and Conflict in the Information Age.* Fairfax Virginia: AFCEA International Press, 1996.

Chabrow, Eric. "Government Information Security Articles." *Government Info Security.* November 17, 2009. http://www.govinfosecurity.com/articles.php?art_id=1946 (accessed November 10, 2010).

Cilluffo, Frank. "Security Affairs." *Cyber Strategy 2.0.* Spring 2006. www.securityaffairs.org/issues/2006/10/cilluggo_nicholas.php (accessed November 2009).

Claburn, Thomas. "CIA Admits Cyberattacks Blacked Out Cities." *Information Week.* January 18, 2008. http://www.informationweek.com/news/Internet/showArticle.jhtml?articleID=205901631 (accessed June 9, 2010).

Clarke, Richard A., and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it.* New York: Harper-Collins, 2010.

CNN Tech. "Epic Cyber Attack Reveals Cracks in United States Defense." *CNN Tech.* May 10, 2001. http://articles.cnn.com/2001-05-10/tech/3.year.cyberattack.idg_1_moonlight-maze-hackers-russian-Internet-addresses?_s=PM:TECH (accessed March 17, 2010).

Coleman, Kevin. "Satellites Could Come Under Cyber Siege." *Defense Systems.* September 22, 2010. http://www.defensesystems.com/Articles/2010/09/02/Digital-Conflict-Cyber-Threat-to-Satellites.aspx (accessed October 23, 2010).

Computer Economics. "Malicious Code Attacks Had $13.2 Billion Economic Impact in 2001." *Computer Economics: Metrics for IT Managers.* September 2002. http://www.computereconomics.com/article.cfm?id=133 (accessed September 18, 2010).

Creery, A. "Industrial Cybersecurity for Power System and SCADA Networks." *Andritz Automation.* http://www.andritzautomation.com/documents/industrialcybersecurity.pdf (accessed August 10, 2010).

Davis, Joshua. *Wired Magazine.* July 21, 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia (accessed August 17, 2010).

Davis, Tom. *A Failure of Initiative: The final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina.* Investigation, Select Bipartisan Committee to Investigate the Preparation for the Response to Hurricane Katrina, Washington D.C.: United States Government Printing Office, 2006.

Dearth, Douglas H. "Rethinking the Application of Power in the 21st Centruy." *Federation of American Scientist.* http://www.fas.org/irp/agency/army/mipb/1997-1/dearth.htm (accessed May 30, 2010).

Denning, Dorothy E. "Hacktivism: An Emerging Threat to Diplomacy." *American Foreign Service Association.* 2000. http://www.afsa.org/fsj/sept00/Denning.cfm (accessed June 7, 2010).

Department of Homeland Security. *Department of Homeland Security.* 2007. http://www.northcom.mil/news/2007/as-07_fact_sheet.pdf (accessed May 25, 2010).

———. "Cyber Storm II Final Report." *Department of Homeland Security*. july 2009. http://www.dhs.gov/files/training/gc_1204738760400.shtm (accessed April 10, 2010).

———. "Fact Sheet: Cyber Storm Exercise." *Department of Homeland Security*. September 13, 2006. http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm (accessed April 10, 2010).

———. "Homeland Security Directive 8: National Preparedness." *Department of Homeland Security.* December 17, 2003. http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm (accessed November 9, 2010).

Dietrich, David Dittrich and Sven. "Command and Control Structures in Malware." *USENIX*. December 6, 2007. http://www.usenix.org/publications/login/2007-12/openpdfs/dittrich.pdf (accessed October 5, 2010).

Dougherty, Michelle. "The 10 Security Domains." *Library of Ahima.* February 2004. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_046425.hcsp?dDocName=bok1_046425 (accessed October 20, 2010).

EC-Council. *Ethical Hacking and Countermeasures Training Program.* Albuquerque: EC-Council, 2010.

Eiserer, Ed Timms and Tanya. “Despite Technology, First Responders Operating on Different Frequencies.” *Police One.* July 4, 2009. http://www.policeone.com/police-products/communications/articles/1852711-Despite-technology-first-responders-operating-on-different-frequencies/ (accessed October 23 , 2010).

ENISA. http://www.enisa.europa.eu/media/faq-on-enisa/general-faqs-on-enisa, (accessed 26 October 2010).

Espiner, Tom. “UK’s Special Coverage on Security.” *Zdnet.* October 14, 2010. http://www.zdnet.co.uk/news/security-threats/2010/10/14/chertoff-advocates-cyber-cold-war-40090538/ (accessed November 10, 2010).

European National Security Agency. “What is ENSIA.” *ENSIA Europe.* 2010. http://www.enisa.europa.eu/media/faq-on-enisa/general-faqs-on-enisa (accessed October 26, 2010).

European National Security Agency. “What Does European Network and Information Security Agency Do.” European Network and Information Security Agency Europe. 2010.

Federal Emergency Management Agency. “National Preparedness Directorate .” *FEMA.* August 11, 2010. http://www.fema.gov/media/fact_sheets/npd.shtm (accessed November 9, 2010).

———. “National Response Framework.” *FEMA.* December 2004. http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf (accessed November 10, 2010).

Federal Emergency Management Agency. *FEMA’s Implementation of Recommendations from Top Officials.* (Department of Homeland Security September 2010), p. 4.

Fox News. “Is a Cyber Attack Targeting Iran’s Nuclear Plant.” *Fox news.* September 23, 2010. http://www.foxnews.com/scitech/2010/09/23/stuxnet-cyberattack-targeting-irans-nuclear-plant/print# (accessed September 23, 2010).

Fox, Stuart. “Viruses are Winning: Malware Threat Outpaces Antivirus Software.” *Tech News Daily.* August 2, 2010. http://www.technewsdaily.com/malware-computer-viruses-challenge-firewall-antivirus-protection-0918/ (accessed October 20, 2010).

Free Developers Handbook. “FreeBSD Developers Handbook.” *FreeBSD.* 2010. http://www.freebsd.org/doc/en/books/developers-handbook/ (accessed October 16, 2010).

Fulghum, David A., Robert Wall and Amy Butler. “Israel Shows Electronic Prowess.” *Aviation Week.* November 25, 2007. http://www.aviationweek.com/aw/generic/story.jsp?id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess&channel=defense (accessed August 10, 2010).

Gasparre, Richard B. “The Israeli ‘E-tack’ on Syria.” *Air Force Technology.* March 10, 2008. http://www.airforce-technology.com/features/feature1625/ (accessed October 5, 2010).

Gershwin, Lawrence K. “Statement for the Record: Cyber Threat Trends.” *Central Intellegence Agency.* June 21, 2001. https://www.cia.gov/news-information/speeches-testimony/2001/gershwin_speech_06222001.html (accessed June 9, 2010).

Goodwin, Jacob. “Experts Call for Wider Testing of P25 Land Mobile Radios.” *Government Security News.* May 30, 2010. http://www.gsnmagazine.com/article/20809/experts_call_wider_testing_p25_land_mobile_radios (accessed October 23, 2010).

Gorman, Siobhan. “Electricity Grid in United States Penetrated by Spies.” *Wall Street Journal* . April 9, 2009. http://online.wsj.com/article/SB123914805204099085.html (accessed May 23, 2010).

———. “Poolitics Politics? and Policy.” *Wall Street Journal.* June 16, 2010. http://online.wsj.com/article/SB10001424052748703280004575309243039061152.html (accessed November 10, 2010).

Greenemeir, Larry. “Quick, Encrypt Everything.” *Information Week.* September 22, 2006. http://www.informationweek.com/blog/main/archives/2006/09/quick_encrypt_e.html;jsessionid=ST4F0EOU3AGVBQE1GHPSKHWATMY32JVN?cid=iwkPrintURL (accessed October 20, 2010).

Gregory, Lawrence Miller and PeterH. *CISSP for Dummies.* Hoboken: Wiley, 2010.

Griffith, Samuel B. *Sun Tzu: The Art of War.* Oxford: Oxford University Press, 1963.

Harris, Shon. *All in One CISSP Exam Guide: Fifth Edition.* New York: McGraw Hill, 2010.

Heickero, Roland. *Emerging Cyber Threats and Rissian Views on Information Warfare and Information Operations.* Stockholm: FOI, Swedish Defence Research Agency, 2010.

Hobsbawn, Eric. “Nationalism.” In *Essential Readings in Comparative Politics*, by Patrick H. O’Niel, O’Neil? 69–76. London: W.W. Norton & Company, 2010.

Hoffman, David E. “United States news from the Washington Post.” *MSNBC.* Febuary 26, 2004. http://www.msnbc.msn.com/id/4394002 (accessed June 9, 2010).

House Budget Committe Staff. “House Budget Committee.” *House Budget.* February 19, 2004. http://budget.house.gov/doc-library/2004/longterm_cuts.pdf (accessed October 23, 2010).

Hower, Rick. “Software QA and Testing Frequently-Asked-Questions.” *Software QA Test.* June 9, 2010. http://www.softwareqatest.com/qatfaq1.html#FAQ1_3 (accessed June 9, 2010).

Hsu, Spencer S. “Obama Integrates Security Councils, Adds New Offices.” *The Washington Post.* May 27, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052603148.html (accessed October 26, 2010).

Hutchinson, Kay Bailey. *Kay Bailey Hutchison United States Senator.* May 21, 2010. http://hutchison.senate.gov/govsites.html.

Intel Coorporation. “Intel Executive Biography.” *Intel.* 2010. http://www.intel.com/pressroom/kits/bios/moore.htm?iid=tech_mooreslaw+body_bio (accessed October 16, 2010).

Kahan, Jerome, Andrew Allen, Justin George, and George Thompson. “An Operational Framework for Resilience.” *Journal of Homeland Security and Emergency Management* 6 (1) (August 2009).

Koontz, Linda. *First Responders: Much Work Temains to Improve Communications Interoperability.* Report to Congressional Requesters, Washington D.C.: Government Accountability Office, 2007.

Kreke, Bryan. *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* Prepared for congressional review commission, Information Systems Sector, McLean: Northrop Grumman Corporation, 2009.

Kurzweil, Ray. “The Law of Accelerated Returns.” *kurzweilAI.net.* March 7, 2001. http://www.kurzweilai.net/articles/art0134.html?printable=1 (accessed November 16, 2009).

LaMonica, Martin. “Spies hacked into the United States electrical grid.” *CNET News.* April 8, 2009. http://news.cnet.com/8301-11128_3-10214898-54.html (accessed May 23, 2010).

Landsman, Andrew. “The Five Phase Approach of Malicious Hackers.” *Network Security Consulting Blog.* May 8, 2009. http://blog.emagined.com/2009/05/08/the-five-phase-approach-of-malicious-hackers/ (accessed July 7, 2010).

LeClare, Phil. “One Billion PCs In Use By The End of 2008.” *Forrester Research.* june 11, 2007. http://www.forrester.com/ER/Press/Release/0,1769,1151,00.html (accessed October 16, 2010).

Lee, Maria S. “Universal Core Advances Information Sharing Across Agencies.” *Mitre.* November 2009. http://www.mitre.org/news/digest/defense_intelligence/11_09/universal.html (accessed Feburary 14, 2010).

Lewis, Brian C. “Information Warefare.” *Federation of American Scientist.* http://www.fas.org/irp/eprint/snyder/infowarfare.htm (accessed November 5, 2009).

Manning, Ronnie. “Phishing Activity Trends.” *Antiphishing.* 2010. http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf (accessed October 16, 2010).

Markoff, John. “Before the Gunfire, Cyberattacks.” *New York Times.* August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&ref=europe (accessed Octobober 5, 2010).

Marks, Paul. “Why the Stuxnet Worm is Like Nothing Seen Before.” *News Science.* October 12, 2010. http://www.newscientist.com/article/dn19504-why-the-stuxnet-worm-is-like-nothing-seen-before.html (accessed October 22, 2010).

McAfee. “Operation Aurora.” *McAfee.* January 14, 2010. http://www.mcafee.com/us/threat_center/operation_aurora.html (accessed October 22, 2010).

Marsan, Carolyn Duffy. “Security.” *Network World.* Februrary 11, 2010. http://www.networkworld.com/news/2010/021110-cybersecurity-einstein-2.html (accessed November 10, 2010).

Miles, Donna. “Department of Defense News.” May 10, 2006. http://www.defenselink.mil/news/newsarticle.aspx?id=15807 (accessed November 16, 2009).

Montalbano, Elizabeth. “Government.” *Information Week.* February 17, 2010. http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=222900723 (accessed November 10, 2010).

Moore, David, Vern Paxson, Stephan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver. “Inside the Slammer Worm.” *University of California San Diego.* 2003. http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf (accessed October 17, 2010).

Moore, David. “CAIDA Analysis of Code-Red.” *The Cooperate Association for Internet Data Analysis.* July 24, 2001. http://www.caida.org/research/security/code-red/#background (accessed October 1, 2010).

———. “The Spread of the Slammer Worm.” *The Coorporate Association for Internet Data Analysis.* 2003. http://www.caida.org/publications/papers/2003/sapphire/ (accessed October 1, 2010).

National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations.* Report to the President, Washington D.C.: National Infrastructure Advisory Council, 2009.

National Security Agency. “Defense in Depth.” *National Security Agency.* 2000. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed October 23, 2010).

New York Times. “Mikheil Saakashvili.” *New York Times.* June 2, 2010. http://topics.nytimes.com/top/reference/timestopics/people/s/mikheil_saakashvili/index.html (accessed June 6, 2010).

Obama, BaracK. “Whitehouse Speaches and Remarks.” *White House.* May 29, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed September 13, 2010).

Ouzounis, Vangelis, Dr. “Policy Recommendations Report.” European Network and Information Security Agency,” 20 February 2009, http://www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations, pp. 101-106, (accessed 26 October 2010).

Paget, Francois. “McAfee Labs.” *McAfee.* July 7, 2010. http://blogs.mcafee.com/mcafee-labs/malware-at-midyear-a-summary (accessed October 20, 2010).

Paquette, Jeremy. “A History of Viruses.” *Symantec.* July 16, 2000. http://www.symantec.com/connect/articles/history-viruses (accessed September 18, 2010).

Paret, Michael Howard and Peter. *Carl von Clausewitz: On War.* New Jersey: Princeton University Press, 1976.

Peterson, R. Eric. *Homeland Emergency Preparedness and the National Exercise Program.* CRS Report for Congress, Washington D.C.: Congressional Research Service, 2008.

Pittman, Elaine. "Cities Implement First Responders' Fee for Nonresidents to Fill Budget Gaps." *Emergency Management.* July 12, 2010. http://www.emergencymgmt.com/grants/Cities-Implement-First-Responders-Fee.html (accessed Ocotober 23, 2010).

Poulsen, Kevin. "Microsoft: Closed source is more secure." *Security Focus.* April 12, 2001. http://www.securityfocus.com/news/191 (accessed June 10, 2010).

Protacio, Mark. "National Emergency Response Interoperability Framework and Resilient Commuincation System of Systems." *Department of Homeland Security.* February 2009. http://www.dhs.gov/xlibrary/assets/st_national_emergency_response_ord.pdf (accessed October 23, 2010).

Reuters. "Computer viruses number growing extraordinarily." *World Bulletin.* April 14, 2009. http://www.worldbulletin.net/news_detail.php?id=40042 (accessed June 7, 2010).

Rice, David. *Geekonomics: The real cost of insecure software.* Boston: Pearson Education, 2008.

Rothschild, Matthew. "What is NorthCom up To?" *Progressive.* November 12, 2008. http://www.progressive.org/mag/wx111208.html (accessed October 30, 2010).

Salsabil. "Saudi forum urges global cyber-terrorism ban." *Dark Web Forum Portal.* December 7, 2007. http://128.196.239.42/portal/Thread?f=IslamicAwakening&t=8306&page=0&hlKeys=cyber+terrorism (accessed August 3, 2010).

Sayer, Bonnie. "The Falcon and The Snowman." *Epinions.* September 30, 2001. http://www99.epinions.com/review/mvie_mu-1007016/content_42021654148 (accessed October 1, 2010).

Search Security. "Distributed Denial-Of Service Attack." *Search Security Definitions.* 2010. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html (accessed October 22, 2010).

Seguin, Steve. “Russian Hackers Continue Attack on Georgia.” *Tom’s Hardware.* August 12, 2008. http://www.tomshardware.com/news/Russian-Hackers-Georgia,6116.html (accessed October 22, 2010).

Sheridan, Dann. “Asymmetric Warfare: An Overview.” *Radioweblogs.* July 1, 2003. http://radio-weblogs.com/0001134/stories/2003/01/11/asymmetricWarfareAnOverview.html (accessed May 6, 2010).

Sokes, Mark A. “China’s Strategic Modernization: Implecations for the United States.” *United States Army War College.* 1 September, 1999. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=74 (accessed May 13, 2010).

Stiennon, Richard. *Surviving Cyber War.* Toronto: The Scarecrow Press, 2010.

Techterms. “Malware.” *Techterms.com.* http://www.techterms.com/definition/malware (accessed September 18, 2010).

Teufel, Hugo. “Privacy Impact Assessment.” *Department of homeland Security.* May 19, 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf (accessed November 10, 2010).

Tikk, Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm and Liis Vihul. “Cyber Attacks Against Georgia: Legal Lessons Identified.” *United States Army War College.* November 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (accessed May 6, 2010).

Tractenberg, Marc. *History & Strategy.* Princeton: Princeton University press, 1991.

United States Department of Defense. *Information Operations Roadmap.* Information Operations Roadmap for the Department of Defense, Washington DC: Department of Defense, 2003.

Transparency International,. *Corruption Perception Index* . 2009. http://www.transparency.org/policy_research/surveys_indices/cpi/2009/cpi_2009_table (accessed October 26, 2010).

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *Guardian.* May 17, 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed October 22, 2010).

United States Department of Defense. *Information Operations Roadmap.* Information Operations Roadmap for the Department of Defense, Washington DC: Department of Defense, 2003.

United States Computer Emergency Response Team. “Evaluation Report.” *Whitehouse.gov.* June 4, 2008. http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2008_TIC_SOC_EvaluationReport.pdf (accessed November 10, 2010).

USNORTHCOM. “Fact Sheet - Exersize Ardent Sentry - Northern Edge 07.” *Northcom.* April 30, 2007. http://www.northcom.mil/news/2007/as-07_fact_sheet.pdf (accessed May 23, 2010).

Ventre, Daniel. “China’s Strategy for Information Warfare: A Focus on Energy.” *Journal of Energy Security.* May 18, 2010. http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361 (accessed May 22, 2010).

Vijayan, Jaikumar. “Training Needed to Halt ‘Spear-Phishing’ Attacks.” *Computerworld.* August 22, 2005. http://www.computerworld.com/s/article/104087/Training_Needed_to_Halt_Spear_Phishing_Attacks (accessed October 16, 2010).

Weiss, Joe. “Assuring Industrial Control System Cyber Security.” *Center for Strategic & International Studies.* August 25, 2008. http://csis.org/publication/assuring-industrial-control-system-ics-cyber-security (accessed May 6, 2010).

Zakon, Robert. *Zakon.org.* http://www.zakon.org/robert/Internet/timeline/ (accessed June 7, 2010).

Wilson, Clay. “Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.” *Federation of American Scientist.* October 17, 2003. http://www.fas.org/irp/crs/RL32114.pdf (accessed October 17, 2010).

Worth, Robert F. “Their Space.” *New York Times.* June 25, 2006. http://www.nytimes.com/2006/06/25/books/review/25worth.html (accessed August 3, 2010).

Ygaber. “What are the benefits of the Internet.” *Dark Web Forum Portal.* February 26, 2008. http://128.196.239.42/portal/Thread?f=Alsayra&t=72572&page=0&hlKeys=cyber+ (accessed August 3, 2010).

Zakon, Robert. *Zakon.org.* http://www.zakon.org/robert/Internet/timeline/ (accessed June 7, 2010).

Zetter, Kim. “Google Hack Attack Was Ultra Sophisticated, New Details Show.” *Wired.* January 14, 2010. http://www.wired.com/threatlevel/2010/01/operation-aurora/ (accessed October 22, 2010).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. AFIT/ENEL
   ATTENTION: Capt James Ray or Ms. Kristy Aler
   Wright-Patterson AFB, Ohio

4. Professor Dorothy Denning
   Naval Postgraduate School
   Monterey, California

5. Professor Eric J. Dahl
   Naval Postgraduate School
   Monterey California

6. Professor Harold Trinkunas
   Naval Postgraduate School
   Monterey California