NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ACTIVE CYBER DEFENSE: ENHANCING NATIONAL CYBER DEFENSE

by

Tiong Pern Wong

December 2011

Thesis Advisor:	Dorothy Denning
Second Reader:	John Arquilla

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE ACTIVE CYBER DEFENSE: ENHANCING NATIONAL CYBER DEFENSE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Tiong Pern Wong	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT (maximum 200 words)

With increased dependency on the Internet, cyber attacks are fast becoming an attractive option for state adversaries, in part because of the ease of hiding one's identity. In response, governments around the world are taking measures to improve their national cyber defenses. However, these defenses, which are generally passive in nature, have been insufficient to address the threat. This thesis explores the possibility of employing active cyber defenses to improve cyber defenses at the national level. Active cyber defense refers to the use of offensive actions, such as counter hacking, pre-emptive hacking, etc., to defend against cyber attacks. This thesis studies the typologies of active cyber defense and examines how this approach can enhance a state's cyber defense posture.

14. SUBJECT TERMS Active cyber defense, Passive cyber defense, Cyber attack, GhostNet, Stuxnet, Estonia, Computer malware	**15. NUMBER OF PAGES** 75
	16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

ACTIVE CYBER DEFENSE: ENHANCING NATIONAL CYBER DEFENSE

Tiong Pern Wong
Singapore Ministry of Defense, Civilian
B.S., University of San Francisco, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN JOINT INFORMATION OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Tiong Pern Wong

Approved by: Dr. Dorothy Denning
Thesis Advisor

Dr. John Arquilla
Second Reader

Dr. John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

With increased dependency on the Internet, cyber attacks are fast becoming an attractive option for state adversaries, in part because of the ease of hiding a perpetrator’s identity. In response, governments around the world are taking measures to improve their national cyber defenses. However, these defenses, which are generally passive in nature, have been insufficient to address the threats. This thesis explores the possibility of employing active cyber defenses to improve cyber defenses at the national level. Active cyber defense refers to the use of offensive actions, such as counter hacking and pre-emptive hacking, among others, to defend against cyber attacks. This thesis studies the typologies of active cyber defense and examines how this approach can enhance a state’s cyber defense posture.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C&C	Command and Control
CIA	Central Intelligence Agency
DDOS	Distributed Denial of Service
DoD	United States Department of Defense
DOS	Denial of Service
EDT	Electronic Disturbance Theater
FBI	Federal Bureau of Investigation
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control Systems
IP	Internet Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Information Technology
IWM	Information Warfare Monitor
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organization
NRC	National Research Council
P2P	Peer-to-Peer
PLC	Programmable Logic Controller
SQL	Structured Query Language
SSR	Symantec Security Response
TOR	The Onion Router
UN	United Nations
USB	Universal Serial Bus
VOA	Voice of America
WTO	World Trade Organization

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my utmost gratitude to my advisor, Professor Dorothy Denning, for her guidance in the subject, and for being extremely trustworthy, supportive and patient throughout the months of research and writing. Her work ethic is insurmountable. She has been tremendously responsive every single time help was needed! As the main advisor, she has given more than any author can ask for.

And with her profound knowledge in computer science and cyber warfare, Professor Denning has been refreshingly insightful to point out the flaws in the initial and subsequent drafts. This proved to be the turning point that allowed and inspired me to work on many overlooked areas.

I would also like to thank my second reader, Professor John Arquilla, for providing invaluable advice to my thesis. Professor Arquilla is a shrewd strategist who is able to pick up the finest details. Also, as an expert in military affairs and warfare, he was able to point out gaps in my thesis and make recommendations for improving it. I am extremely honored and humbled to have worked with him throughout these months.

In addition, I would like to give special thanks to my wife for her constant support and understanding. Her encouragement and assistance in taking care of the family and kids have been critical in the completion of the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE AND SCOPE

The purpose of this thesis is to study the benefits of applying active cyber defenses to enhance cyber defenses at a national level. Based on the definition from the *U.S. DoD Dictionary of Military Terms*, active defense refers to the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.[1] Thus, active cyber defense would refer to the use of offensive cyber actions, such as counter hacking or pre-emptive hacking, among others, within cyberspace to achieve a similar outcome. The thesis examines the limitations of existing passive defenses such as firewalls, intrusion detection/prevention systems, patching, and auditing. It then explores different types of active defenses, examines their strengths and weaknesses, and studies how they can contribute to the cyber defense posture.

B. BACKGROUND

Cyber attacks are becoming an attractive option for the enemies of a state, social movements, terrorists, etc. One reason is the ever-increasing reliance on computers and the Internet; for governments and militaries around the world, these systems have become easy targets.[2] It has been reported that more than one hundred countries are trying to break into the United States' government networks, and that NATO headquarters receives more than one hundred cyber attacks each day.[3] Another reason for an adversary's interest in cyber attacks is the ease of hiding a perpetrator's identify on the Internet. Many cyber attacks are launched via compromised computers, thereby masking the origin of the attacks. For example, in the cyber attacks against Georgia in 2008, the distributed

[1] *U.S. DoD Dictionary of Military and Associated Terms*, http://www.dtic.mil/doctrine/dod_dictionary/data/a/2043.html.

[2] Lawrence Gershwin, "Cyber Threat Trends and U.S. Network Security," Statement for the Record to the Joint Economic Committee, National Intelligence Council, 21 June 2001, http://www.dni.gov/nic/testimony_cyberthreat.html.

[3] Siobhan Gorman and Stephen Fidler, "Cyber Attacks Test U.S, Allies, and Foes," *Wall Street Journal*, 25 September 2010, http://online.wsj.com/article/SB10001424052748703793804575511961264943300.html.

denial of service (DDOS) attacks were traced to multiple "hacked" computers around the world. These compromised computers, or bots, were victims themselves, providing a protective layer between the attacker and the target systems in Georgia.[4] Another similar example was the cyber attacks on Estonia in 2007. This issue of attribution is further complicated by various privacy and international laws, or lack thereof, around the world.[5]

In response, governments worldwide have taken measures to improve their national cyber defenses. President Obama identified cyber attacks as one of the most serious economic and national security challenges that the United States faces. The administration reviewed cyber policies and programs, releasing the Comprehensive National Cybersecurity Initiative.[6] Also, the U.S. Cyber Command was set up, achieving full operational capability on November 3, 2010.[7] In Europe, NATO established the Cooperative Cyber Defence Centre of Excellence in May 2008 to enhance NATO's cyber defense capabilities. The center's mission is to enhance capability, cooperation and information sharing among NATO's partners through education, research and development, lessons learned and consultation.[8] In addition, many Information Technology (IT) security vendors have offered innovative products to enhance cyber security.

Despite such measures, the number of cyber attacks is still on the rise. Cyber defense can spread across a wide spectrum, ranging from prevention and response to deterrence and investigation. Today, existing cyber defenses are generally passive in nature, thereby failing to extend across the full range of operations. This is unlike traditional war fighting, in which active defenses are utilized as part of a state's defense.

[4] "Overview by the U.S.-CCU of the Cyber Campaign Against Georgia in August of 2008," *U.S.-Cyber Consequence Unit Special Report*, August 2009.

[5] Duncan B. Hollis and David G. Post, "Do Cyber-Attacks Require a Duty to Assist?" *Law Technology News*, 29 April 29 2010, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202453759405&slreturn=1&hbxlogin=1.

[6] "The Comphrehensive National Cybersecurity Initiative," National Security Council, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[7] "Cyber Command achieves full operational capability," Air Force Space Command, 3 November, 2010, http://www.afspc.af.mil/pressreleasearchive/story.asp?id=123229293.

[8] NATO Cooperative Cyber Defence Center of Excellence, http://www.ccdcoe.org.

As Abraham Sofaer highlighted in his book *The Best Defense? Legitimacy and Preventive Force*, states have long conducted preventive wars as forms of defense.[9]

In a similar regard, in the National Research Council (NRC) report, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,” the authors briefly touched on various active cyber defenses, such as non-cooperative intelligence gathering, counterstrike, and preemptive defense.[10] Non-cooperative intelligence gathering refers to the gathering of information about the attack and the attacker through the use of any tools or means. Counterstrike refers to counter hacking of an attacker’s system. Preemptive defense refers to the conduct of an attack on an adversary’s system/network in imminent anticipation of the adversary conducting an attack on the victim’s own system.[11] Although these actions are highly controversial,[12] particularly in terms of legality and legitimacy, they may be able to contribute and offer something new to an overall cyber defense posture.

As such, this thesis seeks to determine how active cyber defense can help in defending against cyber attacks.

C. METHODOLOGY

The thesis will study the different types of cyber attacks and the current state of defenses against them. It will explore the different typologies of active cyber defense and

[9] Abraham D. Sofaer, *The Best Defense? Legitimacy and Preventive Force* (Stanford, CA: Hoover Institution Press, 2010), 32–52.

[10] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,” National Research Council (Washington, D.C.: The National Academies Press, 2009), 142–149.

Note that while the authors refer to preemptive defense in the report, it is likely that they meant preventive defense instead. Based on the definition by Abraham Sofaer, a preventive strike is the “use of force against an anticipated attack based on a judgment that the attacker will use existing or potential means to attack in the future, or to engender other types of harm, including, for example, harm to hostages, attacks by non-state actors, or the mistreatment by a State of its own nationals.” As for preemptive strike, it refers to strikes that uses “force against an attack that is believed to be imminent based on evidence that hostile action has begun or is about to occur.”

[11] Ibid.

[12] Ibid., 239–241.

discuss what they can offer. It will then discuss three cases of cyber attack and illustrate the key benefits that active cyber defenses could have offered for each of the cases.

D. OVERVIEW

Chapter I introduces the purpose and scope of the thesis, i.e. to study the benefits of employing active cyber defenses as a complement to passive cyber defenses in order to better counter cyber attacks at a national level. It also provides some background on the current state of cyber defense.

Chapter II discusses the different types of cyber attacks and the passive defenses that are customarily used against them. It will highlight some of the limitations and challenges of these defenses. The chapter will then touch on the specific difficulties encountered in actual cases of cyber attacks.

Chapter III lays out the different typologies of active cyber defense. These are cyber exploitation, counter hack, preemptive cyber attack, and preventive cyber attack. For each of the typologies, their characteristics, strengths and weaknesses will be examined. The chapter will then discuss how these methods can help in an overall cyber defense posture.

Chapter IV examines three major cases of cyber attacks and study how active cyber defense could have helped in defending against the attacks. The cases are: GhostNet,[13] the worm that carried out cyber espionage; cyber attacks that occurred against Estonia in 2007;[14] and Stuxnet,[15] the worm targeted at disrupting industrial control systems.

[13] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, 29 March 2009, http://www.infowar-monitor.net/ghostnet.

[14] Roland Heickero, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," 2010.

[15] "W32.Stuxnet Dossier Version 1.4," Symantec Security Response, February 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Chapter V summarizes the findings of the earlier chapters and reviews the benefits of active cyber defense. In conclusion, it will also highlight some possible areas for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. UNDERSTANDING CYBER ATTACK AND DEFENSE

A. INTRODUCTION

Cyber attacks are generally considered to be attacks on computer systems and networks. The attacks can originate from individuals, groups, and nation-states for a variety of reasons. Regardless of motivation, they often aim to alter or steal information, or to disrupt the computer system or network. As there is a wide range of attacks of varying magnitude, this chapter will focus on the more noteworthy types. It will also discuss current defenses against them and examine particular cyber attacks that had significant impact.

B. TYPES OF CYBER ATTACK

1. Web Defacement

Web defacements are attacks that alter the contents of a website or hijack its domain name, redirecting users to a false site. As reported by Zone-H, a website archive of versions of defaced websites, the number of web defacement attacks has been rising consistently. There were 300,000 web defacements recorded in 2003. However, in 2010, the numbers increased to an astounding 1,400,000.[16] Until May 2011, there had already been approximately 400,000 defacements reported (see Figure 1). The attackers range from script kiddies[17] to the politically motivated skilled hackers.

[16] Zone-H.org, "Unrestricted information, Yearly & Monthly & Daily attacks," http://www.zone-h.org/stats/ymd.

[17] In a Carnegie Mellon report prepared for the U.S. Department of Defense in 2005, script kiddies are defined as "the more immature but unfortunately often just as dangerous exploiter of security lapses on the Internet. The typical script kiddy uses existing and frequently well known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses in other computers on the Internet - often randomly and with little regard or perhaps even understanding of the potentially harmful consequences." See Nancy Mead, Eric Hough, and Theodore Stehney, "Requirements Engineering (Square) Methodology), Carnegie Mellon Software Engineering Institute (November 2005): 56, http://www.cert.org/archive/pdf/05tr009.pdf.

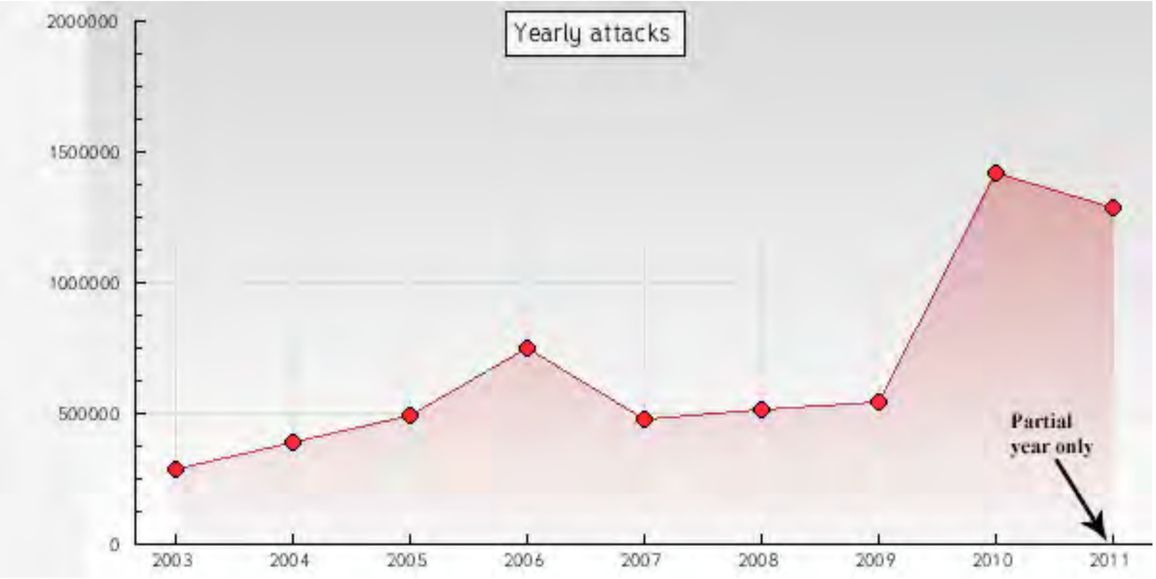


Figure 1. Number of web defacement attacks from January 2003 to October 2011[18]

A good example of politically motivated web defacement occurred during the war against Iraq in 2003. According to F-Secure, web defacements started forty-eight hours preceding the attack on Iraq, and continued to increase during the war. The site F-Secure classified the responsible hackers into three groups: U.S.-based patriotic hackers, Islamic extremist groups from around the world, and peace activitists who were against the war.[19] Figure 2 shows the number of web defacements that occurred during the tenth to twelfth weeks of the war against Iraq.

[18] "Unrestricted information| Yearly & Monthly & Daily Attacks," http://www.zone-h.org/stats/ymd.

[19] "Iraq War and Information Security," F-Secure, 28 March 2003, http://www.f-secure.com/virus-info/iraq.shtml.

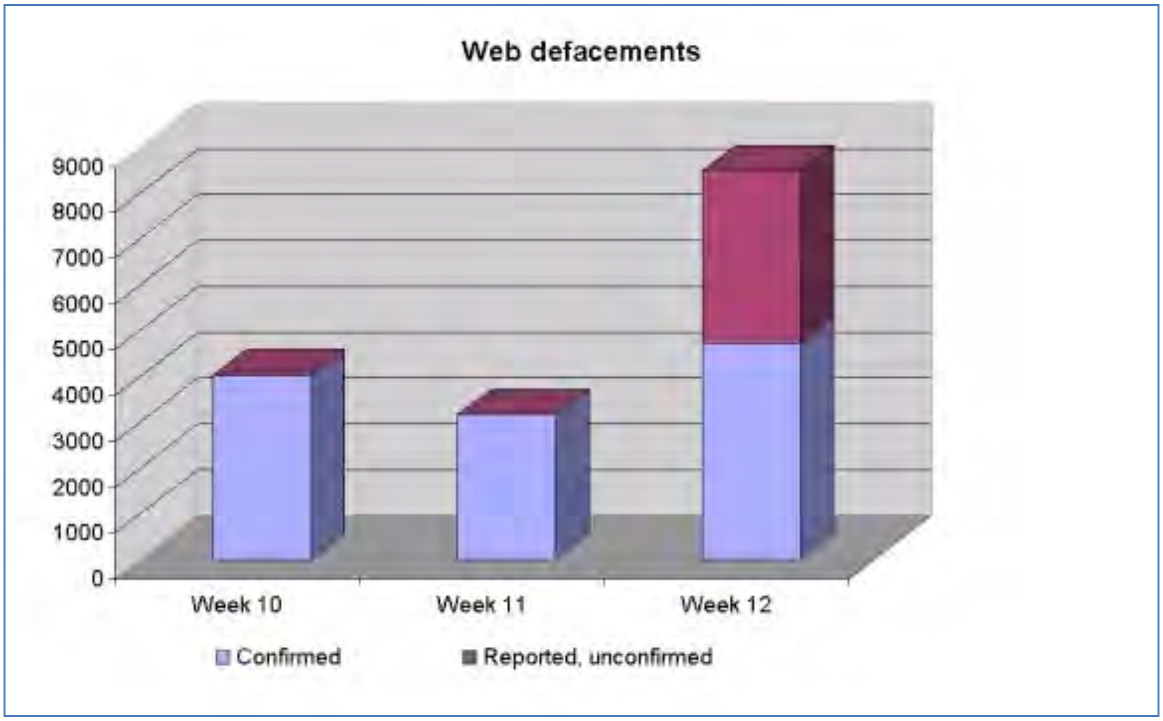


Figure 2. Number of web defacements during week 10–12[20]

In another example, the hacker group "Iranian Cyber Army" hijacked the Voice of America (VOA) website in February 2011, posting a statement demanding that the U.S. Secretary of State, Hillary Clinton, listen to "the voice of oppressed nations" and "stop interfering in Islamic countries." This group was also responsible for hijacking Twitter in December 2009.[21]

2. Denial of Service/Distributed Denial of Service (DDOS)

Denial of service (DOS) attacks aim to cripple or disrupt access to their targets. Typically this is achieved by consuming the bandwidth of the target's network or exhausting resources on the target's system.[22] Often, DOS attacks are carried out via botnets, which are networks of compromised machines that have been infected with

[20] "Iraq War and Information Security," http://www.f-secure.com/virus-info/iraq.shtml.

[21] William Ide, "Iranian Hackers Attack VOA Internet Sites," *Voice of America*, 22 February 2011, http://www.voanews.com/english/news/usa/Iranian-Hackers-Attack-VOA-Internet-Sites-116678844.html.

[22] "Uses of botnet," The Honeynet Project, 10 August 2008, http://www.honeynet.org/node/52.

malware and placed under control of the attacker. Botnets tend to stay dormant until they are given some tasks from their command and control server, which can be located in any part of the world. They are most often used to send spam, but they are also used for fraud and to perform denial of service attacks, with the botnet as a whole conducting what is then called a distributed denial of service (DDOS) attack.[23]

3. Malware (Malicious Software) Attack

This classification includes various forms of malware such as viruses, worms, and Trojans.[24] Viruses are programs that can attach themselves to other software and then replicate when that software is executed. The effects can range from stealing sensitive information to causing disruption. Worms are self-replicating malware. They can scan for vulnerable systems and exploit them. They can also spread via removable devices such as USB thumb drives, an example being the Stuxnet worm. Trojans are malicious code hidden inside legitimate software to avoid detection. Often these are backdoors that allow the attacker full/remote access to the systems that are infected. Although they do not spread on their own, they can reach millions of targets through spam and web downloads. An example of this is the Zeus Trojan.[25]

4. Zero-Day Attacks

These attacks occur when an attacker (humans or artificial-intelligence controlled malware) exploits a computer system through an unpublished vulnerability for which no patch (fix) has been issued.[26] While such attacks are much less frequent than those that exploit known vulnerabilities for which the vendors have released patches, they are far more difficult to detect and defend against since their signatures will not be incorporated

[23] “Botnets,” Shadowserver, http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets.

[24] “Glossary,” McAfee, http://home.mcafee.com/VirusInfo/Glossary.aspx.

[25] Elinor Mills, “Zeus Trojan Steals $1 Million from U.K. Bank Accounts,” CNET, 10 August 2010, http://news.cnet.com/8301–27080_3–20013246–245.html.

[26] Tony Bradley, “Zero Day Exploits,” Internet/Network Sercurity, About.com, http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm.

into anti-malware products. Moreover, even after a vendor has discovered or been notified of a security flaw, it may take some time before a security update is developed and released.

C. TYPES OF CYBER DEFENSE

Many IT security product vendors have been rigorously promoting cutting-edge security solutions and products to defend against various forms of cyber attacks. In addition, organizations have been tightening and enforcing more stringent policies. Such policies cover the storage and handling of classified data, background screening of individuals involved in sensitive job functions, password requirements, types of personal communication devices allowed, types of data allowed to flow between networks, and the frequency in which servers should be patched.[27] Table 1 briefly describes some of the current defense strategies for the types of attacks mentioned in the previous section.

[27] "Information Security Policy Templates," SANS, http://www.sans.org/security-resources/policies.

Table 1. Defenses against cyber attacks.

Attack Type	Recommended defenses – Policies and Technology
Web Defacement	- Ensure servers are patched regularly - Ensure web scripts are well written - Check user input to prevent SQL (Structured Query Language) injection[28] - Deploy software to automatically restore baseline copy of defaced web pages, e.g., Tripwire Remediation Manager[29]
DDOS	- Ensure servers are patched regularly - Have firewalls filter out malformed packets - Maintain a Blacklist of attacking IP addresses - Have bandwidth redundancy - Use load distribution and abnormal request filtering, e.g., Akamai[30]
Malware attack	- Have firewalls filter out malformed packets - Deploy Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) / Anti-Virus (AV), and ensure their signatures are updated regularly - Monitor network traffic - Use application white listing, e.g., Bouncer[31]
Zero-day attack	- Deploy an anomaly monitoring system, e.g., Netwitness[32]

[28] SQL injection is an attack in which malicious code is inserted into instances of SQL server for parsing and execution. See MSDN, Microsoft, http://msdn.microsoft.com/en-us/library/ms161953.aspx.

[29] “Automated Correction of Bad IT Configurations,” Tripwire, http://www.tripwire.com/it-compliance-products/te/remediation/.

[30] “Akamai Security Solutions,” Akamai, http://www.akamai.com/html/solutions/security/ddos_defense.html.

[31] “Introducing Bouncer by CoreTrace,” CoreTrace, http://www.coretrace.com/products/BOUNCER_by_CoreTrace/default.aspx.

[32] “Spectrum,” Netwitness, http://netwitness.com/products-services/spectrum.

A cyber attack is often multifaceted since it can involve a combination of the attacks mentioned above. For example, in the case of a worm attack, it could spread by exploiting misconfigured servers, or exploiting both known and unknown (zero-day) vulnerabilities. After the initial attacks, malware such as Trojans and backdoors could be installed in the compromised systems. Such malware could also spread through removable devices as in the case of Stuxnet, or through spam or web downloads. Once installed, the malware could communicate with remote servers to receive instructions for data collection, sabotage, or conducting DDOS attacks. All these signify the complexities and sophistication of cyber attacks and suggest that existing defenses may not be sufficient.

D. THE REALITY

Based on the *U.S. Defense Department Military Dictionary*, passive defense refers to "measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative."[33] These measures are exactly what the above defensive strategies are about. The recommendations serve to prevent or limit the impact of a cyber attack. When defenses are properly implemented, they may help with forensic investigation and damage control, shorten the time for response and recovery, and deter future attacks.

Unfortunately, results of these measures have not been optimal as shown by the continual increase in the number of cyber attacks. None of the above defenses has been fully successful.

1. Increased Opportunities

With the number of vulnerabilities increasing over the years as reported by the IBM X-Force[34] (see Figure 3), there are more opportunities for potential attackers than ever before.

[33] "Passive Defense," Answers.com, http://www.answers.com/topic/passive-defense.

[34] The IBM X-Force is a R&D team that studies and monitors the latest threat trends including vulnerabilities, exploits, viruses and other malware, spam, phishing, and malicious web content. See http://www-03.ibm.com/security/landscape.html.

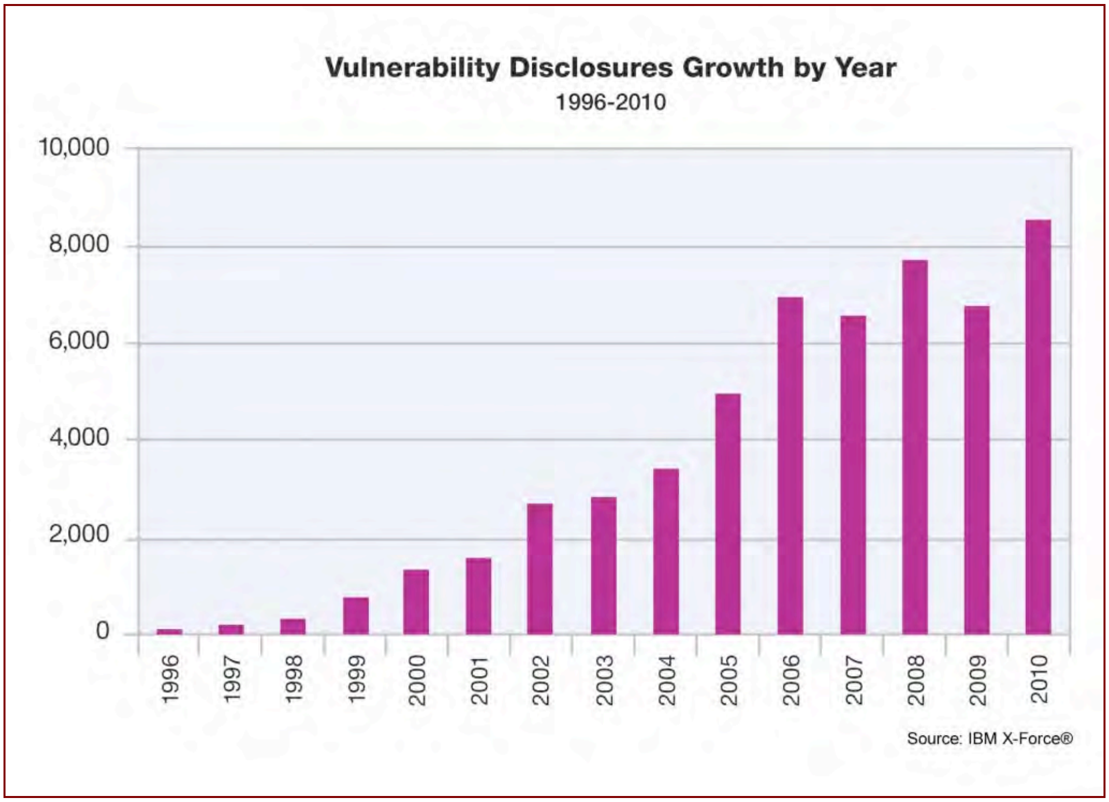


Figure 3. Vulnerabilities growth by year

Apart from the increase in vulnerabilities, the attacks are also becoming more sophisticated. To make matters worse, vendors require time to develop and test their security updates before offering them to their customers. And, at the enterprise level, additional tests are needed to ensure the security updates are compatible with all existing components and do not disrupt functionality. As such, there is often a fairly large window of opportunity for attacks to continue to be effective. Adding to this window of opportunity is the fact that often vulnerabilities remain undisclosed for a period of time.[35]

2. Difficulty in Detection and Filtration

Another reality is that it is difficult to detect something that exploits an unknown vulnerability or uses a new avenue of attack. Moreover, it is difficult to defend the

[35] Bryan Casey, "Over 8000 New Vulnerabilities Disclosed in 2010 – That's a Record," The IBM Institute for Advanced Security Expert Blog, 31 March 2011, http://www.instituteforadvancedsecurity.com/expertblog/2011/03/31/over-8000-new-vulnerabilities-disclosed-in-2010-thats-a-record/.

perimeter of the network without knowing from where an attack originates. Thus, such a perimeter defense becomes very reactive and may not be able to shut down an attack. For example, an attacker can first launch a series of attacks on a target from IP addresses originating from Europe. The target, upon detecting the origin of these attacks, can immediately configure new rules on its firewall to drop incoming traffic from those IP addresses. However, the attacker can easily overcome this by utilizing IP addresses from another location. This shows that such a blacklisting approach is not very effective. Another approach would be to make use of white listing.[36] However, depending on the nature of the business, such an approach may not always be applicable. For example, in the case of the website of a ministry of foreign affairs, it would be difficult to have a white list, since the website needs to be accessible from all addresses.

Furthermore, skilled attackers can utilize sophisticated covert channels[37] to ensure their activities remain obscure and hidden from network traffic monitoring systems and/or intrusion detection systems. An example of such a channel is the HTTP Tunnel. Utilizing this application, an attacker can disguise his traffic to look like regular web surfing traffic, thereby preventing detection by the network monitoring systems.[38]

While there are new defense technologies such as behavioral analysis and anomaly detection, they are not mature as yet and often lead to many false positives.

3. Attribution

Apart from detecting the attack signal itself, the other challenge is attribution. This problem can be divided into two parts: technical attribution and human attribution.[39] Technical attribution involves the analysis of technical components of the cyber attack to trace and locate the IP address of the machine originating the attack. Human attribution

[36] The use of a white list refers to the maintenance of a list of allowed IP addresses, as opposed to a black list, which is a list of disallowed IP addresses.

[37] A covert channel is a communication channel that is hidden or disguised within a legitimate communication channel. See http://www.sans.org/reading_room/whitepapers/covert/.

[38] HTTP Tunnel, http://www.http-tunnel.com/html/.

[39] W. Earl Boebert, "A Survey of Challenges in Attribution," *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council (Washington, D.C.: The National Academies Press), 43.

involves the analysis of all avenues of information pertinent to the attack to identify the person or organization responsible for the attack. Both aspects of attribution are a challenge owing to the multiple barriers (or techniques) by which attackers can mask their routes. These include the use of botnets, The Onion Router (TOR),[40] and covert channels, etc.

E. SOME CASES OF CYBER ATTACKS

1. Conficker

The Conficker worm is responsible for one of the largest worm infections to date. First detected on November 21, 2008, it spread to over seven million government, business, and home computers in over two hundred countries.[41] Some of the more severely impacted victims include the French Navy,[42] where fighter planes were grounded due to the worm infection, and the United Kingdom's Navy, where as many as three-quarters of its ships had infected computers.[43] Over a period of six months, the worm upgraded itself five times, each time adding new functionalities such as infection vectors, propagation and communications methods and even self-defense mechanisms. This illustrates how upgrades compound the difficulty in defending against such advanced malware. Each time a new defense mechanism is in place, such as an updated signature for the anti-virus or intrusion prevention system, the worm can be upgraded to defeat that mechanism. In this manner, defenses will always be one step behind attacks.

2. GhostNet

GhostNet refers to a massive case of cyber espionage against the Tibetan community, India, and other targets, allegedly perpetrated by China. Based on a study

[40] TOR is a network of virtual tunnels that allow users to anonymize their traffic. See http://www.torproject.org/about/overview.html.en.

[41] Conficker Working Group, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Introduction.

[42] Kim Willsher, "French Fighter Planes Grounded by Computer Virus," *The Telegraph*, 7 February 2009, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

[43] Lewis Page, "MoD Networks Still Malware-Plagued After Two Weeks," *The Register*, 20 January 2009, http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/.

conducted by Information Warfare Monitor, the GhostNet malware infected over 1300 computers in 103 countries, of which as many as 30% were considered high-value targets located at various ministries of foreign affairs, embassies, and other government facilities.[44] Through reverse engineering of the GhostNet system, the Information Warfare Monitor found a "covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems."[45] However, despite the in-depth research conducted by the Information Warfare Monitor, no conclusion could be drawn as to who was ultimately in control of GhostNet. The attackers' IP addresses, while traced to Hainan Island, China, were insufficient to implicate any involvement of the Chinese government. The computers with those IP addresses could have been compromised proxy computers used to deliberately mislead the true attacker. This attack emphasized two important issues. Many government networks continue to be vulnerable, and more importantly, attribution in cyber space is extremely difficult to establish. Attribution is especially important, because without solving it, appropriate actions cannot be carried out against a perpetrator.

3. Stuxnet

Stuxnet was the first worm targeted at industrial control systems. Such systems are used in gas pipelines and power plants. Attacks against these systems are especially serious because in the design of many industrial control systems, security has never been a focus, leaving these systems vulnerable. While Stuxnet shares similar characteristics with the Conficker worm, it is far more complex. Apart from utilizing very advanced techniques to achieve stealth capability and propagation via USB sticks, Stuxnet contains sophisticated code to reprogram a Program Logic Controller in order to cause physical damages (Stuxnet is believed to have damaged about one thousand centrifuges at Iran's nuclear enrichment facility at Natanz) and exploits four zero-day vulnerabilities.[46] While this worm was only discovered in July 2010, Symantec Security Response (SSR) was

[44] "Tracking GhostNet: Investigating a Cyber Espionage Network," http://www.infowar-monitor.net/ghostnet.

[45] Ibid., 6.

[46] "W32.Stuxnet Dossier Version 1.4."

able to confirm that it existed at least one year prior to that. The SSR also observed over 40,000 unique external IP addresses, spanning 155 countries. The successful spread of Stuxnet further brings to question whether existing cyber defenses are adequate, especially in the case of industrial control systems.

F. CONCLUSION

Cyber attacks have become more pervasive and more serious. This may be due to several factors, including an increase in the use of computers across many sectors such as government, military, industry, and finance; an increase in actors wishing to exploit and attack these computers for economic, political, and other advantages; and a growing supply of new vulnerabilities along with attack tools to exploit them, as well as all the previously discovered vulnerabilities that have not been fixed in victim computers. As presented by the different cases discussed, the attacks have also become increasingly sophisticated. Not only have they been able to defeat many of their targets' cyber defenses, their perpetrators have been difficult to trace and identify. Apart from continuing to improve existing defenses, which are passive, there is a need to consider employing active cyber defenses. In the following chapters, the thesis will examine how active defenses have contributed to traditional warfare, and how some of the concepts could be applied to cyber defense.

III. ACTIVE CYBER DEFENSE

A. INTRODUCTION

As mentioned earlier, active defenses refer to the employment of limited offensive actions (such as preventive and preemptive strikes) and counterattacks to deny a contested area or position to the enemy. These strategies have long been an integral part of traditional domains of warfare. They have been used to preempt a capability, to prevent a war, and to counter attacks.

In the context of cyber defense, active defenses can be utilized in the same manner. This chapter will discuss the typologies of active cyber defense, what they can offer, and how they can help in defending against cyber attacks.

B. TYPOLOGIES OF ACTIVE CYBER DEFENSE

In broad terms, the typologies of active cyber defense can be categorized into exploitation, counter attack, preemptive attack, and preventive attack.

1. Cyber Exploitation

This typology refers to the exploitation of computer systems involved in a cyber attack in order to obtain intelligence that can aid in the analysis of the attack and in determining attribution.

During or after a cyber attack, passive defenses such as forensics and auditing of logs can only reveal the IP addresses of the immediate attack sources. However, as discussed before, many attacks are launched through multiple hops, consisting of hacked computers. Thus, to determine the true origin of an attack, an effective way to trace through the attack path undertaken by the attacker is needed.

One widely researched technique, which does not require any exploitation of the attacking computers, is IP traceback.[47] However, this technique is not yet mature,

[47] Andrey Belenky and Nirwan Ansari, “IP Traceback with Deterministic Packet Marking,” *IEEE Communications Letters* 7, no. 4 (April 2003): 162.

resulting in compatibility and performance issues.[48] Also, the attribution systems built on techniques such as IP traceback need to be implemented at as many ISPs as possible in order for results to be accurate.[49] This raises the issue of cost. Without any financial gain, there is little motivation for the ISPs to implement attribution systems, even if they are working perfectly. Furthermore, the trustworthiness of the information may be questionable when a non-friendly country is involved.[50] For illustration, there may be network traffic transmitted from the U.S. to Russia over a network that extends into the North Korean network. To what extent will the North Koreans be willing to cooperate to release attribution information? And even if they were willing to release the information, would it be reliable?

Through cyber exploitation, these issues may be avoided. After obtaining the last IP address of the computer used by the attacker (based on results from forensics and log audits), the computer could be exploited or "hacked back." After gaining access, in-depth analysis could determine the next system in the chain. By repeating the process, the attack path could be identified, eventually leading to the computer used for the attack.[51] Once that is achieved, forensic needs to be performed on this computer so as to determine the owner of the computer. By investigating the documents stored on the computer, web surfing history and cache files, e-mails, etc., the owner or user of that computer could be identified.[52] The information retrieved from the investigation may then provide clues as to who the mastermind is, and whether a state is involved. For example, there could be an e-mail conversation or document containing instructions from some state official. However, that would be inconclusive since the official could be acting on his own accord.

[48] Ping Wang et al., "A New Approach for Solving the IP Traceback Problem for Web Security," *Advances on Information Sciences and Service Sciences* 3, no. 2 (March 2011).

[49] Jeffrey Hunker, Bob Hutchinson, and Jonathan Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution," Institute for Information Infrastructure Protection, January 2008, http://ww.thei3p.org/docs/publications/whitepaper-attribution.pdf.

[50] Matt Bishop, C. Gates, and J. Hunker. "The Sisterhood of the Traveling Packets," *In Proceedings of the 2009 Workshop on New Security paradigms*, 2009, 61.

[51] David Wheeler and Gregory Larsen, "Techniques for Cyber Attack Attribution," Institute For Defense Analyses, October 2003, 23.

[52] Keith Jones, Richard Bejtlich, and Curtis Rose, *Real Digital Forensics* (New Jersey: Addison-Wesley, 2008), 205–300.

To get to the truth, more investigation would be needed. The official's computer could be exploited. By monitoring his e-mails and documents, more clues and evidence may be gathered. In any case, there would be technical and legal considerations concerning such exploitation. These will be discussed at the end of this chapter.

At this point, appropriate legal actions could be taken against the attacker, or if the attacker were a foreign government, actions such as economic sanctions, conventional/cyber counter attack, and others, could be taken. Or perhaps for strategic reasons, the defending nation may even choose not to reveal its knowledge of the attacker. Regardless, the capacity to undertake such a cyber exploitation to achieve a more thorough attack analysis and attribution leads to deterring potential attackers.

Many attackers would take advantage of the very architecture of the Internet to mask their traces. In doing so, they could then carry out their attacks without any fear of being identified or facing other consequences. They would compile a pool of vulnerable computers that they have hacked, and subsequently log in through a series of these hacked computers before launching the attack.[53] Alternatively, they could also connect via anonymous proxy servers or TOR to launder their traffic.[54] While a counter attack on the attacker may not be possible until an actual location is determined, it can still be useful. As discussed previously, exploiting the various hacked computers would allow the reconstruction of the attack path, which in turn would reveal the location of the attacker. Once that is obtained, actions could be taken to disable the attacker's systems. Knowing that he may no longer hide in the shadows of the Internet and that his systems may be attacked, he is likely to be further deterred.

2. Counter Attack

The U.S. Department of Defense defines counter attack as an "attack by part or all of a defending force against an enemy attacking force, for such specific purposes as regaining ground lost or cutting off or destroying enemy advance units, and with the

[53] Stuart Staniford-Chen, L. Todd Heberlein, "Holding Intruders Accountable on the Internet," *Proceedings 1995 IEEE Symposium on Security and Privacy*, IEEE, May 1995, 39.

[54] "Tor: Overview," Tor project, http://www.torproject.org/about/overview.html.en.

general objective of denying to the enemy the attainment of the enemy's purpose in attacking. In sustained defensive operations, it is undertaken to restore the battle position and is directed at limited objectives."[55] An example of a counter attack in history is the siege of Bastogne during the Second World War. On December 20, 1944, the Germans laid siege at the town of Bastogne, Belgium, as part of their efforts to capture Antwerp. While the siege was ongoing, U.S. Lt. Col. Creighton Abrams, who later commanded U.S forces in Vietnam, led a counter attack against the Germans, and succeeded in punching through the German lines, thereby ending the seven-day siege.[56]

In the case of a cyber attack, the equivalent would be to counter hack the attacker responsible for the cyber attack, instead of relying on more passive means such as a perimeter firewall or an intrusion prevention system to filter or block the attacks.[57] One of the earliest examples of a cyber counter attack occurred in 1998. A group of activists by the name of the Electronic Disturbance Theater (EDT) had launched a "web sit-in" (DOS attack) against a Pentagon website. The Pentagon reacted by redirecting the incoming web traffic to a web application, which subsequently caused the attacker's web browsers to crash, thereby neutralizing the attacks.[58]

In another example, during the World Trade Organization (WTO) Summit in January 2000, the WTO server was the target of a DOS attack by Electrohippies (E-hippies), an activist group based in the United Kingdom. Conxion Inc., the company at which the WTO server was hosted, was able to trace back the IP addresses to the E-

[55] Defense Technical Information Center. http://www.dtic.mil/doctrine/jel/doddict/data/c/01331.html.

[56] Colonel S.L.A Marshall, "Bastogne The First Eight Days," *U.S. Army In Action Series*, The Center of Military History, http://www.history.army.mil/books/wwii/Bastogne/bast-fm.htm.

[57] Incidentally, the Pentagon has announced a new cyber strategy in that computer attacks coming from another country can be regarded as an act of war, and that it reserves the right to respond by kinetic means. See Siobhan Gorman and Julian Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, 31 May 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

[58] Robert Wildt, "Should you Counter-Attack when Network Attackers Strike?" Global Information Assurance Certification Paper, SANS Institute, 13 December 2000.

hippies' server. Instead of filtering the incoming attacks, Conxion redirected the attacks back to the E-hippies server, and was able to disable that server for several hours.[59]

Both examples show how counter attacks have been used to effectively stop attacks. Counter attack does not just prevent the attacks from succeeding; it aims to prevent the attacker from launching further attacks. In the case of a DDOS attack carried out by a botnet controlled via C&C servers, counter attacks could be carried out either against the C&C servers or the computer/network of the attacker.

This is identical to that of command and control warfare as described by Martin Libicki in *What is Information Warfare*? In conventional warfare, command and control systems are widely used to enhance battlefield communications and effectiveness. Libicki described an effective way to cripple the enemy's command and control warfare system by decapitating the enemy's command structure from its body of command forces.[60] In the context of a DDOS attack from a botnet under centralized command and control, a similar approach would be to shut down the C&C servers. Since the bots receive their instructions from the C&C servers, doing so will prevent further instructions from propagating to the bots. It would also aid in neutralizing the attack. While backup C&C servers may surface, this process may be repeated until all C&C servers are shut down. An additional or alternative response would be to send out code to the bots, instructing them to be idle. Thereafter, their respective ISPs and security product vendors could be involved to work with the owners to remove the bots.

If a sample of a bot code can be obtained, the code may contain the IP addresses or domain names of the C&C servers. Alternatively, the bot could be executed in a controlled environment, and be monitored closely as to where it tries to connect. Doing so can also reveal the whereabouts of the C&C servers. However, if no such sample is available, exploitation could be done on one of the bots involved in the DDOS attack. After gaining access to that bot, analysis could be performed. Once the IP addresses of

[59] Jayawal, Vikas, William Yurcik, and David Doss, "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?" June 2002, http://www.scribd.com/doc/38380481/Internet-Hack-Back-Counter-Attacks-as-Self-Defense-or-Vigilantism.

[60] Martin Libicki, *What is Information Warfare?* Institute for National Strategic Studies, National Defense University, August 1995, http://www.ndu.edu/inss/actpubs/act003/a003ch03.html.

the C&C servers were discovered, an attack could be launched on that server to take it offline. Alternatively, relevant authorities and corresponding ISPs/owners could be notified so that the server could be cleaned up and, if necessary, seized for further investigations.

A recent example of such a counter initiative is the taking down of the Coreflood botnet by the FBI in April 2011.[61] The Coreflood botnet had infected over two million computers around the world, stealing the users' credentials (usernames and passwords), and other personal and financial information. After obtaining a court order, the FBI proceeded to seize the five C&C servers and take down the twenty-nine Internet domain names used by Coreflood. With control over the C&C servers, the FBI also arranged for instructions to be propagated down to the bots that effectively placed them in a dormant state.

In cases where the botnet's command structure is based on a peer-to-peer (P2P) architecture instead of centralized C&C servers, the above operation would not work. Instead, other forms of counter attack would be required. However, since P2P bots propagate instructions to one another rather than retrieve the instructions from a central C&C server, it is possible to conduct a man-in-the-middle attack and intercept/manipulate the communications between the bots. In doing so, neutralizing instructions (such as instructing the bots to enter a dormant mode) could be transmitted to other bots.[62]

Counter attack could also be useful as a form of deterrent. As Patrick Morgan explained, deterrence refers to "efforts to avoid being deliberately attacked by using threats to inflict unacceptable harm on the attacker in response."[63] He added that such harm could involve making the cost of attack too great for the attacker to continue, or it could be in the form of retaliation. In the context of a cyber attack, retaliation would

[61] Chris Lefkow, "U.S. disables Coreflood botnet, seizes servers," *PHYSORG.COM*, April 13, 2011, http://www.physorg.com/news/2011–04-disables-coreflood-botnet-seizes-servers.html.

[62] Felix Leder, Tillmann Werner, Peter Martini, "Proactive Botnet Countermeasures – An Offensive Approach," NATO Cooperative Cyber Defence Centre of Excellence, March 2009, http://www.ccdcoe.org/publications/virtualbattlefield/15_LEDER_Proactive_Coutnermeasures.pdf.

[63] Patrick Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (2010), http://www.nap.edu/catalog/12997.html.

imply a counter cyber attack. Therefore, if the attacker knew that there could be a counter attack or retaliation, he would be more likely to be deterred.[64] This is, however, contingent upon the defender's ability to pierce through the attacker's veil of anonymity.

3. Preemptive Strikes

A preemptive strike is one that uses "force against an attack that is believed to be imminent based on evidence that hostile action has begun or is about to occur."[65] As with counter attack, preemption has been seen throughout military history.[66] For example, in 1967, Israel believed it was launching a preemptive war against Egypt when the latter massed its troops on Israel's borders.[67]

In the context of cyberspace, a preemptive strike can be described as "conducting an attack on a system or network in anticipation of that system or networking conducting an attack on your system."[68] Assuming a scenario where a state (Blue) has gathered intelligence that a hostile state (Red) has plans to mount a cyber attack against it, Blue can launch a preemptive cyber operation against Red. Doing so can help achieve the following:

1) Cripple the enemy's attack capability. In the case of the Six Day War in 1967, the moment Israel found out that Egypt had been building up its troops at Israel's borders, Israel launched an attack against the Arabs. The preemptive attack by the Israeli forces destroyed nearly four hundred Egypt-based military aircraft.[69] In the cyber operation mentioned above, upon penetrating Red's networks, Blue can cripple Red's cyber attack capability through the disruption of Red's network.

[64] David Clark and Susan Landau, "Untangling Attribution," *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (2010), http://www.nap.edu/catalog/12997.html.

[65] *The Best Defense?, Legitimacy and Preventive*, 9.

[66] Ibid., 70.

[67] *The Best Defense?, Legitimacy and Preventive Force*,70.

[68] "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities," 149.

[69] "1967: Israel Launches Attack on Egypt," *BBC News*, http://news.bbc.co.uk/onthisday/hi/dates/stories/june/5/newsid_2654000/2654251.stm

2) Deterrence. Upon infiltrating Red's network, Blue can subtly make its presence known, thereby alerting Red that its network has been compromised. Doing so might deter Red from launching an attack on Blue. This is described by W. Earl Boebert in the NRC report, as the "awareness on the part of potential attackers that such "cyber patrolling" was being conducted and would in and of itself act as a deterrent, since they would be faced with additional security tasks as well as the uncertainty as to the degree to which they may themselves have been penetrated and placed at risk."[70]

4. Preventive Strikes

While conceptually a preventive strike may seem similar to a preemptive strike, there is an important distinction. As Abraham Sofaer described, a preventive strike is the "use of force against an anticipated attack based on a judgment that the attacker will use existing or potential means to attack in the future, or to engender other types of harm, including, for example, harm to hostages, attacks by non-state actors, or the mistreatment by a State of its own nationals."[71] This implies that such an attack is launched before any non-imminent attack or threat that does not qualify as an attack under international law.[72]

A good example of a preventive strike occurred in 1981, when Israel launched an attack on the nuclear reactor at Osirak, in Iraq. At that time, the uranium-powered reactor was nearing completion, but there were no signs of its being stocked with nuclear fuel. However, Israel claimed that the reactor would be capable of producing devastating nuclear weapons, and that it could not allow such an enemy to develop weapons of mass destruction against Israelis.[73]

With a similar argument, a preventive cyber attack can be launched against a hostile actor (both state and non-state) to prevent the latter from acquiring any cyber offensive capability. It can also achieve the similar deterrent effect as with the case of a preemptive attack mentioned above. That is, when the hostile actor realized that its

[70] "A Survey of Challenges in Attribution," 49.

[71] *The Best Defense?, Legitimacy and Preventive Force*, 9.

[72] Ibid.

[73] "1981: Israel Bombs Baghdad nuclear reactor," *BBC News*, http://news.bbc.co.uk/onthisday/hi/dates/stories/june/7/newsid_3014000/3014623.stm.

network had been compromised, it might think twice about pursuing cyber attack capability. However, a preventive cyber attack can also be extended to a non-cyber related offensive capability. A good example of this would be Stuxnet, the first computer worm targeted at industrial systems, or more specifically at nuclear facilities.[74] While Stuxnet spread to computers around the world, the infection was concentrated mainly in Iran.[75] It appears that the creator of Stuxnet intended to use the worm to prevent the buildup of nuclear weapon capability in Iran. President Mahmoud Ahmadinejad also publicly acknowledged that Stuxnet had disrupted Iran's nuclear program.[76] As it seems, the Stuxnet has already encouraged emulation by others, as evident by the Duqu malware. As reported by Symantec, Duqu has been labeled as a precursor to the next Stuxnet.[77]

C. LIMITATIONS AND CONSIDERATIONS

The typologies mentioned in this chapter are not without their limitations. First of all, such measures are very controversial and may violate certain international laws. Secondly, even if such measures can be justified, there are technical challenges.

1. Technical Aspects

One of the key success factors in utilizing active cyber defenses is the ability to launch a cyber attack. For the counter strike to be successful, the active defender needs to be able to exploit vulnerabilities in the systems used by the attacker.[78] While the attacker is likely to be using computers that he has previously hacked (intermediate computers),

[74] Aleksandr Matrosov et al., *Stuxnet Under the Microscope*, Revision 1.31, ESET, 23, Jan 2011, http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

[75] Ibid., 15.

[76] Larry Dignan, "Iran admits Stuxnet hurt nuclear programme," *ZDNet*, 30 November 2010, http://www.zdnet.co.uk/news/security-threats/2010/11/30/iran-admits-stuxnet-hurt-nuclear-programme-40091018/.

[77] Jaikumar Vijayan, "Update: Duqu Exploits Zero-Day Flaw in Windows Kernel," *Computerworld*, 1 November 2011, http://www.computerworld.com/s/article/9221372/Update_Duqu_exploits_zero_day_flaw_in_Windows_kernel?taxonomyId=85.

[78] "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities," 83.

he is also likely to have patched any known vulnerabilities on those intermediate computers.[79] As such, it could take massive efforts to research a new vulnerability that would allow the counter attack to succeed. This poses a big challenge because such research can be time consuming. If it takes too long, it would delay the counter attack resulting in more extensive damages to the defender. Furthermore, this delay would also create a wider window of opportunity for the attacker to mask his traces and/or further secure the intermediate computers. Just as in the siege of Bastogne, should Lt. Col. Abrams have delayed his counter attack by a few more days, the allies' casualties would have risen considerably. The Germans could also have had reinforcements in place, thereby strengthening their positions to repel the counter attack.

One possibility to address the timeliness issue is to allocate more resources to discovering vulnerabilities. Unfortunately, that in itself is a challenge, as there is a severe shortage of cyber security experts.[80] The research could be performed in advance, but this requires identifying the systems used by potential adversaries. Such information could be acquired from exploitation or other sources of intelligence and then used to steer the research, resulting in readiness for a counter, preemptive, or preventive attack.

2. Legal Aspects

Assuming technical concerns are overcome, there are still legal issues relating to the use of active defenses. Traditionally, active defenses have been controversial. For example, after the Israeli bombing of the Osirak nuclear reactor in June 1981, there was a broad agreement among various nations that the bombing was unacceptable. The Reagan administration condemned the attack and the British government claimed that the action had violated international law.[81] Should a state carry out a cyber attack against another

[79] "Techniques for Cyber Attack Attribution," 23.

[80] Eric Beidel and Stew Magnuson, "Government, Military Face Severe Shortage of Cybersecurity Experts," *National Defense Magazine*, August 2011, http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx.

[81] Nicholas Kristof, "The Osirak Option," *The New York Times*, 15 November 2002, http://www.nytimes.com/2002/11/15/opinion/the-osirak-option.html.

state on the basis of preventing a potential threat from occurring, it would likely draw critical scrutiny from nations around the world.

Based on the International Law of Armed Conflict (LOAC), a state must have "good" reasons for using force or violence against another state.[82] Articles 39 and 42 of the UN Charter "permit the Security Council to authorize uses of force in response to 'any threat to the peace, breach of the peace, or act of aggression' in order to 'maintain or restore international peace and security.'" Article 51 adds that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs…"[83] Thus, in the cyber context, when would it be legal for a nation to launch a cyber attack (counter attack, preventive attack, or preemptive attack) against another? What would the "good" reasons be? Assuming the reasons were adequate, what would the rules that govern the use of a cyber attack be?

What about exploitation of the intermediate system? In the case of Coreflood, the FBI, after obtaining the court order, seized several of the servers. Thereafter, they were able to fully analyze the hardware legally. However, what would happen when an intermediate system was located in a foreign country? This could be a complex issue because different countries would have different laws, interests, and even capacity to handle the situation.[84] Or perhaps the foreign country could be on unfriendly or non-cooperative terms. The Council of Europe's Convention on Cybercrime aims to harmonize state laws and foster inter-state cooperation, but not all countries have signed on or agreed to its principles.[85]

Given these factors, when would it be legal to proceed with an exploitation? And in the process of the exploitation, who will be held responsible should the system become

[82] "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities," 242.

[83] Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Charter of the United Nations, http://www.un.org/en/documents/charter/chapter7.shtml.

[84] James Carafano, "Getting Cyber-Serious? – FBI Targets Botnet," *Security Debrief*, 21 April 2011, http://securitydebrief.com/2011/04/21/getting-cyber-serious-fbi-targets-botnet/.

[85] Council of Europe's Convention on Cybercrime, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp.

unstable? Also, legitimate users of that system could have their privacy violated. For example, sniffers could be deployed to analyze the network traffic passing through the system and documents could be extracted as part of a forensic investigation. The sniffers could reveal the users' credentials to other systems, and the documents might contain private information. Proceeding with such exploitation could possibly violate the privacy of individuals or other domestic laws of that country. As such, could legal actions be taken against the party responsible for the exploitation/investigation? Furthermore as Kesan and Hayer cautioned in their paper, Mitigative *Counterstriking*, such hostile actions could escalate into kinetic armed conflict.[86]

D. CONCLUSION

The discussion presented in this chapter has shown that active cyber defenses can be useful in defending against cyber attacks. They can help address attribution; deter potential attackers; and mitigate, preempt, and prevent cyber attacks. However, this does not imply that active cyber defenses can replace passive defenses. Passive defenses are still required as part of an overall cyber defense posture. For example, passive defenses can be used to block the attacker, while active defenses can be used to go after the attacker, thereby preventing him from launching further attacks.

The use of active defenses is likely to continue to generate controversy, particularly due to the unanswered questions listed earlier. Regardless, active cyber defenses will need to be executed within the context of an overall strategy that takes into account the above issues to ensure that the benefits outweigh the costs and risks. Active defenses are a double-edged sword and have the potential to do more harm than good if not implemented with utmost care and in adherence to laws and ethical principles.

[86] Jay P. Kesan and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," *Harvard Journal of Law and Technology*, Forthcoming 2012, April 2011, 65, http://papers.ssrn.com/pape.tar?abstract_id=1805163.

IV. CASE STUDIES

A. INTRODUCTION

This chapter examines three of the more prominent cases of cyber attacks in recent history. They are GhostNet, the cyber espionage incident that affected 103 countries;[87] massive cyber attacks against Estonia;[88] and Stuxnet, the first computer worm targeted at industrial systems.[89] The chapter will describe the attacks and discuss how active cyber defense could have played a part in defending against them.

B. GHOSTNET

1. Overview

GhostNet was touted as the largest spying operation to have been uncovered at the time, based on the number of affected countries.[90] A ten-month investigation by the Information Warfare Monitor (IWM) discovered that GhostNet had infected 1,295 computers in 103 countries. As many as thirty percent of these computers were deemed high-value targets. They included computers belonging to various ministries of foreign affairs and embassies.[91] The Figure 4 depicts the geographical locations of the compromised computers.

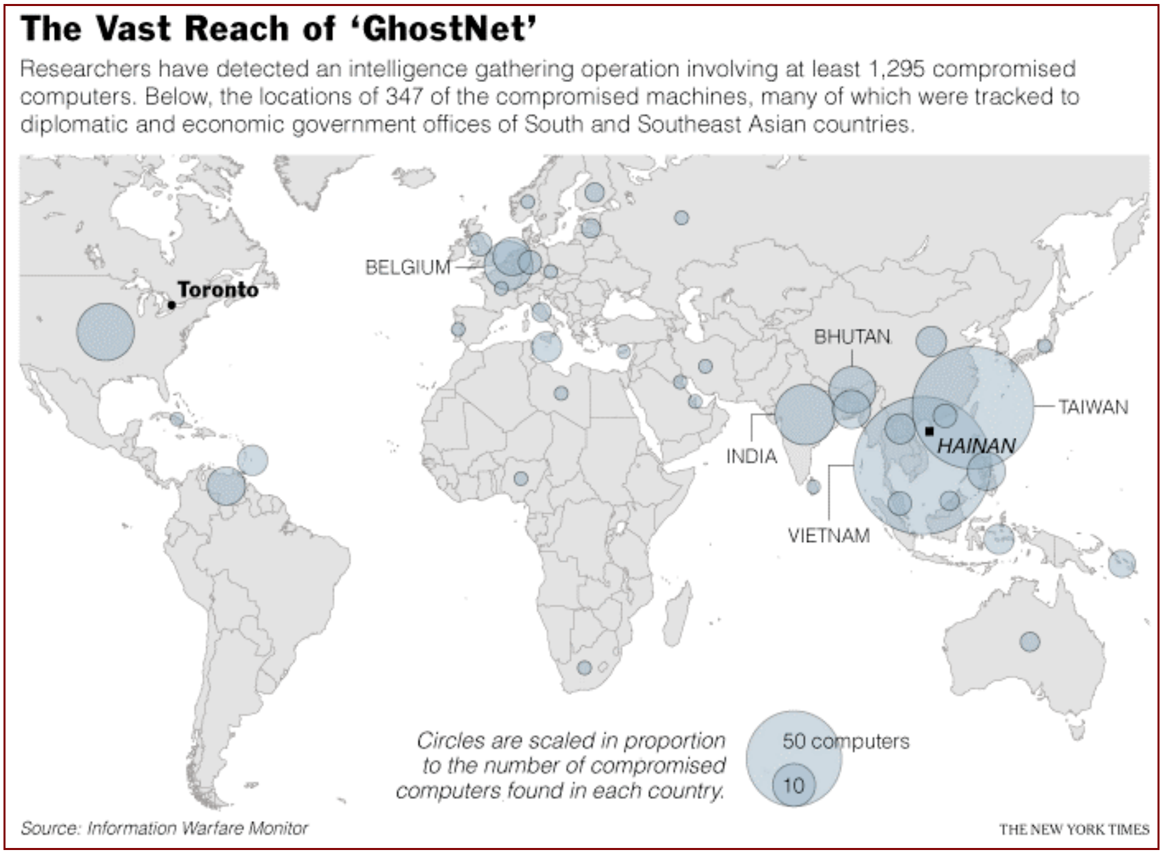
[87] "Tracking GhostNet: Investigating a Cyber Espionage Network."

[88] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, 16 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

[89] "Stuxnet Under the Microscope."

[90] "Major Cyber Spy Network Uncovered," *New York Times*, 29 March 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html.

[91] "Tracking GhostNet: Investigating a Cyber Espionage Network."



The Vast Reach of 'GhostNet'

Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.

Circles are scaled in proportion to the number of compromised computers found in each country.

Source: Information Warfare Monitor

THE NEW YORK TIMES

Figure 4. The vast reach of GhostNet[92]

2. The Investigation

The primary mode of infection in GhostNet was social engineering. The attacker first sent an e-mail with an attachment to the target with an appealing message to entice the target to open the attachment. Once the target opened the attachment, the target's computer proceeded to download and install the Gh0st RAT malware.[93] Gh0st RAT is a Remote Access Trojan that allowed the attacker to have near unrestricted access to the infected computers.[94] The Trojan connected to command and control servers on the

[92] "The Vast Reach of GhostNet," *The New York Times*, 28 March 2009, http://www.nytimes.com/imagepages/2009/03/28/technology/20090329_SPY_GRAPHIC.html.

[93] "Tracking GhostNet: Investigating a Cyber Espionage Network," 18.

[94] Ibid.

Internet to retrieve instructions. The instructions could command the software to transmit any files to and from a remote computer, activate the webcam or microphone, or other directives.[95]

By monitoring the computers in Dharamsala and at various Tibetan missions, IWM was able to determine the IP addresses of the servers hosting Gh0st RAT and for command and control. With further analysis, four hosting servers and six command and control servers were mapped out. Three of the four hosting servers were located in China. The fourth was located in the U.S. Five of the six command and control servers were located in China, with the sixth in Hong Kong.[96]

While the majority of the command and control servers' IP addresses were traced back to China, the Chinese government denied any involvement.[97] Without concrete evidence, identity of the perpetrator remains a problem. And as IWM rightfully pointed out, GhostNet "could have been conducted by a state other than China, but using servers within China for strategic purposes."[98] Thus, despite the in-depth analysis by IWM, it is uncertain as to the identity of the true culprit.

3. How Could Active Cyber Defenses Have Helped in This Scenario?

In this scenario, active cyber defense might be able to do what IWM failed to do, that is, to reconstruct the attack path and identify the actual attacker. The IWM mentioned in its report that its network trace had ended at the location of the command and control servers, and that it was not conclusive as to who was behind GhostNet. As such, a more affirmative way to deduce the attacker's identity would have been to monitor the command servers and then determine who was uploading the instructions. This can be done in two ways. First would be to involve the authorities and service providers of the

[95] "Tracking GhostNet: Investigating a Cyber Espionage Network,"14–15, 39.

[96] Ibid., 30.

[97] "China Denies Any Role in GhostNet Computer Hacking," *Voice of America*, 31 Mar, 2009, http://www.voanews.com/english/news/a-13–2009–03–31-voa12–68812997.html?CFTOKEN=37567981&CFID=253397922&jsessionid=843016046241f811765c716e398086338793.

[98] "Tracking GhostNet: Investigating a Cyber Espionage Network," 48–49.

country where the C&C servers are located. This approach would be similar to that taken with Coreflood, where the FBI first obtained a court order before seizing the servers.[99] With access to the servers, logs and other data on the servers can be analyzed to help trace and identify the person who uploaded the instructions for Gh0st RAT. In one instance, IWM found that stolen files were uploaded to a C&C server located in Beijing, China.[100] In a situation when cooperation from the authorities and/or service providers is lacking, this C&C server could have be exploited. For example, hacking into the C&C server would allow data to be examined and analyzed that would otherwise be impossible to acquire. Thereafter, the attacker could be traced in the same manner described above.

Another way to conduct cyber exploitation is to adopt the original concept of the Trojan Horse as used by the Greeks when they wanted to gain entrance into Troy.[101] In the cyber context, backdoors could be embedded in seemingly important documents located within the computers infected by GhostRat. When the attacker retrieved and opened these documents, his computer would be compromised. Thereafter instructions could be sent to the backdoor to extract system and network information, to be used to determine the location and identity of the attacker. Of course, this will only work if the attacker opens the documents and the backdoor is successfully installed. Subsequently, Internet access is required in order for the information to be sent out.

C. CYBER ATTACK ON ESTONIA

1. Overview

In April 2007, Estonia experienced a massive cyber attack that nearly shut down the nation's digital infrastructure. The attack lasted from April 27, 2007, to May 18, 2007, and occurred in parallel to the rioting in the streets as part of a protest against the Estonian government for relocating a Soviet-era Second World War memorial.[102] While

[99] Chris Lefkow, "U.S. disables Coreflood botnet, seizes servers," *Physorg.com*, April 13, 2011, http://www.physorg.com/news/2011–04-disables-coreflood-botnet-seizes-servers.html.

[100] "Tracking GhostNet: Investigating a Cyber Espionage Network," 25.

[101] "The Trojan War," http://www.stanford.edu/~plomio/history.html.

[102] Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defence Centre of Excellence, 2010, 15.

the media described this attack as "the first war in cyberspace,"[103] others termed it a "cyber riot."[104] Regardless, the impact was significant due to Estonia's high dependency on the Internet. Online sites belonging to various government agencies, newspapers, banks, and Internet service providers were severely disrupted during this period.

The attacks were carried out in four waves and consisted of DDOS and web defacement attacks.[105] The government targets included the Estonian Government Briefing Room, the Estonian Ministry of Defense, leading political parties, and the parliament. The private sector targets included two of the largest banks in Estonia, three news organizations, and telephone exchanges.[106] Notably, 97 percent of Estonians are dependent on e-banking, further signifying the seriousness of the attack.[107]

2. Responding to the Attacks

The Estonian CERT, system administrators, and top IT experts worked together to respond to the attack. The first technical response was to increase the bandwidth or throughput capacity to the targets so they could handle more traffic.[108] By May 10, 2007, the bandwidth capacity for the Estonian government networks had increased several times above its regular capacity. Apart from this, other technical measures were in place as well. Security patches were installed; firewall rules configured to filter out the malicious traffic; external servers blocked, along with other measures. However, that did

[103] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, 29 May 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html.

[104] Bill Brenner "Black Hat 2007: Estonia Attacks Were A Cyber Riot, Not Warfare," 3 August 2007, http://searchsecurity.techtarget.com/news/1266728/Black-Hat-2007-Estonian-attacks-were-a-cyber-riot-not-warfare.

[105] "International Cyber Incidents: Legal Considerations," 19–20.

[106] "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," 40.

[107] Tom Espiner, "Estonia's Cyberattacks: Lessons Learned, A Year On," *ZDNet*, 1 May 2008, http://www.zdnet.co.uk/news/security-threats/2008/05/01/estonias-cyberattacks-lessons-learned-a-year-on-39408158/.

[108] "International Cyber Incidents: Legal Considerations," 24.

not stop all the attacks. It was reported that the attackers managed to obtain inside information on the attack and were able to adjust their attacks to overcome the defenses.[109]

Other responses included support coming from the international community. For example, U.S. governmental institutions tried to help locate and shut down various sources of attack.[110] However, this was not an easy task. Arbor Networks reported that the attacks originated from all over the world instead of from a few locations.[111] The Estonian Informatics Centre, which was responsible for Estonia's information systems and the Internet, confirmed the attacks were from as many as 178 countries.[112] Also, the attackers intentionally moved the C&C servers to countries that were on unfriendly terms with Estonia, thereby preventing any potential cooperation in stopping the attacks or apprehending the culprits.[113] As a result, not all the C&C servers used by the botnets could be shut down.

Toward the end of May 2007, the attacks gradually stopped. This came about as news spread that the criminals responsible for the attacks were being brought to justice.[114] This was confirmed when NATO reported that the attackers had stopped their attacks deliberately rather than being shut down.[115]

3. How Could Active Cyber Defenses Have Helped in This Scenario?

The initial wave of attacks was traced to individuals with Russian nationalist sympathies who carried out the attacks by following instructions posted on various Internet forums and websites.[116] For the individuals who lacked the sophistication to

[109] "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," 41.

[110] "International Cyber Incidents: Legal Considerations," 24.

[111] Ibid., 23.

[112] Charles Clover, "Kremlin-Backed Group Behind Estonia Cyber Blitz," *Financial Times*, 11 March 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3–0000779fd2ac.html#axzz1XqpZTRzc.

[113] "International Cyber Incidents: Legal Considerations," 28.

[114] Ibid., 24.

[115] McAfee Virtual Criminology Report, "Cybercrime: The next wave," 2007, 12.

[116] "International Cyber Incidents: Legal Considerations," 23.

spoof their IP addresses, passive defenses such as auditing the logs sufficed to trace their identities. As for the more experienced perpetrators, access to the intermediate computers used for laundering their network traffic was needed in order to trace them. For computers located in the less friendly countries, cyber exploitation might have been used to gain access. Thereafter, with more analysis, subsequent cyber attacks could be launched to shut down the attackers' systems. If the computers were located in friendly countries, the computers could be seized and analyzed through legal means.

Subsequent waves of attacks were observed to be highly coordinated and had central command and control features.[117] As mentioned in chapter three, one way to stop such attacks is to take down the C&C servers. If they are found to be located in a cooperative country, the approach against the Coreflood botnet can be adopted. If not, cyber exploitations and attacks could be used to try to shut down the attacks. For example, after obtaining the IP address of an attacking computer from the firewall logs, that attacking computer could be exploited. After that, a thorough analysis on that computer could be conducted, potentially revealing the IP address of the C&C server. Thereafter, the C&C server can be exploited so as to determine the culprit responsible for the attack. To stop further attacks, the server can be shutdown through a cyber attack.

Several of the IP addresses involved in the attack were traced to Russia, with some of them belonging to Russian state institutions.[118] However, given that the computers themselves could have been compromised and under the control of a botnet owner, there was insufficient evidence to determine the true culprit.[119] While the Russian government was accused of the attacks, it denied allegations.[120] However, the true attacker may have been determined if the attack computers in Russia could have been examined for further analysis. Of course, that would have required cooperation from the Russian ISPs and authorities. But, if that were lacking, the computers could have been

[117] "International Cyber Incidents: Legal Considerations," 23.

[118] "Russia Accused of Unleashing Cyberwar to Disable Estonia."

[119] "International Cyber Incidents: Legal Considerations," 23.

[120] "Estonia Hit by 'Moscow Cyber War,'" *BBC News*, 17 May 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

exploited remotely so that the analysis could be carried out. Likewise, botnets located elsewhere and involved in the attacks could be approached in the same manner.

Another possibility of employing active cyber defense in this scenario would be to tamper with the script used for the cyber attacks. As reported, a downloadable batch of scripts designed to ping flood Estonian websites were posted to several Russian language message boards.[121] Given the lack of cooperation from Russia,[122] the sites hosting these message boards could have been hacked. Thereafter the script could be modified so that it would do something instead of launching the attack. At the same time, the sites could be monitored to track the attacker's whereabouts.

D. STUXNET

1. Overview

The first of its kind, Stuxnet is a sophisticated computer worm that targets industrial control systems. It was first discovered on computers in Iran by VirusBlokAda, an IT security firm based in Belarus, in June 2010.[123] However, from the in-depth analysis by Symantec, the worm was confirmed to have existed at least one year prior.[124] The worm spreads by exploiting several software vulnerabilities in the Microsoft Windows operating systems, and is capable of spreading via removable devices (such as USB drives). After infecting a new computer, the worm can contact a command and control server for any instructions, including upgrading itself. This worm was designed to locate specific industrial control systems and modify the code on the corresponding Siemens programmable logic controllers (PLCs) for malicious purposes.[125] Some sources

[121] Eneken Tikk et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," Cooperative Cyber Defence Centre of Excellence (November 2008): 10.

[122] Eneken Tikk and Kadri Kaska, "Legal Cooperation to Investiage Cyber Incidents: Estonia Case Study and Lessons," *Proceedings of the 9th European Conference on Information Warfare and Security*, (2010): 288–295.

[123] Robert McMillan, "Siemens: Stuxnet Worm Hit Industrial Systems," *Computerworld*, 14 September 2010, http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems.

[124] "W32.Stuxnet Dossier Version 1.4," 2.

[125] Ibid., 1.

have suggested that Stuxnet was designed to sabotage Iran's Bushehr nuclear reactor.[126] Others suggested that Stuxnet targeted the nuclear facility at Natanz, due to its particular configuration.[127] As reported by Symantec, Stuxnet sought out very specific industrial control systems, and 60 percent of the 100,000 infected computers were located in Iran.[128]

2. How Could Active Cyber Defenses Have Helped in This Scenario?

Since Stuxnet was discovered, several resources have been made available to guide others in terms of defending against industrial control system attacks.[129] However, they are passive in nature, and may not be sufficient in determining the identity of the attacker as discussed in the earlier chapter. As with the other cases mentioned above, active cyber defenses could have helped address the issue of attribution. While Iranian intelligence claimed that enemy spy services were responsible for Stuxnet, there is inadequate evidence to prove this. As published by Symantec, several references within the Stuxnet code could simply have been misdirection on the part of the attackers.[130] Apart from the references, Symantec found that the command and control servers used by Stuxnet were located in Malaysia and Denmark.[131] These servers could have been seized or exploited via cyber means to gain insight to the attackers. If the identity of the attackers could be confirmed, appropriate legal and/or political actions could follow.

[126] Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?" *PCWORLD*, 21 September 2010, http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

[127] Kim Zetter, "Report Strengthens Suspicions That Stuxnet Sabotaged Iran's Nuclear Plant," *Wired*, 27 December 2010, http://www.wired.com/threatlevel/2010/12/isis-report-on-stuxnet/.

[128] "W32.Stuxnet Dossier Version 1.4," 5–6.

[129] Richard Stiennon, "Defending Against Stuxnet," http://www.intelligentwhitelisting.com/blog/defending-against-stuxnet.

Anup Ghosh, "Defending Against Stuxnet Type Threats," *Invincea*, 1 Oct 2010, https://www.invincea.com/blog/2010/10/defending-against-stuxnet-type-threats/.

[130] Gregg Kelzer, "Iran Arrests 'Spies' After Stuxnet Attacks on Nuclear Program," *Computerworld*, 2 October 2010, http://www.computerworld.com/s/article/9189218/Iran_arrests_spies_after_Stuxnet_attacks_on_nuclear_program.

[131] "W32.Stuxnet Dossier Version 1.4," 21.

Another possible active cyber defense for this case is in the form of cyber counter attack. Based on the study by Symantec, there was a possible attack scenario in which an early version of Stuxnet or other malicious binary would steal and upload the industrial control system (ICS) schematics from compromised systems to some servers.[132] Thereafter, the attacker would develop a newer version of Stuxnet, tailored specifically for the ICS facility.

In this setting, special Trojans could be embedded in the documents containing the schematics. When the documents are accessed on a friendly computer, the Trojan will not take any actions. (Unique signatures could be hidden within the computers of legitimate users thereby allowing the Trojan to identify them as friendly computers. Any other computers accessing the document will then be deemed as hostile.) However, if the documents are accessed on a hostile computer, the Trojan will become active. It will capture system and network information, and send it back to the investigators alerting them of the compromise. This information, together with various documents extracted from the hostile computer, can assist in identifying the attacker.

In addition, some of the documents with the ICS schematics could contain misleading or false information. When attackers try to interpret the information, they will be led astray.

Regardless, Stuxnet has demonstrated a new threat to ICS. As Ralph Langner, a well-respected expert in industrial control systems security, pointed out, "The problem is not Stuxnet. Stuxnet is history. The problem is the next generation of malware that will follow."[133] Stuxnet has shown the world that it is possible to cripple industrial control systems, and that is an attractive option for hostile states (and non-states alike). The Poneman Institute reported that the majority of companies in the energy sector are not prepared to defend against such threats.[134] To make things worse, the source code of

[132] "W32.Stuxnet Dossier Version 1.4," 3.

[133] "Was Stuxnet Built to Attack Iran's Nuclear Program?"

[134] Anthony Freed, "Report Shows Energy Infrastructure Susceptible to Attack," *Infosec Island*, 7 April 2011, https://www.infosecisland.com/blogview/12808-Report-Shows-Energy-Infrastructure-Susceptible-to-Attack.html.

Stuxnet has been made available on the Internet.[135] This implied that new and perhaps even more sophisticated variants of Stuxnet could be created with greater ease. In view of this, it is crucial to strengthen measures to deter potential attackers. As Patrick Morgan highlighted, a good cyber deterrence posture needs to include "capacities for suitable retaliation."[136] Cyber exploitation could contribute to attributing the attacker, while cyber counter attack would be a suitable retaliation.[137]

E. CONCLUSION

This chapter has shown how active cyber defenses could have made a difference in three major incidents, particularly in the areas of attribution. Should there be sufficient intelligence suggesting an imminent threat, a corresponding preemptive cyber attack can be launched against the hostile state, thereby preventing the cyber attack.

Active cyber defenses could be employed in ways similar to that of espionage and covert actions conducted by intelligence agencies. For example, according to Dr. David Perry from the University of Santa Clara, the CIA has recruited agents in foreign countries to help provide intelligence, as well as plot assassinations of various foreign leaders.[138] In a cyber context, the computer network of a hostile state could be exploited and network sensors installed. These sensors could have functionalities similar to those of an intrusion detection system or network packet sniffer. When the sensors detect activities that suggest the threat of a cyber attack, the network or corresponding servers could be disrupted and/or shutdown.

While such active cyber defenses may be considered inappropriate, some have argued that these are acceptable as they are part of self-defense. One such individual is

[135] "The Stuxnet Source Code Available Online," *PenTestIT*, 4 July 2011, http://www.pentestit.com/2011/07/04/stuxnet-source-code-online.

[136] Patrick Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, National Research Council (Washington, DC: The National Academies Press),75.

[137] As a further deterrent, the new U.S. policy highlighted earlier, states that counter attack could also be in the form of kinetic response.

[138] Dr. David Perry, "Repugnant Philosophy: Ethics, Espionage, and Covert Action," Markkula Center For Applied Ethics, Santa Clara University, http://www.scu.edu/ethics/publications/submitted/Perry/repugnant.html.

Professor Jay Kesan of the University of Illinois at Urbana-Champaign. In his forthcoming paper “Mitigative Counterstrike: Self-Defense and Deterrence in Cyberspace,” he argues that self-defense “is accepted as an essential element of protection in virtually all other legal contexts, and should be preserved in the cyber realm.”[139] In the case of the cyber attacks on Estonia, this argument suggests that Estonia could have conducted cyber exploitation and/or attacks on the Russian ISPs (where the attacks were last traced to) as a form of self-defense.

[139] “Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,” 92.

V. CONCLUSION

A. SUMMARY

This thesis has studied different types of cyber attacks and the limitations of existing passive defenses against them. It has proposed augmenting these passive measures with active ones and explored typologies of active cyber defenses and the benefits they can offer to an overall cyber defense posture. Three prominent cases of cyber attacks were used to illustrate how active cyber defenses could have made differences in defending against the attacks.

Active cyber defenses are not meant to replace passive defenses. Rather, they are meant to complement the latter, and should be considered in any national level cyber program. This concluding chapter summarizes the benefits and typologies of active cyber defense. It briefly lays down some technical and legal considerations, and then highlights some areas of possible future research.

B. ACTIVE CYBER DEFENSE

Active cyber defenses may one day offer strategic advantages similar to those for active defenses in conventional warfare. They can help establish attribution of a cyber attack, deter attacks by creating the fear of retaliatory attacks in potential attackers, or even preempt an imminent attack. The typologies of active cyber defense are cyber exploitation, counter cyber attack, preemptive cyber attack, and preventive cyber attack.

Cyber exploitation refers to the hacking of third party or the attackers’ computers and networks for the purpose of gaining information about the attack, including the source of the attack, the methods and tools used, the scope of the attack, and data that may have been taken. Cyber exploitation, when carefully carried out, need not disrupt target computers and may even goes undetected.

Counter cyber attack refers to the launching of a cyber attack against an attacker. The objective could be to interrupt an attack in progress and limit its effects. The counter attack could take the form of DOS attack or intrusion into the attacker’s network.

Alternatively, if the attacker is stealing sensitive documents, it could take the form of booby-trapping the documents with a remote-controlled Trojan, which then could be used to collect information about the attacker and/or shut down the attacker's computer or network.

Preemptive cyber attack refers to the launching of a cyber attack against an adversary in anticipation of an imminent cyber attack. Preventive cyber attack refers to the launching of a cyber attack against an adversary based on a judgment that the adversary will be attacking.

C. CONSIDERATIONS

1. Technical Considerations

In order to employ active cyber defenses successfully, the defender must have the capability to launch a cyber exploitation or cyber attack. Unless the defender is launching a simple DOS attack, this means that the defender must be able to exploit some vulnerability on the attacking computer or network. To improve the chances of success, it would be best to exploit a zero-day vulnerability since known vulnerabilities may have been patched on the target system. However, exploiting a zero-day vulnerability requires either an internal research program or access to researchers who are willing to provide information and exploit tools for zero-days on a confidential and sole-source basis. Finding zero-day vulnerabilities can be resource intensive, particularly when the researchers do not have access to the software code and need to reverse engineer the software. Even if the software code is available, the process of code auditing can be onerous due to the lengthy lines of code and vast numbers of software and hardware systems to investigate. To make matters worse, the process needs to be ongoing. New versions of software and operating systems are rolled out periodically, and it is uncertain when they will be adopted. When that happens, previously found zero-day vulnerabilities would likely be rendered useless. While there is a market for buying and selling zero-day vulnerabilities,[140] it is still important for any government to have its own capability, or a set of dedicated researchers who are working toward it. The reason is that the government would need to verify the zero vulnerability (or exploit) it intends to purchase, as well as subsequently develop or customize the exploit to suit its needs. Also, without the dedicated resource, it may not be able to react promptly when faced with a cyber attack.

To limit the impact of a cyber attack, it is crucial to stop the attack quickly. This means that the defender must have cyber tools for active defense, including zero-day exploit tools, ready at hand, along with the knowledge about how to use them. In an analogy to conventional warfare, for a counter attack to be useful, the defender must first have troops that are well trained in warfare. If the defender only starts drafting soldiers and training them when an adversary is attacking, it will be too late. A city may be overrun before any counter attack can take place. Soldiers need to be trained and well equipped, so that they can be deployed at any time. In the cyber aspect, the defender must have adequate exploits in place to launch a successful counter attack. Moreover, if the defender intends to booby-trap sensitive documents that the attacker is downloading, the defender needs to be able to detect the attacker's activity and insert a Trojan into the stolen files while the attack is in progress and without slowing down the attacker's downloads.

2. Nontechnical Considerations

Conducting cyber attacks, including active cyber defense, is controversial. Widely accepted principles for fighting conventional wars have been encoded in the international law of armed conflict (LOAC), which includes the Geneva and Hague Conventions, and the UN Charter. But what about cyber attacks? Would it be legal and ethical under the LOAC to conduct a defensive cyber attack (be it a counter, preventive, or preemptive attack) against another nation? And what would the appropriate justifications be? In the cyber attack against Estonia, given the lack of assistance from the Russian government,

[140] Jordan Robertson, "Google Attack Highlights 'Zero-Day' Black Market," *Seattle Times*, 28 January 2010, http://seattletimes.nwsource.com/html/businesstechnology/2010916578_apustecchinagooglesecurityhole.html.

would it have been acceptable for Estonia to launch a cyber attack or exploitation against those computers in Russia? Or in the case of GhostNet, would it have been lawful for the various countries infected by Gh0st RAT to conduct cyber exploitations and counter cyber attacks against the service providers and computers located in China? Would attacking the service providers, being uninvolved third parties, have been deemed acceptable collateral damages? In conventional war, these actions could be defended on the basis of self-defense when non-excessive collateral damage is often acceptable. However, at present, there is considerable uncertainly in addressing these issues under international law and the lack of a unified framework.[141] Finally, apart from these, the ethics of cyber attacks need to be considered too.

D. FURTHER RESEARCH

Looking at the above-mentioned considerations, there are some possible avenues for future research. One important issue to note is that the research time required to find new vulnerabilities and exploits needs to be reduced. As discussed, often computer systems are upgraded with newer versions of software. If it takes too long to find a zero-day vulnerability, then a working exploit may not be available when the need for a counter cyber attack arises. At present, researchers rely on both manual efforts and automated tools, such a fuzzer,[142] to send multiple malformed data into software, forcing them to crash. Then, by analyzing the crash information and further manipulation of the malformed data, the researcher may be able to generate software code to exploit the vulnerability that caused the crash. However, this whole process is challenging and tedious and often fails to yield results. As such, any research in improving the process of vulnerability detection and exploit generation would be very helpful.

Another possible area of research would be in the automation of Trojan injection into documents. One of the counter cyber attack examples described above involves the insertion of a Trojan into documents that the attacker was detected to be downloading. An automated system needs to be in place to facilitate that detection and automatically

[141] "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," 64.

[142] "Fuzzing," OWASP, https://www.owasp.org/index.php/Fuzzing.

insert the Trojan into the relevant documents. This could be something similar to that of an Intrusion Detection System (IDS), but with the ability to alter the content of the documents in real time.

A third area of research is in the policy area. As Professor Jay Kesan mentioned in his paper "Mitigative Counterstrike," there is a need "to legally solidify the right to use self-defense in cyberspace, while also protecting the rights of potential uninvolved third parties who might be harmed by mitigative counterstrikes."[143] Thus, further research could be conducted so as to construct a framework for new cyber-specific legal principles that could be adopted by the international community. The framework should complement existing international laws and address the use of active cyber defenses, particularly conditions under which their use would be appropriate; privacy issues; and collateral damage. In this regard, the U.S. has reportedly started crafting such a legal framework.[144] However, until it is completed and accepted by other nations in the world, the use of active cyber defense is likely to continue to engender controversy.

[143] "Mitigative counterstriking: Self-Defense and Deterrence in Cyberspace," 3.

[144] Jim Wolf, "U.S. Crafting Framework for Cyber Offense: General," *Reuters*, 19 October 2011, http://www.reuters.com/article/2011/10/19/us-usa-cyber-warfare-idUSTRE79I2MS20111019.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"1967: Israel launches attack on Egypt." *BBC News*. http://news.bbc.co.uk/onthisday/hi/dates/stories/june/5/newsid_2654000/2654251.stm.

"1981: Israel Bombs Baghdad nuclear reactor." *BBC News*. http://news.bbc.co.uk/onthisday/hi/dates/stories/june/7/newsid_3014000/3014623.stm.

"Akamai Security Solutions." Akamai. http://www.akamai.com/html/solutions/security/ddos_defense.html.

"Automated Correction of Bad IT Configurations." Tripwire. http://www.tripwire.com/it-compliance-products/te/remediation/.

Beidel, Eric, and Stew Magnuson. "Government, Military Face Severe Shortage of Cybersecurity Experts." *National Defense Magazine*. August 2011. http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx.

Belenky, Andrey and Nirwan Ansari. "IP Traceback with Deterministic Packet Marking." *IEEE Communications Letters*, vol. 7, no. 4, April 2003.

Bishop, Matt, C. Gates, and J. Hunker. "The Sisterhood of the Traveling Packets." *In Proceedings of the 2009 Workshop on New Security paradigms*, 2009.

Boebert, W. Earl. "A Survey of Challenges in Attribution." *Proceedings of a workshop on Deterring CyberAttacks*, National Academy of Sciences. http://www.nap.edu/catalog/12997.html.

"Botnets." Shadowserver. http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets.

Bradley, Tony. "Zero Day Exploits." Internet/Network Security, About.com. http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm.

Brenner, Bill. "Black Hat 2007: Estonia attacks were a cyber riot, not warfare." 3 August 2007. http://searchsecurity.techtarget.com/news/1266728/Black-Hat-2007-Estonian-attacks-were-a-cyber-riot-not-warfare.

Carafano, James. "Getting Cyber-Serious? – FBI Targets Botnet." *Security Debrief*, 21 April 2011. http://securitydebrief.com/2011/04/21/getting-cyber-serious-fbi-targets-botnet/.

Casey, Bryan. “Over 8000 New Vulnerabilities Disclosed in 2010 – That’s a Record.” The IBM Institute for Advanced Security Expert Blog, 31 March 2011. http://www.instituteforadvancedsecurity.com/expertblog/2011/03/31/over-8000-new-vulnerabilities-disclosed-in-2010-thats-a-record/.

Charter of the United Nations. http://www.un.org/en/documents/charter/chapter7.shtml.

“China Denies Any Role in GhostNet Computer Hacking.” *Voice of America*, 31 Mar, 2009. http://www.voanews.com/english/news/a-13–2009–03–31-voa12–68812997.html?CFTOKEN=37567981&CFID=253397922&jsessionid=843016046241f811765c716e398086338793.

Clark, David, and Susan Landau. “Untangling Attribution.” *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. http://www.nap.edu/catalog/12997.html.

Clover, Charles. “Kremlin-backed group behind Estonia cyber blitz.” *Financial Times*, 11 March 2009. http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3–0000779fd2ac.html#axzz1XqpZTRzc.

Colonel Marshall, S.L.A. “Bastogne The First Eight Days.” *U.S. Army In Action Series*, The Center of Military History. http://www.history.army.mil/books/wwii/Bastogne/bast-fm.htm.

Conficker Working Group. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Introduction.

Council of Europe’s Convention on Cybercrime. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp.

“Cyber Command achieves full operational capability.” Air Force Space Command, 3 November 2010. http://www.afspc.af.mil/pressreleasearchive/story.asp?id=123229293.

“Cybercrime: The next wave.” McAfee Virtual Criminology Report, 2007.

Defense Technical Information Center. http://www.dtic.mil/doctrine/jel/doddict/data/c/01331.html.

Dignan, Larry. “Iran admits Stuxnet hurt nuclear programme.” *ZDNet*, 30 November 2010. http://www.zdnet.co.uk/news/security-threats/2010/11/30/iran-admits-stuxnet-hurt-nuclear-programme-40091018/.

Espiner, Tom. “Estonia’s cyberattacks: Lessons learned, a year on.” *ZDNet*, 1 May 2008.

http://www.zdnet.co.uk/news/security-threats/2008/05/01/estonias-cyberattacks-lessons-learned-a-year-on-39408158/.

"Estonia hit by 'Moscow cyber war'." *BBC News*, 17 May 2007. http://news.bbc.co.uk/2/hi/europe/6665145.stm.

Freed, Anthony. "Report Shows Energy Infrastructure Susceptible to Attack." *Infosec Island*, 7 April 2011. https://www.infosecisland.com/blogview/12808-Report-Shows-Energy-Infrastructure-Susceptible-to-Attack.html.

"Fuzzing." OWASP. https://www.owasp.org/index.php/Fuzzing.

Gershwin, Lawrence. "Cyber Threat Trends and U.S. Network Security." Statement for the Record to the Joint Economic Committee. National Intelligence Council, 21 June 2001. http://www.dni.gov/nic/testimony_cyberthreat.html.

Ghosh, Anup. "Defending Against Stuxnet Type Threats." *Invincea*, 1 Oct 2010.https://www.invincea.com/blog/2010/10/defending-against-stuxnet-type-threats/.

"Glossary." McAfee. http://home.mcafee.com/VirusInfo/Glossary.aspx.

Gorman, Siobhan and Fidler, Stephen. "Cyber Attacks Test U.S, Allies, and Foes." *Wall Street Journal Online*, 25 September 2010. http://online.wsj.com/article/SB10001424052748703793804575511961264943300.html.

Gorman, Siobhhan and Julian Barnes. "Cyber Combat: Act of War." *The Wall Street Journal Online*, 31 May 2011. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

Heickero, Roland. "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations." 2010.

Hollis, Duncan B. and David G. Post. "Do Cyber-Attacks Require a Duty to Assist?" *Law Technology News*, April 29, 2010. http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202453759405&slreturn=1&hbxlogin=1.

Hunker, Jeffrey, Bod Hutchinson, and Jonathan Margulies. "Role and Challenges for Sufficient Cyber-Attack Attribution." Institute for Information Infrastructure Protection, January 2008. http://ww.thei3p.org/docs/publications/whitepaper-attribution.pdf.

HTTP Tunnel. http://www.http-tunnel.com/html/.

IBM X-Force. http://www-03.ibm.com/security/landscape.html.

Ide, William. “Iranian Hackers Attack VOA Internet Sites.” *Voice of America*, 22 February 2011. http://www.voanews.com/english/news/usa/Iranian-Hackers-Attack-VOA-Internet-Sites-116678844.html.

“Information Security Policy Templates.” SANS, http://www.sans.org/security-resources/policies.

“Introducing Bouncer by CoreTrace.” CoreTrace. http://www.coretrace.com/products/BOUNCER_by_CoreTrace/default.aspx.

“Iraq War and Information Security.” F-Secure, 28 March 2003. http://www.f-secure.com/virus-info/iraq.html.

Jayawal, Vikas, William Yurcik, and David Doss. “Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?” June 2002. http://www.scribd.com/doc/38380481/Internet-Hack-Back-Counter-Attacks-as-Self-Defense-or-Vigilantism.

Jones, Keith, Richard Bejtlich, and Curtis Rose. *Real Digital Forensics*. New Jersey: Addison-Wesley, 2008.

Kelzer, Gregg. “Iran arrests ‘spies’ after Stuxnet attacks on nuclear program.” *Computerworld*, 2 October 2010. http://www.computerworld.com/s/article/9189218/Iran_arrests_spies_after_Stuxnet_attacks_on_nuclear_program.

Kesan, Jay P., and Carol M. Hayes. “Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace.” April 2011. http://search.proquest.com/docview/864222100?accountid=12702.

Kristof, Nicholas. “The Osirak Option.” *The New York Times*. http://www.nytimes.com/2002/11/15/opinion/the-osirak-option.html.

Landler, Mark, and John Markoff. “Digital Fears Emerge After Data Siege in Estonia.” *The New York Times*, 29 May 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html.

Leder, Felix, Tillmann Werner, and Peter Martini. “Proactive Botnet Countermeasures – An Offensive Approach.” NATO Cooperative Cyber Defence Centre of Excellence, March 2009.

http://www.ccdcoe.org/publications/virtualbattlefield/15_LEDER_Proactive_Coutnermeasures.pdf.

Lefkow, Chris. “U.S. disables Coreflood botnet, seizes servers.” *PHYSORG.COM*, 13 April 2011. http://www.physorg.com/news/2011–04-disables-coreflood-botnet-seizes-servers.html.

Libicki, Martin. *What is Information Warfare?* Institute for National Strategic Studies, National Defense University, August 1995. http://www.ndu.edu/inss/actpubs/act003/a003ch03.html.

Lukasik, Stephen J. “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains.” *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council, 2010.

Markoff, John. “Vast Spy System Loots Computers in 103 Countries.” *The New York Times*, 28 March 2009. http://www.nytimes.com/2009/03/29/technology/29spy.html.

Matrosov, Aleksandr, et al. “Stuxnet Under the Microscope.” Revision 1.31, ESET, 23 Jan 2011. http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

McMillan, Robert. “Siemens: Stuxnet worm hit industrial systems.” *Computerworld*, 14 September 2010. http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems.

———. “Was Stuxnet built to Attack Iran’s Nuclear Program?” *PCWORLD*, 21 September 2010. http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

Mead, Nancy, Eric Hough, and Theodore Stehney. “Requirements Engineering (Square) Methodology).” Carnegie Mellon Software Engineering Institute, November 2005. http://www.cert.org/archive/pdf/05tr009.pdf.

Mills, Elinor. “Zeus Trojan steals $1 million from U.K. bank accounts.” *CNET*, 10 August 2010. http://news.cnet.com/8301–27080_3–20013246–245.html.

Morgan, Patrick. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.” *Proceedings of a Workshop on Deterring Cyber Attacks:Informing Strategies and Developing Options for U.S. Policy*. http://www.nap.edu/catalog/12997.html.

MSDN, Microsoft. SQL Injection. http://msdn.microsoft.com/en-us/library/ms161953.aspx.

NATO Cooperative Cyber Defence Center of Excellence. http://www.ccdcoe.org.

"Overview by the U.S.-CCU of the Cyber Campaign Against Georgia in August of 2008." *U.S.-Cyber Consequence Unit Special Report*, August 2009.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: The National Academies Press, 2009.

Page, Lewis. "MoD networks still malware-plagued after two weeks." *The Register*, 20 January 2009. http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/.

"Passive Defense." Answers.com. http://www.answers.com/topic/passive-defense.

Perry, David. "Repugnant Philosophy: Ethics, Espionage, and Covert Action." Markkula Center For Applied Ethics, Santa Clara University. http://www.scu.edu/ethics/publications/submitted/Perry/repugnant.html.

Robertson, Jordan. "Google attack highlights 'zero-day' black market." *The Seattle Times*, 28 January 2010. http://seattletimes.nwsource.com/html/businesstechnology/2010916578_apusteccchinagooglesecurityhole.html.

SANS. http://www.sans.org/reading_room/whitepapers/covert/.

Soafer, Abraham D., *The Best Defense? Legitimacy and Preventive Force*. Stanford, CA: Hoover Institution Press, 2010.

"Spectrum." Netwitness. http://netwitness.com/products-services/spectrum.

Staniford-Chen, Stuart, and L. Todd Heberlein. "Holding Intruders Accountable on the Internet." *Proceedings 1995 IEEE Symposium on Security and Privacy*, May 1995.

Stiennon, Richard. "Defending Against Stuxnet." http://www.intelligentwhitelisting.com/blog/defending-against-stuxnet.

"The Comphrehensive National Cybersecurity Initiative." National Security Council. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

"The Stuxnet Source Code Available Online." *PenTestIT*, 4 July 2011. http://www.pentestit.com/2011/07/04/stuxnet-source-code-online.

"The Trojan War." http://www.stanford.edu/~plomio/history.html.

"The Vast Reach of GhostNet." *The New York Times*, 28 March 2009. http://www.nytimes.com/imagepages/2009/03/28/technology/20090329_SPY_GRAPHIC.html.

Tikk, Eneken, et al. "Cyber Attacks Against Georgia: Legal Lessons Identified." November 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

Tikk, Eneken, and Kadri Kaska. "Legal Cooperation to Investigate Cyber Incidents: Estonia Case Study and Lessons." *Proceedings of the 9th European Conference on Information Warfare and Security*, 2010.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. "International Cyber Incidents: Legal Considerations." NATO Cooperative Cyber Defence Centre of Excellence, 2010.

TOR Project. http://www.torproject.org/about/overview.html.en.

"Tracking GhostNet: Investigating a Cyber Espionage Network." Information Warfare Monitor, 29 March 2009. http://www.infowar-monitor.net/ghostnet.

Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian*, 16 May 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

U.S. DoD Dictionary of Military and Associated Terms. http://www.dtic.mil/doctrine/dod_dictionary/data/a/2043.html.

"Uses of botnet." The Honeynet Project, 10 August 2008. http://www.honeynet.org/node/52.

Vijayan, Jaikumar. "Update: Duqu exploits zero-day flaw in Windows kernel." *Computerworld*, 1 Nov 2011. http://www.computerworld.com/s/article/9221372/Update_Duqu_exploits_zero_day_flaw_in_Windows_kernel?taxonomyId=85.

"W32.Stuxnet Dossier Version 1.4." Symantec Security Response, February 2011.

Wang, Ping et al. "A New Approach for Solving the IP Traceback Problem for Web Security." *Advances on Information Sciences and Service Sciences*. Volume 3, Number 2, March 2011.

Wheeler, David, and Gregory Larsen. "Techniques for Cyber Attack Attribution." Institute For Defense Analyses, October 2003.

Wildt, Robert. "Should you Counter-Attack when Network Attackers Strike?" *Global Information Assurance Certification Paper*, SANS Institute, 13 December 2000.

Willsher, Kim. "French fighter planes grounded by computer virus." *The Telegraph*, 7 February 2009. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

Wolf, Jim. "U.S. crafting framework for cyber offense: general." *Reuters*, 19 October 2011. http://www.reuters.com/article/2011/10/19/us-usa-cyber-warfare-idUSTRE79I2MS20111019.

Zetter, Kim. "Report Strengthens Suspicions that Stuxnet Sabotaged Iran's Nuclear Plant." *Wired*, 27 December 2010. http://www.wired.com/threatlevel/2010/12/isis-report-on-stuxnet/.

Zone-H.org – Unrestricted information, Yearly & Monthly & Daily attacks. http://www.zone-h.org/stats/ymd.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California