NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERSECURITY "LANES IN THE ROAD" FOR THE DEPARTMENT OF HOMELAND SECURITY

by

David G. Shaffer

June 2016

Thesis Advisor: Erik Dahl
Second Reader: Wade Huntley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE CYBERSECURITY "LANES IN THE ROAD" FOR THE DEPARTMENT OF HOMELAND SECURITY		**5. FUNDING NUMBERS**	
6. AUTHOR(S) David G. Shaffer			
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)

The roles and responsibilities for cybersecurity within the national government are not clearly delineated. This thesis asks if the current allocations of cybersecurity responsibilities to DHS are optimal for achieving national cybersecurity objectives. To answer this question, the evolution of cybersecurity policies within the United States is evaluated, looking specifically at DHS. Additionally, FBI, NSA/DOD, and DNI cybersecurity roles are identified. The Sony Pictures Entertainment cyber-attack is examined as a case study for how a real-world event is handled, and to determine the pros and cons of the current allocation of responsibilities. The evidence from the Sony cyber-attack suggests that the Secret Service, under DHS, is not ready to conduct a proper investigation for a cyber-attack but that the FBI is. This thesis identifies numerous responsibility allocation changes that would streamline cybersecurity at the national level. The main recommendations are that DHS should be the lead agency for improving and strengthening cybersecurity, while the FBI should be the lead agency for investigating cyber-attacks, unless the attack is against one of the people that the Secret Service protects, in which case they should become the lead investigator with direct support from the FBI.

14. SUBJECT TERMS Department of Homeland Security, DHS, cyber, cybersecurity, Sony cyber-attack			**15. NUMBER OF PAGES** 83
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CYBERSECURITY "LANES IN THE ROAD" FOR THE DEPARTMENT OF HOMELAND SECURITY

David G. Shaffer
Lieutenant, United States Navy
B.S., Oregon State University, 2010

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
June 2016**

Approved by: Erik Dahl
Thesis Advisor

Wade Huntley
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The roles and responsibilities for cybersecurity within the national government are not clearly delineated. This thesis asks if the current allocations of cybersecurity responsibilities to DHS are optimal for achieving national cybersecurity objectives. To answer this question, the evolution of cybersecurity policies within the United States is evaluated, looking specifically at DHS. Additionally, FBI, NSA/DOD, and DNI cybersecurity roles are identified. The Sony Pictures Entertainment cyber-attack is examined as a case study for how a real-world event is handled, and to determine the pros and cons of the current allocation of responsibilities. The evidence from the Sony cyber-attack suggests that the Secret Service, under DHS, is not ready to conduct a proper investigation for a cyber-attack but that the FBI is. This thesis identifies numerous responsibility allocation changes that would streamline cybersecurity at the national level. The main recommendations are that DHS should be the lead agency for improving and strengthening cybersecurity, while the FBI should be the lead agency for investigating cyber-attacks, unless the attack is against one of the people that the Secret Service protects, in which case they should become the lead investigator with direct support from the FBI.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CNSS	Committee on National Security Systems
COMINT	Communications Intelligence
CNCI	Comprehensive National Cyber Security Initiative
CMF	Cyber Mission Force
CSD	Cyber Security Division
CTF	Cyber Task Forces
CTIIC	Cyber Threat Intelligence Integration Center
DOD	Department of Defense
DHS	Department of Homeland Security
DOJ	Department of Justice
DNI	Director of National Intelligence
ECSAP	Electronic Crimes Special Agent Program
ECTF	Electronic Crimes Task Force
ELINT	Electronic Intelligence
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FNR	Federal Network Resilience
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act
ITU	International Telecommunication Union
IP	Internet Protocol
NCIJTF	National Cyber Investigative Joint Task Force
NCFTA	National Cyber-Forensics & Training Alliance

NCCIC	National Cybersecurity and Communications Integration Center
NSA	National Security Agency
NSCID	National Security Council Intelligence Directive
NSD	National Security Directive
NSPD	National Security Presidential Directive
CS&C	Office of Cybersecurity and Communications
OEC	Office of Emergency Communications
PDD	Presidential Decision Directive
PPD	Presidential Policy Directive
R&D	Research and Development
SSD	Secret Service Division
SECDEF	Secretary of Defense
SIGINT	Signals Intelligence
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience
TELINT	Telemetry Intelligence
USCYBERCOM	U.S. Cyber Command
USSS	United States Secret Service

ACKNOWLEDGMENTS

I would like to thank both of my advisors, Erik Dahl and Wade Huntley, for their help and support, from figuring out what to write about, all the way to the final product. Additionally, my deepest love and appreciation for my wife, Andrea, and daughter, Rebecca. Andrea is always there for me when I need to take a break and also for when I need to be “gently reminded” that I need to get back to work. Thank you for everything you have done for me and for taking care of Rebecca so I could finish everything.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

With increasing attention on the problem of cybersecurity as a critical aspect of homeland security, many agencies of the federal government, including the Department of Homeland Security (DHS), have established offices that focus on cybersecurity. It is not yet clear what the "lanes in the road" are for government agencies when it comes to addressing cyber threats. This thesis asks the question: Are the current allocations of U.S. cybersecurity responsibilities to DHS optimal for achieving U.S. national cybersecurity objectives? To answer the question this thesis evaluates the evolution of DHS and its role in cybersecurity, along with a review of the cybersecurity roles of the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), Department of Defense (DOD), and the Director of National Intelligence (DNI). The 2014 Sony Pictures Entertainment hack is used as a real-world event case study, to show the pros and cons of the current allocation of responsibilities.

B. SIGNIFICANCE

Fifty years ago, cybersecurity was not an issue. With the evolution of technology and the interconnectedness of the cyber world, it is now at the forefront of national security. Cyberspace provides a common ground for advancing and developing technology that reaches across countries and serves as a link to share ideas that can either benefit or harm the world. The extensive reach of cyberspace that is only lightly regulated can serve as an entry point for adversaries that puts at risk the nation's information system and the critical infrastructures that are linked to it.

In the words of the U.S. *Comprehensive National Security Initiative*, "President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country

are not adequately prepared to counter."[1] This is why multiple agencies have cybersecurity divisions, from the Department of Homeland Security to the Department of Defense. The roles for cybersecurity are blurred, which causes overlapping within the federal government, often causing multiple departments and agencies to respond, committing resources to the same issues with little or no interagency communication. At other times, no agency responds to a cyber threat, since it is unclear which agency is responsible. The overlap also wastes resources; if two or more agencies are preparing or attempting to address an issue, then critical funds are being depleted from many areas instead of the appropriate allocation. Additionally, if agency responsibilities were clear they could then make sure they have the right personnel for the job as opposed to the right personnel being spread across multiple agencies. Overlapping responsibility can cause increased costs, inter-departmental fighting, duplication, loss of the big picture, and failure to accomplish the task.

C. LITERATURE REVIEW

The following literature review is intended to provide background information regarding the research problem: cybersecurity "lanes in the road" for DHS. This review includes sources from the government, academia, and private sector.

Advances in technology have had an impact on everyone's life. A smartphone that is only a little larger than a deck of cards can "email, text and talk to each other, take pictures, get directions, watch television, control home appliances, read the news, play games and manage schedules."[2] While this new technology has helped people in many ways, it has also created a new route for crime and increased the need for security. Former NSA Director Mike McConnell says, "There are two kinds of organizations: those that have been penetrated and are aware, and those that have been penetrated and are unaware."[3] Going along with McConnell, DNI Clapper feels that cyber now poses a

[1] Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative*, accessed August 21, 2015, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[2] Partnership for Public Service, and Booz Allen Hamilton, "Cyber In-Security II: Closing the Federal Talent Gap, April 2015, 1, http://ourpublicservice.org/publications/viewcontentdetails.php?id=504.

[3] Partnership for Public Service, and Booz Allen Hamilton, "Cyber In-Security II."

larger threat then terrorism.[4] The main issue is the number of cyber-attacks that happen. Most of those cyber-attacks are at the low or moderate level of skill, but the vast number of attacks is what causes the problem.[5]

In the paper, "Importance of Cyber Security," Rajesh Kumar Goutam argues that cybercrime is increasing throughout the world and therefor increases the need for cybersecurity.[6] The International Telecommunication Union (ITU) agrees with the need for cybersecurity and holds that "many end-users … lack the awareness and resources to manage cyber-security risks adequately."[7] This is mitigated by capacity building for cybersecurity, and ensuring that a culture of cybersecurity is present at every level.[8] The idea of needing cybersecurity alone is not universal, and Ulrik Franke and Joel Brynielsson identify that not only is cybersecurity important but cyber situational awareness is of greater importance.[9] Situational awareness is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."[10] Cyber situational awareness is situational awareness but applied to cyberspace.[11] Both see situational awareness as being above cybersecurity, and that with enough situational awareness, cybersecurity would become an afterthought.[12]

---

[4] Aaron Boyd, "DNI Clapper: Cyber Bigger Threat Than Terrorism," *Federal Times*, February 4, 2016, http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/.

[5] Ibid.

[6] Rajesh Kumar Goutam, "Importance of Cyber Security," *International Journal of Computer Applications* 111, no. 7 (2015), http://research.ijcaonline.org/volume111/number7/pxc3901250.pdf.

[7] Eric Lie, Rorry Macmillan and Richard Keck, "Cybersecurity: The Role and Responsibilities of an Effective Regulator" (draft background paper, International Telecommunications Union, Beirut, Lebanon, November 2009) 11, http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

[8] Ibid.

[9] Ulrik Franke and Joel Brynielsson, "Cyber Situational Awareness: A Systematic Review of the Literature," *Computers and Security* 46 (2014): doi: 10.1016/j.cose.2014.06.008.

[10] Ibid.

[11] Ibid.

[12] Ibid.

Cybersecurity at the international level is one of the main focuses for many states. Some states are working on lowering the burden of proof for state activity in cyber activities in order to shape their cybersecurity in a more defensive or military manner.[13] While some states are working on increasing their military national cybersecurity other states are working on increasing the international thresholds for cyber use of force and cyber armed attacks, so that cyber espionage and other forms of cyber activities can be undertaken without fear of international retaliation.[14]

Some corporate leaders feel that it is their responsibility to protect their company and customers from cyber threats that originate from within the United States and the United States government should not deal with internal cybersecurity. The federal government, according to this view, should only be concerned with foreign states conducting cyber-attacks.[15] On the other hand, the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency feels that, "there are issues—consumer safety or national defense—where the market response will always be inadequate."[16] From this statement it can be seen that the idea of individual companies providing their own cybersecurity with no regulation or input from the government is not seen as a good answer. To help cybersecurity for the government and private sector information sharing is vital. The sharing of cyber intelligence can help or hinder cybersecurity across the board and currently that sharing still needs better development in order to be useful.[17]

---

[13] Scott J. Shackelford and Richard B. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," *Georgetown Journal of International Law* 35, no. 1 (2003): 17, http://www.lexisnexis.com.libproxy.nps.edu/lnacui2api/api/version1/getDocCui?lni=53YF-4BH0-02C9-F0KV&csi=270944,270077,11059,8411&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true.

[14] Ibid.

[15] Suzanne C. Nielsen, "Pursuing Security in Cyberspace: Strategic and Organizational Challenges," *Orbic* 56, no. 3 (2012): 348, http://www.sciencedirect.com.libproxy.nps.edu/science/article/pii/S0030438712000300.

[16] Ibid.

[17] Thomas D. Wagner, "Sharing Cyber Intelligence in Trusted Environments: A Literature Review," Birmingham City University, accessed on May 20, 2016, 5, https://www.bcu.ac.uk/Download/Asset/633bd91b-4d73-e511-80ce-005056831842.

Secretary of Defense Robert Gates has said he believes the Pentagon does not have enough people with the right skills in order to address cybersecurity.[18] In 2009, the report, "Cyber In-Security: Strengthening the Federal Cybersecurity workforce," written by the Partnership for Public Service and Booz Allen Hamilton, found that Secretary Gates was correct and that the government was having issues with recruitment and retention of skilled cybersecurity personnel.[19] In 2015, the next report from the Partnership for Public Service and Booz Allen Hamilton, "Cyber In-Security II: Closing the Federal Talent Gap," found that the findings in their report from 2009 were still accurate for the most part.[20] The government is on the right path for recruiting and retaining cybersecurity personnel, the momentum for the changes required is almost non-existent though. The federal government is not a competitive employer when compared to the private sector for cyber-trained personnel.[21]

Who should be in charge of cybersecurity is widely debated. Melissa Hathaway, formerly the National Security Council senior director for cyberspace, argues that the White House needs to take the lead for cybersecurity efforts and needs to put out more specific guidance for the agencies to follow.[22] Hathaway also argues that the agencies have too many overlapping authorities for cybersecurity, and that they do not see the large picture needed to meet the challenges for the country.[23] A single agency not understanding the larger picture could have disastrous effects on cybersecurity, if they think the right actions are being taken but those actions do not meet the current objectives or threats.

---

[18] Partnership for Public Service, and Booz Allen Hamilton, "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," July 2009, 2, https://www.boozallen.com/content/dam/boozallen/media/file/CyberIn-Security_2009.pdf.

[19] Ibid.

[20] Partnership for Public Service, and Booz Allen Hamilton, "Cyber In-Security II," 1.

[21] Ibid.

[22] Jaikumar Vijayan, "Cybersecurity Official Says White House should Lead," *Computerworld* 43, no. 16 (2009): 6, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/34185659?accountid=12702.

[23] Ibid.

Arben Asllani, Charles Stephen White, and Lawrence Ettkin have a completely different view of how cybersecurity should be thought of and handled. They feel that cybersecurity should be treated as a public good, such as public safety.[24] They see no legal difference between the government ensuring safety on the street or in food processing to ensuring safety in cyberspace.[25] Treating cybersecurity as a public good would justify the government, at all levels, to improve and regulate cybersecurity. The authors provide six different aspects of how the government should provide cybersecurity. First, public education on cybersecurity needs to be taught at schools to improve general understanding of its importance. Second, a better framework for fighting cybercrime through the criminal justice system needs to be established. Third, once that framework is implemented then cyberterrorism needs to be fought and the perpetrators brought to justice. Fourth, information security needs to be regulated for who has access to personal information that is stored in electronic form. Fifth, the Internet needs to be regulated for content, but ensuring that the First Amendment is not violated. Finally, the pre-established patent, copyright, and trademark laws need to be better enforced on the Internet. If the government starts treating cybersecurity as a public good and does the six things listed, then our nation's cybersecurity efforts will remain ahead of our adversaries.[26]

According to Paul Kurtz, the former executive director of the Cyber Security Industry Alliance, the United States issue with forward progress for cybersecurity is that there is a lack of leadership and therefor guidance on what to do and when to do it.[27] Furthering the idea that nobody knows who is in charge of cybersecurity is Senator Barbara Mikulski. She argues that the nation needs "clarification of who is in charge" for

---

[24] Arben Asllani, Charles Stephen White, and Lawrence Ettkin, "Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals," *Journal of Legal, Ethical and Regulatory Issues* 16, no. 1 (2013): 9, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1370351181?accountid=12702.

[25] Ibid.

[26] Ibid.

[27] "White House, Congress Flunk on Cyber Security, CSIA Says," *TechWeb*, December 14, 2005, 1, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/201509659?accountid=12702.

cybersecurity.[28] Mark D. Young looked at the entire government focusing on DOD for cybersecurity and argued that the allocation of resources is not the problem; instead it is the lack of specific doctrine. He discusses the top-down approach in government with the White House at the top putting out requirements and then the departmental level adds to those requirements and so on. His main argument is that the established policy is not specific enough. A cyber-doctrine is needed to establish what the goal is enabling groups to train and build a skilled cyber force.[29]

There are multitudes of ideas for the issue of who should be in charge of U.S. national cybersecurity efforts. The argument that cybersecurity responsibility does not fall to one agency but is the responsibility of everyone is commonly heard. This concept relates to the idea that no one entity can secure cyberspace without the help of everyone that has access to that system. The requirement for collaboration is seen numerous times in the literature; many experts argue that everyone has a role to play in cybersecurity, from an individual person all the way up to the government. Christine de Souza, for example, argues that no single agency should take the lead on cybersecurity but that all government agencies and private industries should take responsibly for their own cybersecurity. With each entity responsible for their own cybersecurity, collaboration between agencies would play a vital role for the nation's cybersecurity.[30] A national cybersecurity effort can only be achieved when everyone involved works together. The different communities need to establish a framework for the public, private, and individual levels, enabling them to collaborate on furthering cybersecurity efforts.[31] According to Melissa E. Hathaway, no cybersecurity entity has been keeping up with the

---

[28] John Curran, "U.S. Should Clarify Leadership Roles in Cybersecurity, Sen. Mikulski Says," Cybersecurity Policy Report, August 2, 2010, 1, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/746442266?accountid=12702.

[29] Mark D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law and Policy* 4, no. 173 (2010), http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf.

[30] de Souza, "National Cyber Security."

[31] Eric Lie, Rorry Macmillan and Richard Keck, "Cybersecurity: The Role and Responsibilities of an Effective Regulator" (draft background paper, International Telecommunications Union, Beirut, Lebanon, November 2009) 11, http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

ever changing and evolving threats in cyberspace.[32] The academic side is vitally important to every aspect of cybersecurity. Experts argue the government should encourage the education of cybersecurity to professionals in order to meet the ever-expanding demand for properly trained personnel in both the public and private sectors.[33]

According to a Department of Justice Office of the Inspector General audit of FBI cyber investigation capabilities, 36% of cyber agents feel they do not have the appropriate level of cyber knowledge to conduct investigations.[34] The Deputy Assistant Director of the FBI's Cyber Division, Steven Chabinsky, argues that the audit did not take into account that the FBI agents feel that anything less than 100% is not enough, so it makes sense that they feel they do not know enough about cyberspace.[35] Going along with this the Director of research for the computer security training company, SysAdmin, Audit, Network, and Security Institute, says that the FBI has the best interagency cooperation program for cybersecurity in the entire government, and that if there are any shortcomings it is due to the volume of cases they handle and not because of their personnel.[36] The Director of the FBI, James Comey, feels that the Secret Service's cyber investigation mission and responsibilities should fall under the FBI.[37] Comey feels that it is a waste of resources to have both the Secret Service's electronic crimes taskforce and the FBI's cyber taskforce, and that there should only be the FBI's.[38]

In the article, "Who Should Lead U.S. Cybersecurity Efforts?" Kevin Newmeyer analyzes five different options for the government to improve leadership of cybersecurity.[39] Those five options are: establishing a National Coordinator within the

---

[32] Melissa E. Hathaway, "Leadership and Responsibility for Cybersecurity," *Georgetown Journal of International Affairs*, Special Issue 2012, http://belfercenter.ksg.harvard.edu/files/71-80-hathaway.pdf.

[33] Lie, "Cybersecurity," 11.

[34] Mathew J. Schwartz, "FBI Defends Cyber Investigation Skills," *Information Week* no. 1300 (2011): 19, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/871111525?accountid=12702.

[35] Ibid.

[36] Ibid.

[37] Committee on Oversight and Government Reform, *United States Secret Service: An Agency in Crisis*, H.R. Rep 114, 190 (2015).

[38] Ibid.

[39] Kevin P. Newmeyer, "Who Should Lead U.S. Cybersecurity Efforts?," *Prism* 3, no. 2 (2012).

White House, placing DOD in charge, creating a new cabinet level cyber department and placing it in charge, creating a Director of Cybersecurity, or placing DHS in charge.[40] The argument for establishing a National Cybersecurity Coordinator is not widely supported, but the other four options have a support base behind them.

Placing DOD in charge of the national cybersecurity efforts is one of the options that Newmeyer proposes.[41] This could be a beneficial arrangement since DOD already defends their own systems and is at the leading edge of advancing cybersecurity methods.[42] Placing the DOD in charge would also pose problems, mainly due to the Posse Comitatus Act, which restricts DOD domestic law enforcement activity.[43] August G. Roesener, Carl Bottolfson, and Gerry Fernandez feel that DOD should have the lead for domestic cyber-attacks, and for the defensive and counteroffensive responses in support of any DOD combatant commander, or U.S. national level agency.[44] Agreeing with their assessment is Admiral James A. Winnefeld Jr., who believes that DOD cybersecurity is at the forefront of the field, but could be better. In order for DOD cybersecurity to reach its full potential it needs to have better integration across all the branches and contractors, and it needs to further its culture of cybersecurity.[45] The integration portion can be achieved through increasing the coordination and cooperation for cybersecurity throughout DOD. The culture of cybersecurity is important so that not only those individuals who are charged with cybersecurity are thinking about it, but also, everybody is thinking about it every time they interact with a cyber component.[46] Secretary of Defense Ash Carter feels that having the same person in charge of both NSA

---

[40] Newmeyer, "Who Should Lead."

[41] Ibid., 121.

[42] Ibid.

[43] Ibid.

[44] August G Roesener, Carl Bottolfson, and Gerry Fernandez, "Policy for U.S. Cybersecurity," *Air & Space Power Journal* 28, no. 6 (2014), 38-39, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1652188677?accountid=12702.

[45] Adm. Winnefeld's Remarks at the West Point Cyber Conference, Joint Chiefs of Staff, May 14, 2015, http://www.jcs.mil/Media/Speeches/tabid/3890/Article/589135/adm-winnefelds-remarks-at-the-west-point-cyber-conference.aspx.

[46] Ibid.

and USCYBERCOM is the correct answer.[47] Admiral Rogers, who is serving as the Commander USCYBERCOM and the Director NSA, feels that the goal is not for security over privacy or vice versa but that it is possible to ensure privacy and also ensure protection at the same time.[48] In order to improve the cybersecurity for DOD, the Pentagon is holding a "Hack the Pentagon" event for qualified participants to attempt to hack into a portion of the Pentagon's network.[49]

Kevin Newmeyer's next option is to create a new cabinet level agency or department that would be in charge of national cybersecurity.[50] Establishing a new agency for cybersecurity could fix many of the problems in the current system.[51] Elizabeth A. Myers talks about cybersecurity as a team sport, that the approach should be whole-of-government. She goes on to say that the best alternative would be to create a national level cyberspace operations center. She recommends that a Cyberspace Operations Center should be established at the cabinet level, similar to how the National Counter-Terrorism Center was established; that way the head of the center would have a direct link to the President.[52] Additionally, Joeli R. Field argues that creating a new cybersecurity agency is the only alternative. Field writes that the established agencies do not coordinate with respect to cybersecurity and creating a new agency that is solely responsible for the entire government's cybersecurity would eliminate that problem. Field

---

[47] Remarks by Secretary Carter to U.S. Cyber Command Workforce at Fort Meade, Maryland, U.S. Department of Defense, March 13, 2015, http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/607024.

[48] Karen Parrish, "Privacy or Security in Cyber? Both, NSA Chief Says," U.S. Department of Defense, March 2, 2016, http://www.defense.gov/News-Article-View/Article/684015/privacy-or-security-in-cyber-both-nsa-chief-says.

[49] Statement by Pentagon Press Secretary Peter Cook on DOD's "Hack the Pentagon" Cybersecurity Initiative, U.S. Department of Defense, March 2, 2016, http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

[50] Newmeyer, "Who Should Lead," 121.

[51] Ibid.

[52] Elizabeth A. Myers, "Cyber as a 'Team Sport': Operationalizing a Whole-of-Government Approach to Cyberspace Operations" (master's thesis, Joint Forces Staff College), http://www.dtic.mil/dtic/tr/fulltext/u2/a545638.pdf.

argues that if in the future when offensive cyber action is required, the single agency model could evolve into having offensive capabilities.[53]

Placing DHS in charge is an attractive solution, since DHS is already set up to coordinate with other government agencies and private industries for cybersecurity.[54] In 2013, Secretary of Homeland Security Janet Napolitano told Congress that a "cyber 9/11" is imminent and recommended that they pass legislation to govern cybersecurity.[55]

Senator Tom Coburn feels that DHS's plan to protect critical infrastructure from cyber-attacks is too vague. Supporting this is a federal report published in January 2015 that says DHS cybersecurity is "unlikely to protect us."[56] Both the Senator's thoughts and the federal report point out problems but do not offer any solutions or ways to improve the situation. The Government Accountability Office conducted research and found that DHS does not have any metrics for measuring if their cybersecurity programs and initiatives are effective.[57] The recommendation is to establish those metrics, conduct a review of their cybersecurity following the metrics and make changes as necessary.[58] Matthew H. Fleming and Eric Goldstein analyzed the authorities and efforts of DHS for securing cyberspace. They identified that the authorities granted to DHS currently are not enough to fulfill their mission for cybersecurity.[59] According to DHS, "cybersecurity is a

---

53 Joeli R. Field, "Cybersecurity: Division of Responsibility in the U.S. Government," National Security Cyberspace Institute, September 18, 2010, http://www.nsci-va.org/CyberReferenceLib/2010-09-18-Cybersecurity-Division%20of%20Responsibility%20in%20the%20US%20Government-Joeli%20Field.pdf.

54 Ibid., 120.

55 "Preventing 9/11 in the Cyber World," *Information Management* 47, no. 3 (2013): 18, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1430501590?accountid=12702.

56 Violet Blue, "New Report: DHS is a Mess of Cybersecurity Incompetence," *ZDnet*, January 14, 2015, http://www.zdnet.com/article/new-report-the-dhs-is-a-mess-of-cybersecurity-incompetence/.

57 Gregory C. Wilshusen, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework* (GAO-16-152) (Washington, DC: U.S. Government Accountability Office, 2015), 2, http://www.gao.gov/assets/680/674300.pdf.

58 Ibid.

59 Matthew H. Fleming, Eric Goldstein and Robert Tuohy, "An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States," Homeland Security Studies and Analysis Institute, May 24, 2011, http://www.homelandsecurity.org/docs/reports/MHF-and-EG-Analysis-of-authorities-supporting-efforts-of-DHS-to-secure-cyberspace-2011.pdf.

shared responsibility," with each person, business, and agency sharing a part of it.[60] The Department of Energy agrees with DHS's statement that cybersecurity is important at every level and believes that every individual Internet user should have a basic understanding of cyber threats as well as the importance of avoiding them.[61]

The Cyber Security Industry Alliance argues that there needs to be a position within DHS that has the sole role of being a liaison between the government and private industry.[62] Currently the assistant secretary for infrastructure protection handles this and that person is spread too thin with their responsibilities to handle this role.[63] Once a liaison position is established they should coordinate between the government and private industry to share more information and establish plans for cyber disruptions.[64]

The Sony Pictures Entertainment cyber-attack, which will be examined in Chapter IV, was a major event where another government attacked a private U.S. company. During its investigation the FBI linked the attackers to North Korea.[65] Sony decided to cancel the release of the movie *The Interview*, due to the threats from the hackers. Once North Korea was identified President Obama said that Sony should not have pulled the movie saying, "We cannot have a society in which some dictator someplace can start imposing censorship here in the United States."[66] According to President Obama the main goal of the attack was for North Korea to impose restrictions on our freedom of

---

[60] Cybersecurity: A Shared Responsibility, U.S. Department of Homeland Security, October 2013, https://www.dhs.gov/blog/2013/10/18/cybersecurity-shared-responsibility.

[61] Cybersecurity Is Every Citizen's Responsibility, U.S. Department of Energy, October 2013, http://energy.gov/articles/cybersecurity-every-citizens-responsibility.

[62] Larry Greenemeier, "Federal Role in Ensuring Cybersecurity Isn't Clear," *Information Week* no. 1023, January 24, 2005, 41, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/229160173?accountid=12702.

[63] Ibid.

[64] "Cyber-Security Group Pushes 12-Point Plan on White House, *TechWeb*, December 8, 2004, 1, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/201528422?accountid=12702.

[65] Kristina Daugirdas and Julian Davis Mortenson, "United States Responds to Alleged North Korean Cyber Attack on Sony Pictures Entertainment," *The American Journal of International Law* 109, no. 2 (2015): 420, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1717302701?accountid=12702.

[66] Ibid.

speech.[67] As a result, Sony did release the movie on its original release date. Seth Rogen, the lead actor in the movie, posted on Twitter, "The people have spoken! Freedom has prevailed! Sony didn't give up! The Interview will be shown at theatres willing to play is on Xmas day!"[68]

A few members of Congress publicly called the cyber-attack an act of war and cyberterrorism, but the White House refrained from using these terms.[69] According to Matt Bogaard, from Bogaard Group Intl. a security consulting firm, the main issue with cybersecurity is the "people part" but the Sony cyber-attack is pointing out to everyone just how important cybersecurity is.[70] There is a group of people, primarily hackers themselves, who feel that North Korea might not be responsible. The main evidence leading back to North Korea was Internet Protocol addresses, and according to this group of people, those are easy to fake.[71]

Secretary of Homeland Security, Jeh Johnson, hopes that other U.S. companies will see the Sony cyber-attack as a "wake-up call to strengthen their cybersecurity protections."[72] He says that every company should see look at their cybersecurity and ensure that the best practices are being followed.[73] Secretary Johnson goes on to offer help from DHS and other federal agencies for increasing their company's cybersecurity.[74] Going along with this DHS Deputy Under Secretary for Cybersecurity

---

[67] Erik Gruenwedel, "FBI Doubles Down on North Korean Ties to Sony Cyber Attack," *Home Media Magazine* 37, no. 1 (2015): 19, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1647424635?accountid=12702.

[68] Andrew Soergel, "Sony Says It's Not Curtains for 'The Interview' After All," U.S. News, December 24, 2014, http://www.usnews.com/news/newsgram/articles/2014/12/24/seth-rogens-and-james-francos-the-interview-back-on-says-sony.

[69] Daugirdas, "United States Responds," 421.

[70] Ted Johnson, "Hack Aftermath," *Variety* 327, no. 11 (2015): 44, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1675636219?accountid=12702.

[71] "Is Kim Jong Un Innocent?; Cyber-Security," *The Economist* 414, no. 8919 (2015): 22, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1641939004?accountid=12702.

[72] Susan Crabtree, "DHS' Johnson: Sony Hack a Wake-up Call for Business," *Washington Examiner*, December 19, 2014, http://www.washingtonexaminer.com/dhs-johnson-sony-hack-a-wake-up-call-for-business/article/2557657.

[73] Ibid.

[74] Ibid.

and Communications Phyllis Schneck feels that every cyber-attack should be seen as a wake-up call.[75]

Despite the considerable amount of literature that exists examining cyber threats, there is little discussion about the specific "lanes in the road" for DHS and other agencies in regards to cybersecurity. This thesis examines those lanes in the road, and how the assignment of responsibilities (or lack of assignment) affects national cybersecurity.

D. EXPLANATIONS AND HYPOTHESES

With the growing importance of cybersecurity, the government is working on getting ahead and staying ahead of the evolving cyber threats. This thesis evaluates two different hypotheses. First, with the "lanes in the road" not clearly defined for cybersecurity, it is hypothesized there are unneeded overlaps in resources and gaps in responsibilities. These overlaps can cause confusion leading to expanding existing gaps in responsibilities or creating new gaps. The second hypothesis is that in order to reduce this confusion, the lead agency for maintaining national cybersecurity should be DHS, and the lead agency for investigating cyber-attacks should be FBI. This would mean that DHS would be responsible for securing government networks, making standard cybersecurity requirements for public and private networks, and actively perusing collaboration across all public and private networks for increased resilience and support. The FBI would be responsible for investigating and determining the who, what, where, when, why, and how after and during a cyber-attack.

E. RESEARCH DESIGN

This thesis has four main objectives: (1) apply a policy and legislative analysis to examine the evolution of cybersecurity policies, in order to determine the current cybersecurity role for DHS; (2) provide an overview of the evolution and current cybersecurity missions for the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Department of Defense (DOD), and the Director of National Intelligence

[75] Christopher J. Castelli, "DHS Official Downplays Potential for Sony Hacking to Spur Cybersecurity Changes," *Inside Cybersecurity*, December 16, 2014, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1636659052?accountid=12702.

(DNI); (3) analyze the Sony Pictures Entertainment cyber-attack; and (4) determine the gaps in the current DHS cybersecurity role and identify ways to mitigate the weaknesses.

The first objective is met by critically analyzing the policies from the White House and DHS along with laws from Congress. The analysis works chronologically from the past to present, and provides historical background and justification. Once the evolution of cybersecurity for DHS has been established the current mission is evaluated for requirements and how DHS fulfills those requirements.

The second objective is met by providing background information for each entity from when they were established to their current cybersecurity mission. This is accomplished by evaluating the directives and laws that apply to each entity.

The third objective is met by analyzing the Sony cyber-attack, looking at before it occurred, the lead up, followed by the actual attack, and finishing with the aftermath including the investigation. The investigation is evaluated to determine if it was successful and if so why, and to determine any shortcomings after the attack.

The fourth objective looks at those gaps determined in the previous three objectives highlighting them and establishes recommendations to either close the gap completely or mitigate the issue to narrow the gap.

F. CHAPTER OVERVIEW

Chapter II analyzes the evolution of cybersecurity within the United States government, primarily focusing on DHS's portion of cybersecurity once it is established in 2001. The next section examines the current cybersecurity mission for DHS and specifically for the Secret Service under DHS.

Chapter III provides a description of the other three national agencies that also have a cybersecurity mission. An overview of the evolution and current mission is provided for the FBI, NSA/DOD, and DNI.

Chapter IV discusses the Sony Pictures Entertainment cyber-attack conducted in November 2014. The timeframe leading up to the attack, the actual attack, and the

aftermath are discussed. The response and investigation is analyzed to determine that it was both successful and a failure.

Chapter V provides a conclusion, policy recommendations, and identifies future research that is needed to properly identify the “lanes in the road” for cybersecurity.

II. DHS CYBERSECURITY EVOLUTION AND CURRENT MISSION

Chapter II provides an overview of the evolution of cybersecurity policy in the United States, specifically for DHS. DHS's current cybersecurity mission is to ensure a secure computer system for the government, and to promote coordination between public and private entities, and this chapter will consider how well that mission has been accomplished. Additionally, the U.S. Secret Service's mission evolution and current mission is examined.

A. EVOLUTION OF CYBERSECURITY POLICIES

Cybersecurity policies have been expanding and shifting for over two decades. The first governmental policy was seen in January 1988, with the "Computer Security Act of 1987" that established government-wide computer security a national priority. The act also provided a means to establish minimal security practices for computers.[76] The next major step forward for cybersecurity was in July 1990, when the "National Security Directive (NSD) 42: National Policy for the Security of National Security Telecommunications and Information System" was published. NSD-42 established the National Security Telecommunications and Information Systems Security Committee, now the Committee on National Security Systems (CNSS). CNSS falls under the President's Critical Infrastructure Protection Board, and Provides advice and guidance for the President, executive department, and other government agencies for system security.[77]

In May 1998, the next relevant cybersecurity directive was established, the "Presidential Decision Directive/NSC-63 (PDD/NSC-63): Critical Infrastructure Protection." PDD/NSC-63 sets the national goal to protect the country's critical infrastructure from both physical attacks and cyber-attacks by 2003. The goal was to

[76] Computer Security Act of 1987, Pub. L. No. 100-235 (1988).

[77] White House, *National Policy for the Security of National Security Telecommunications and Information System*, National Security Directive 42, Washington, DC, 1990, http://fas.org/irp/offdocs/nsd/nsd42.pdf.

prevent attacks, but if an attack was successful then the disturbance to the infrastructures services must be "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[78] The devastating terrorist attacks on September 11, 2001, caused widespread support for reform to prevent terrorism. Eleven days after the attacks on September 22, 2001, the Office of Homeland Security was created in the White House. The purpose of the office was to oversee and coordinate "a comprehensive national strategy to safeguard the country against terrorism and respond to any future attacks."[79]

Another response to the 9/11 attacks was Congress passing Public Law 107–56 in October 2001, titled "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001."[80] This was better known as the Patriot Act. This increased the authority and capacity of a variety of agencies in order to more efficiently counter terrorism. It also expanded the authority and capabilities of those agencies involved in cybersecurity.

In November 2002, after the Office of Homeland Security had operated as part of the White House for just over a year, the "Homeland Security Act of 2002" was passed. The Homeland Security Act formally made the Department of Homeland Security (DHS) a stand-alone, cabinet-level department. The DHS officially opened its doors on March 1, 2003.[81]

In February 2003, "Executive Order (E.O.) 13286: Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security" was signed. E.O. 13286 designated the Secretary of Homeland Security as the Executive Agent of the National Communication System Committee of Principals. This placed the Secretary in charge of those who owned or

---

78 White House, *Critical Infrastructure Protection*, Presidential Decision Directive/NSC-63, Washington, DC, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

79 Creation of the Department of Homeland Security, U.S. Department of Homeland Security, modified October 2014, http://www.dhs.gov/creation-department-homeland-security.

80 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001).

81 Creation of the Department of Homeland Security, U.S. Department of Homeland Security.

leased telecommunication assets that are part of the National Communication System or has importance to national security.[82] This was the start of DHS taking a major role in cybersecurity.

Later that same year in December 2003, "Homeland Security Presidential Directive (HSPD) No. 7: Critical Infrastructure Identification, Prioritization, and Protection," assigned the Secretary of Homeland Security the responsibility for critical infrastructure protection coordination and designated the DHS the lead agency for the information and telecommunications sectors.[83] This caused DHS, which had been established to safeguard the nation against terrorism, to see its role expanding to include almost anything related to national security, which includes cybersecurity. HSPD-7 also included that the privacy of American citizens will not be infringed while enhancing cybersecurity.

In January 2008, the "National Security Presidential Directive (NSPD) 54" and "Homeland Security Presidential Directive (HSPD) 23," both classified, were signed.[84] The Comprehensive National Cyber Security Initiative (CNCI) was launched, under the directions of NSPD-54 and HSPD-23.[85] CNCI lists three main goals. First, "establish a front line of defense" by increasing cybersecurity situational awareness across the entire nation.[86] Second, "defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities."[87] Third, "strengthen the future cybersecurity

82 Exec. Order No. 13286, http://fas.org/irp/offdocs/eo/eo-13286.htm.

83 White House, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive No. 7, Washing, DC, 2003, https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf.

84 Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative*, accessed 21 August 2015, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

85 Ibid.

86 Ibid.

87 Ibid.

environment" by advertising and supporting cyber education.[88] CNCI also defined DHS as the head liaison between the government and the private sector for cybersecurity.[89]

In October 2011, the President signed "E.O. 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." This called for two simultaneous goals, to responsibly share and safeguard classified information while protecting privacy and civil liberties. This E.O. applies to those agencies that either utilize classified information or own a classified network.[90] "E.O. 13618: Assignment of National Security and Emergency Preparedness Communications Functions," was signed in July 2012. E.O. 13618 addressed the government's requirement to be able to communicate during a national security crisis or emergency situation. The National Communications System is dissolved and DHS is required to establish a program office to assist in assigning specific responsibilities to federal government entities for communications functions.[91]

In February 2013, "Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience" was signed. The purpose of PPD-21 is to advance the "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[92] The national systems for "prevention, protection, mitigation, response, and recovery" must all be continually updated.[93] PPD-21 assigns responsibility at the federal, state, local, tribal, territorial, and public and private owners for critical infrastructure security and resilience.[94] Securing critical infrastructure includes both the physical and cyber aspects of security. The Secretary of Homeland Security is required to

88 Executive Office, *CNCI*.

89 Ibid.

90 Exec. Order No. 13587, https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.

91 Exec. Order No. 13618, https://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-.

92 The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21, Washington, DC, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

93 Ibid.

94 Ibid.

"provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure."[95] In order to carry out these requirements, additional roles and responsibilities are added under the Secretary of Homeland Security. To protect critical infrastructure DHS must analyze capabilities, and challenges to be able to identify potential vulnerable points that could be exploited by our adversaries.[96]

PPD-21 identifies eight specific things that DHS must do in order to ensure the protection of critical infrastructure. First, it must prioritize the current threats, both physical and cyber, and coordinate with other federal and private entities to mitigate those threats. Second, DHS must maintain situational awareness centers for potential threats to critical infrastructure.[97] Third, the information gained through the situational awareness centers and other intelligence must be shared with the appropriate federal or private entity to strengthen their resilience. Fourth, DHS must identify and assess vulnerabilities then coordinate with government and private agencies to mitigate them.[98] Fifth, DHS must act as the central coordinating effort for the federal government's response to cyber or physical attacks. Sixth, DHS must support the Attorney General to investigate and prosecute any threats or attacks.[99] Seventh, DHS must coordinate with the federal and private agencies that own or operate critical infrastructures in order to map and analyze all aspects of the infrastructure. Eighth, DHS is to submit a report annually on the status of critical infrastructure.[100] In addition to these requirements, PPD-21 also expands the research and development (R&D) requirements, and a plan will be released every four years to direct the R&D initiatives.[101] This directive, which supersedes HSPD-7, ensures that DHS is the central entity for critical infrastructure protection and the main focal point for private industry to work with.

---

95 White House, PPD-21.

96 Ibid.

97 Ibid.

98 Ibid.

99 Ibid.

100 Ibid.

101 Ibid.

"E.O. 13636: Improving Critical Infrastructure Cybersecurity" was signed in February 2013. E.O. 13636 addresses cybersecurity in four main ways. First, it expands a DHS program focused on sharing techniques and information that is important to critical infrastructure among government agencies and the private sector.[102] Second, a method was established for determining which infrastructures counted as critical, to determine which ones needed increased protection.[103] Third, the "National Institute of Standards and Technology" was required to establish a list of effective cybersecurity techniques for critical infrastructure protection.[104] Fourth, the agencies that had regulation authority were required to evaluate the level of current requirements and their ability to address risks.[105]

In February 2015, "E.O. 13691: Encouraging Private-Sector Cybersecurity Collaboration" was signed. The goal is to establish new "information sharing and analysis organizations to serve as focal points for cybersecurity information sharing as collaboration within the private sector and between the private sector and government."[106] Part of the new collaboration between the private sector and government is DHS was granted the power to share classified intelligence with the private sector for advancing cybersecurity efforts.[107] Later in February 2015, a Presidential Memorandum was signed titled "Establishment of the Cyber Threat Intelligence Integration Center (CTIIC)." CTIIC connects the dots at the national level for foreign cyber threats, and provides that intelligence to the appropriate agencies.[108] They also provide threat analysis briefs to policymakers.[109] This is critical to cybersecurity in that it can provide a heads up

---

[102] Exec. Order No. 13636, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[103] Ibid.

[104] Ibid.

[105] Ibid.

[106] Exec. Order No. 13691, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[107] Exec. Order No. 13691.

[108] White House, *Establishment of the Cyber Threat Intelligence Integration Center*, Presidential Memorandum, Washington, DC, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

[109] Ibid.

to a cyber-attack allowing a response that can prevent an attack from being successful instead of responding after an attack has happened.

B. CURRENT DHS CYBERSECURITY MISSION

DHS is the lead agency for national cybersecurity concerns, and has divided its cybersecurity efforts between two offices: the Cyber Security Division (CSD) and the Office of Cybersecurity and Communications (CS&C). These two offices work towards different objectives but both are furthering the national cybersecurity interests, through strengthening the coordination between private and public cybersecurity and expanding the education level in regards to cybersecurity and cyber threats.

CSD was formed in 2011, under the Homeland Security Advanced Research Projects Agency. CSD's mission is to:

> Contribute to enhancing the security and resilience of the nation's critical information infrastructure and the Internet by: developing and delivering new technologies, tools and techniques to enable DHS and the U.S. to defend, mitigate and secure current and future systems, networks and infrastructure against cyber-attacks; conduct and support technology transition, and lead and coordinate research and development (R&D) among the R&D community which includes department customers, government agencies, the private sector and international partners.[110]

CSD furthers these three mission areas by coordination and cooperation with other agencies at the federal, state, municipal levels, private sector companies, and the research community.[111] This allows them to gather the advancements of the cybersecurity initiatives and be able to share that information across the board, to further not only the U.S. government's cybersecurity but also effect change in the private sector for increasing cybersecurity for U.S. interests.

CS&C was created in 2006, by Congress under the Assistant Secretary for Cybersecurity and Communications. CS&C is "responsible for enhancing the security,

---

[110] Cyber Security Division, U.S. Department of Homeland Security, modified August 2015, http://www.dhs.gov/science-and-technology/cyber-security-division.

[111] Ibid.

resilience, and reliability of the Nation's cyber and communications infrastructure."[112] The goal is to prevent or at least minimize the disruption to critical information infrastructure. CS&C is not only looking at protecting the federal domain but also the private sector. Their mission is carried out through five divisions: The Office of Emergency Communications (OEC), The National Cybersecurity and Communications Integration Center (NCCIC), Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR), Federal Network Resilience (FNR), and Network Security Deployment.

OEC supports and promotes the communications used by the government and first responders during emergency situations. They provide "training, coordination, tools, and guidance to help its federal, state, local, tribal, territorial and industry partners develop their emergency communications capabilities."[113] NCCIC is a "24x7 cyber situational awareness, incident response, and management center."[114] They share information to the public and private sectors to establish a greater understanding of cybersecurity vulnerabilities, actions, and responses.[115]

SECIR is the focus for engagement and coordination of national cybersecurity initiatives for both the government and the private sector. They are designed to streamline the coordination with external partners, while simultaneously gathering expertise on cybersecurity.[116] FNR is focused on risk management for cybersecurity. They develop innovative approaches to drive change by developing metrics that have a measurable impact.[117] Network Security Deployment was established to be the cybersecurity

---

[112] Office of Cybersecurity and Communications, U.S. Department of Homeland Security, modified July 2015, http://www.dhs.gov/office-cybersecurity-and-communications.

[113] Office of Emergency Communications, U.S. Department of Homeland Security, modified September 23, 2015, http://www.dhs.gov/office-emergency-communications.

[114] About the National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security, modified September 22, 2015, http://www.dhs.gov/national-cybersecurity-communications-integration-center.

[115] Ibid.

[116] Stakeholder Engagement and Cyber Infrastructure Resilience, U.S. Department of Homeland Security, modified September 23, 2015, http://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience.

[117] Federal Network Resilience, U.S. Department of Homeland Security, modified September 22, 2015, http://www.dhs.gov/federal-network-resilience.

engineering and acquisition center of excellence. They operate the National Cybersecurity Protection System, which "provides intrusion detection, advanced analytics, information sharing, and intrusion prevention capabilities that combat and mitigate cyber threats to the Federal Executive Branch information and networks."[118]

The divisions of CS&C all fill a different part of the cybersecurity mission and provide a more focused look at their piece. The breakdown of responsibility within DHS is established in order to provide the best structure for furthering the national cybersecurity interests. The link between the government and the private sector is seen in almost every aspect of cybersecurity.

C. U.S. SECRET SERVICE CYBER MISSION

There are other agencies under DHS that contribute to national cybersecurity, such as U.S. Immigrations and Customs Enforcement, and the United States Secret Service (USSS). This thesis will only evaluate the Secret Services cyber mission, due to their mission focusing on cyber investigation. Additionally, they have a direct link to the Sony Pictures Entertainment cyber-attack that is discussed in Chapter IV.

In 1865, the Department of the Treasury formed the Secret Service Division (SSD) to battle counterfeiting currency.[119] In 1894, President Grover Cleveland requested that SSD provide him part-time protection.[120] SSD continued to provide part-time protection until President McKinley was assassinated in 1901. After that Congress asked SSD to protect the president. It was not until 1906 that Congress funded the protection of the president.[121]

---

[118] Network Security Deployment, U.S. Department of Homeland Security, modified September 22, 2015, http://www.dhs.gov/network-security-deployment.

[119] USSS History, U.S. Secret Service, accessed April 15, 2016, http://www.secretservice.gov/about/history/events/.

[120] Shawn Reese, *The U.S. Secret Service: History and Missions* (CRS Report No. RL34603) (Washington, DC: Congressional Research Service, 2014), 7.

[121] Ibid.

In 1943, the SSD was renamed the United States Secret Service.[122] In 1986, Congress passed the "Computer Fraud and Abuse Act of 1986" that authorized the Secret Service jurisdiction alongside the FBI for investigating identity theft along with fraud and related activity committed against protected computers.[123] Investigation jurisdiction being jointly provided to the Secret Service and the FBI allows them to investigate any intrusion on a protected computer. The cybersecurity law explains a protected computer system as "protects federal computers, bank computers and computers connected to the Internet."[124]

In 1995, the Secret Service established their first Electronic Crimes Task Force (ECTF) in New York. The purpose of the ECTF was "prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures."[125] In 2001, the Patriot Act required the USSS to expand the ECTF.[126] There are now thirty-one different locations for the ECTF. The ECTF's role has expanded as well; it now provides support and resources to investigations that meet certain criteria. Those criteria are "significant economic or community impact; participation of organized criminal groups involving multiple districts or transnational organizations; or use of schemes involving new technology."[127] The ECTF was expanded for the purpose of "preventing, detecting, and investigating various forms of electronic crimes."[128] The expansion of the ECTF made the Secret Service the primary agency for

---

[122] Records of the U.S. Secret Service [USSS]: Record Group 87, 1863–1988, National Archives and Records Administration, accessed April 15, 2016, http://www.archives.gov/research/guide-fed-records/groups/087.html#87.1.

[123] U.S. Department of Justice, *Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section Criminal Division* (Washington, DC: OLE, 2015) http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[124] Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (CRS Report No. R42659) (Washington, DC: Congressional Research Service, 2010), 2.

[125] U.S. Secret Service Electronic Crimes Task Forces, U.S. Department of Homeland Security, accessed April 15, 2016, https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf.

[126] *USA PATRIOT Act,* Pub. L. No. 107-56, 115 Stat. 272 (2001).

[127] Electronic Crimes Task Forces, U.S. Department of Homeland Security.

[128] *USA PATRIOT Act,* Pub. L. No. 107-56, 115 Stat. 272 (2001).

investigating cyber-attacks. In 2002, the USSS was moved from the Department of the Treasury to the new DHS. Under Subtitle C of the Homeland Security Act of 2002, the functions, personnel, assets, and obligations of the USSS were to remain the same and that the USSS would continue to be a distinct entity.[129]

The USSS has shown itself to be a leader in cybersecurity and has a vested interest in protecting the countries critical infrastructure, financial infrastructure, and government cyberspace. In order to accomplish this, the USSS has adopted a six pronged approach:

- Providing advanced computer forensics and network intrusion investigation training to enhance the skills of special agents through the Electronic Crimes Special Agent Program (ECSAP)
- Establishing a Computer Emergency Response Team in coordination with Carnegie Mellon University
- Maximizing partnerships with international law enforcement counterparts through overseas field offices and by forward deploying ECSAP agents to international working groups
- Providing training, examination services and research into cutting edge processes to extract potential evidence from mobile devices to include cellular phones, skimming devices and GPS units
- Providing computer-based training to state and local law enforcement partners to enhance their investigative skills at the National Computer Forensics Institute
- Collaborating through an established network of 46 Financial Crimes Task Forces and 39 Electronic Crimes Task Forces[130]

This chapter covered the evolution of cybersecurity policy changes in the United States. DHS was specifically identified for their role in national cybersecurity. DHS works to ensure network security across the entire nation, from protecting government computers to helping the private sector protect itself. USSS, as a part of DHS, has a major role to play in cybersecurity, and is currently the lead agency for investigating cyber-attacks.

---

[129] Homeland Security Act of 2002, Pub. L. No. 107-296 (2002).

[130] The Investigative Mission: Cyber Operations, U.S. Secret Service, accessed April 15, 2016, http://www.secretservice.gov/investigation/.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FBI, NSA/DOD, DNI CYBERSECURITY OVERVIEW

Chapter II provided an overview of the evolution of cybersecurity policy in the United States, looking specifically at DHS. DHS's current cybersecurity mission was identified and discussed. DHS works to ensure a secure computer network for the government, and promotes coordination between public and private entities. The evolution of USSS's cybersecurity mission and its current mission within DHS was identified.

Chapter III describes the evolution and current cybersecurity missions for the FBI, NSA/DOD, and DNI. These three agencies were chosen for study due to their national level cybersecurity missions, and the fact that they have broad cybersecurity missions comparable to DHS. Analyzing these entities will provide a more rounded analysis of DHS's cybersecurity mission, by understanding how other national level agencies developed their cybersecurity mission and how they each interact with the whole.

A. FEDERAL BUREAU OF INVESTIGATION

In 1905, Charles Bonaparte was appointed the Attorney General by President Theodore Roosevelt.[131] The Department of Justice (DOJ) frequently utilized USSS agents to conduct investigations. This frustrated Bonaparte because Secret Service investigations were expensive, and its agents would report to the Chief of the Secret Service instead of to him.[132] On May 27, 1908, Congress passed a law forbidding the DOJ from utilizing USSS agents for investigations.[133] Later that same year Bonaparte established a small group of special agents. The group had no name, but would eventually grow to become the FBI.[134] On July 26, 1908, the special agents were ordered to report to Chief Examiner Stanley W. Finch, and just under a year later on March 16, 1909,

[131] A Brief History of the FBI, Federal Bureau of Investigation, accessed May 13, 2016, https://www.fbi.gov/about-us/history/brief-history.

[132] Ibid.

[133] Ibid.

[134] Ibid.

Attorney General George Wickersham named the group of special agents the Bureau of Investigation.[135]

The FBI has authority under the "Computer Fraud and Abuse Act of 1986," to investigate crimes committed against federally protected computers.[136] Protected computers are those used by the government or financial institutions and those computers that could affect the economy.[137] In 2002, the FBI created the Cyber Division to "combat cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, and cybercrime by applying the highest level of technical capability and investigative expertise."[138] The FBI initiated a cyber-specific agent training program in order to ensure it was prepared to operate in cyberspace.[139]

In January 2008, the "Comprehensive National Cyber Security Initiative" (CNCI) was launched. The CNCI supports mandates issued in the "National Security Presidential Directive 54" and "Homeland Security Presidential Directive 23," both which are classified. To increase the government's cybersecurity operations, CNCI required an investment increase for cybersecurity monitoring, training, and information-sharing for the government and the private sector. As part of the CNCI the FBI established the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF is the nation's central hub for the coordination of cyber investigations.[140] The NCIJTF expands coordination between the Intelligence Community and federal law enforcement against

- Cyber terrorists exploiting vulnerabilities in critical infrastructure control systems;
- Nation-state theft of intellectual property and trade secrets;

---

135 Brief History of the FBI, FBI.

136 U.S. Department of Justice, *Prosecuting Computer Crimes*, 158.

137 Ibid.

138 Ten Years After: The FBI Since 9/11-Cyber, Federal Bureau of Investigation, accessed May 13, 2016, https://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber.

139 Ibid.

140 Cyber Task Forces, Federal Bureau of Investigation, accessed May 13, 2016, https://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1.

- Financially-motivated criminals stealing money or identities or committing cyber extortion;
- Hacktivists illegally targeting businesses and government services;
- Insiders conducting theft and sabotage.[141]

The FBI has also established Cyber Task Forces (CTF) that focus on cybersecurity threats, in all 56 of its field offices.[142] The CTF coordinates at the local and national level to try to de-conflict any issues. The mission of each CTF is:

> In support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each CTF synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions.[143]

The FBI is also expanding its cyber capabilities in three other ways. The first is the National Cyber-Forensics & Training Alliance (NCFTA). NCFTA was established in 1997, and enables "law enforcement, private industry, and academia to build and share resources, strategic information, threat intelligence to identify, stop emerging cyber threats and mitigate existing ones."[144] iGuardian is the second method the FBI is utilizing to increase cybersecurity. iGuardian is "a secure information portal allowing industry-based, individual partners to report cyber intrusion incidents in real time."[145] The third method is InfraGard. InfraGard is a partnership with the FBI and the private sector, that encompasses businesses, academia, law enforcement agencies, and other entities working together to prevent attacks against the United States.[146]

---

[141] Cyber Task Forces, FBI.

[142] Ibid.

[143] Ibid.

[144] National Cyber-Forensics & Training Alliance, Federal Bureau of Investigation, accessed May 13, 2016, https://www.fbi.gov/about-us/investigate/cyber/national-cyber-forensics-training-alliance.

[145] iGuardian: The FBI's Industry-Focused Cyber Intrusion Reporting Platform, Federal Bureau of Investigation, accessed May 13, 2016, https://www.fbi.gov/stats-services/iguardian.

[146] InfraGard: Partnership for Protection, InfraGard, accessed May 13, 2016, https://www.infragard.org/.

B. NATIONAL SECURITY AGENCY AND DEPARTMENT OF DEFENSE

The National Security Agency (NSA) and the Department of Defense (DOD) both play an integral part to U.S. cybersecurity. In past conflicts, our nation's adversaries were able to be defined by national boundaries.[147] Today, cyberspace has abolished those boundaries, with the entire world operating and relying on the same interconnected networks, and the NSA and DOD are critical to protecting those networks.[148]

1. National Security Agency

On December 29, 1952, the "National Security Council Intelligence Directive (NSCID) No. 9: Communications Intelligence (COMINT)" was signed by President Truman.[149] NSCID-9 established the NSA under the authority of the Secretary of Defense (SECDEF).[150] NSCID-9 also defines NSA's mission as, "provide an effective, unified organization and control of the communications intelligence activities of the United Stated conducted against foreign governments, and to provide for integrated operational policies and procedures pertaining thereto."[151] The next major change to NSA's mission was in December 1971, SECDEF Laird published "DOD Directive S-5100.20," to define the "authorities, functions, and responsibilities of the NSA."[152] DOD Directive S-5100.20 broadened NSA's COMINT mission. NSA's mission was expanded to include all Signals Intelligence (SIGINT). SIGINT was defined as to include COMINT, Electronic Intelligence (ELINT), and Telemetry Intelligence (TELINT).[153] This expanding of NSA's responsibilities now made them in charge of intelligence collection for all electronic methods.

---

147 Cyber, National Security Agency, modified May 3, 2016, https://www.nsa.gov/what-we-do/cyber/.

148 Ibid.

149 White House, *Communications Intelligence*, National Security Council Intelligence Directive No. 9, Washington, DC, 1952.

150 Ibid., 5.

151 Ibid.

152 U.S. Department of Defense, *Department of Defense Directive S-5100.20* (Washington, DC: Secretary of Defense, December 23, 1971).

153 Ibid.

NSA's mission can be broken down into two areas: SIGINT, and Information Assurance.[154] SIGINT is comprised of collecting, processing, and disseminating intelligence from foreign entities.[155] SIGINT for NSA includes collecting information from foreign communications, radars, and any other electronic system. The information collected is generally in foreign languages, technical documents, encoded, or otherwise safeguarded. Once NSA collects the information they need to translate it into usable intelligence. This needs to happen as close to real time as possible for NSA's customers to utilize the intelligence. NSA provides intelligence to the White House, executive branch agencies, DOD, and U.S. allies.[156] NSA's second mission is, preventing unauthorized access to the government's networks, which is Information Assurance. NSA protects national security information and systems from our advisories.[157] The main objective of the Information Assurance mission is preventing advisories from accessing, viewing, stealing, or changing any part of the information system.[158] NSA's specific cyber mission is to use both SIGINT and Information Assurance to identify, and prevent any cyber threat to the government networks.[159]

2. Department of Defense

In 1775, the American Revolution led to the creation of the Army, Navy, and Marine Corps. Fourteen years later in 1789 the War Department was established, with the Department of the Navy being created in 1798.[160] It was not until 1947, that the different services where united into the same department, called the National Military Establishment. Also in 1947, the War Department was renamed the Department of the Army, and the Department of the Air Force was established.[161] In 1949, the three service

---

[154] Frequently Asked Questions, National Security Agency, modified May 3, 2016, https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml.

[155] Ibid.

[156] Ibid.

[157] Ibid.

[158] Ibid.

[159] Cyber, National Security Agency.

[160] Ibid.

[161] Ibid.

secretaries lost their cabinet level status and the National Military Establishment was then renamed the Department of Defense.[162] The overarching mission for DOD is to "provide the military forces needed to deter war and to protect the security of our country."[163]

In June 2009, the SECDEF directed Commander U.S. Strategic Command to create the U.S. Cyber Command (USCYBERCOM), which became operational in October 2010. The mission for USCYBERCOM is:

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[164]

USCYBERCOM is a subordinate of U.S. Strategic Command as a sub-unified combatant command.[165] It is comprised of five service elements; the Army, Navy, Marine Corps, and Air Force; each have their own cyber command that is a subordinate of USCYBERCOM.[166] The Coast Guard also has a cyber command that is a subordinate of DHS but works directly with USCYBERCOM.[167] USCYBERCOM has also established Cyber Mission Force (CMF) in order to fulfil the three missions and five goals outlined in the DOD Cyber Strategy.[168] Admiral Michael Rogers, Commander USCYBERCOM, says that the formation of CMFs is designed to turn "strategy and plans into operational outcomes."[169] Approximately half of the desired CMF teams have been established with the goal being 133 teams, and a total of 6,200 personnel.[170] The teams

---

[162] Cyber, NSA.

[163] Ibid.

[164] U.S. Cyber Command, U.S. Strategic Command, modified March 2015, https://www.stratcom.mil/factsheets/2/Cyber_Command/.

[165] Ibid.

[166] Ibid.

[167] Ibid.

[168] Ibid.

[169] Statement of Admiral Michael S. Rogers: Hearing before the Committee on Armed Services, Senate, (2015) (Statement of Admiral Michael S. Rogers, Commander U.S. Cyber Command), 6.

[170] Ibid., 7.

that have been established, are guarding networks, and have helped "Combatant Commanders deny freedom of maneuver to our adversaries in cyberspace."[171] The CMFs are being developed to carry out defensive and offensive cyberspace operations.[172]

In April 2015, the DOD Cyber Strategy was published, identifying three cybersecurity missions for DOD. First, "DOD must defend its own networks, systems, and information."[173] Second, "DOD must be prepared to defend the United States and its interests against cyber-attacks of significant consequence."[174] Third, "DOD must be able to provide integrated cyber capabilities to support military operations and contingency plans."[175] These three missions are followed up with five strategic goals in order to fulfil the missions. The five strategic goals are:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the DOD information network, secure DOD data, and mitigate risks to DOD missions;
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence;
4. Build and maintain viable cyber operations and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.[176]

In 2010, SECDEF, with the President's approval, made the Director of NSA the Commander USCYBERCOM in a dual-hatted role.[177] This means that the two agencies

---

[171] Statement of Admiral Michael S. Rogers, 7.

[172] "The Facts: Cyber Mission Force," U.S. Army Cyber Command, March 2, 2016, http://www.arcyber.army.mil/fact_sheets/ARCYBER%20fact%20sheet%20-%20Cyber%20Mission%20Force%20(2March2016).pdf.

[173] U.S. Department of Defense, *Department of Defense Cyber Strategy* (Washington, DC: Secretary of Defense, April 17, 2015).

[174] Ibid.

[175] Ibid.

[176] Ibid.

[177] Statement of Admiral Michael S. Rogers, 2.

will work together and coordinate their efforts for a greater outcome.[178] Even with the same leader the two entities have very different roles to play. NSA conducts SIGINT and Information Assurance while USCYBERCOM operates under U.S. Code Title 10 and Title 32.[179] USCYBERCOM is a consumer of the SIGINT and Information Assurance that NSA provides. The two missions from NSA are vital to the Network Warfare that USCYBERCOM trains for.[180] Both NSA and USCYBERCOM play important roles for national cybersecurity.

C. DIRECTOR OF NATIONAL INTELLIGENCE

The Director of National Intelligence (DNI) was created under the "Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004" that was signed on December 17, 2004.[181] On April 21, 2005, the first DNI, John D. Negroponte, was sworn in.[182] The main mission for the DNI is to integrate the Intelligence Community (IC).[183] The IC is comprised of 17 different independent agencies within the Executive Branch that collaborate together under the DNI to provide the intelligence necessary for operations.[184]

In February 2013, "PPD-21: Critical Infrastructure Security and Resilience" was signed. PPD-21 directed the IC, under the direction of the DNI, to provide intelligence pertaining to threats against critical infrastructure, to the appropriate entities.[185] Additionally, PPD-21 authorized the DNI to oversee safeguarding of national security systems.[186]

---

[178] Statement of Admiral Michael S. Rogers, 2.

[179] FAQ, National Security Agency.

[180] Ibid.

[181] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 (2004).

[182] History, Office of the Director of National Intelligence, accessed May 13, 2016, https://www.dni.gov/index.php/about/history.

[183] Mission, Vision & Goals, Office of the Director of National Intelligence, accessed May 13, 2016, https://www.dni.gov/index.php/about/mission.

[184] Office of the Director of National Intelligence, Office of the Director of National Intelligence, accessed May 13, 2016, https://www.dni.gov/index.php.

[185] White House, Presidential Policy Directive 21.

[186] Ibid.

In February 2015, the President directed the DNI to create the Cyber Threat Intelligence Integration Center (CTIIC).[187] CTIIC connects the dots for national intelligence that deals with foreign cyber threats, and provides that to other departments and agencies along with policymakers.[188] CTIIC provides its intelligence primarily to NCCIC, NCIJTF, and USCYBERCOM to help them fulfil their missions.[189] CTIIC does not collect intelligence, or attempt to replicate other functions currently performed by other agencies.[190] Since they do not collect information the data flow is only in one direction; from CTIIC to other government agencies. There is no feedback loop established for CTIIC to determine if they are providing what the agencies need.

The FBI, NSA/DOD, DNI, along with DHS ensure that our country is safe from cyber threats and work to further the level of cybersecurity, cyber education, and coordination across public and private entities. This chapter discussed the evolving missions for the FBI, NSA/DOD, and DNI to enhance the cybersecurity for the nation. An understanding of the other national level cybersecurity entities is important to see what each provided and how that all fits together to fulfill the national cybersecurity objectives.

[187] White House, "Fact Sheet: Cyber Threat Intelligence Integration Center," Washington, DC, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

[188] Ibid.

[189] Ibid.

[190] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SONY PICTURES ENTERTAINMENT CYBER-ATTACK

Chapter III discussed the evolving mission and the current responsibilities for the FBI, NSA/DOD, and DNI cybersecurity. These entities plus DHS make up the national level cybersecurity effort. Chapter IV looks at the Sony Pictures Entertainment cyber-attack. The first section provides background information leading up to the attack, and the actual attack is discussed in the following section, along with the aftermath and subsequent investigation.

A. BEFORE THE CYBER-ATTACK

The Sony cyber-attack involved the movie *The Interview*. *The Interview* is a comedy, where two reporters (played by Seth Rogen and James Franco) are recruited by the CIA to kill the Democratic People's Republic of Korea's (North Korea) dictator Kim Jong-un. In the original script there was a fictional dictator instead of Kim but it was later changed before filming. North Korea was regarded as fair game in Hollywood, unlike China since China has a large film market.[191] In June 2014, the first trailer for the film was released. A couple days after the trailer release a North Korean government spokesman warned Sony that the release of *The Interview* would be seen as "the most blatant act of terrorism and war."[192] The spokesman then threatened a merciless counter-measure if the film was released. North Korea later filed official complaints with the White House and the United Nations.[193]

Sony was not prepared for the blowback they were to receive over *The Interview*. Doug Belgrad, a studio executive, told Sony's CEO Michael Lynton that he was "doing homework on whether there is any precedent on depicting and/or killing a living leader on film."[194] Lynton consulted with "extremely knowledgeable experts" and was given no

191 Peter Elkind, "Inside the Hack of the Century," *Fortune*, July 2015, 73, http://nics.syr.edu/wp-content/uploads/2016/04/Inside-the-Hack-of-the-Century.pdf.

192 Ibid., 74.

193 Ibid.

194 Ibid.

indication of a possible cyber-attack.[195] Bruce Bennett, an expert on North Korea for the Rand Corporation, reportedly did tell Lynton that a cyber-attack was possible, but that North Korea frequently makes empty threats, also advising him that there was probably nothing to fear.[196]

Although many people involved with the film felt it was simply empty threats, North Korea had already been linked to numerous previous cyber-attacks. The country is believed to have "several thousand army hackers."[197] Prior to the Sony cyber-attack the most notable cyber-attack linked to North Korea is the DarkSeoul attack against The Republic of Korea (South Korea). On April 20, 2013, a coordinated cyber-attack was conducted that had destructive effects.[198] The attack was disguised as the work of hacktivists but was determined to have been carried out by North Korea. The attack caused South Korea's main three television stations (KBS, MBC, YTN) to be taken off the air, and ATMs, Internet and mobile banking services of the three main banks (Jeju, Nonghyup, Shinhan) to be frozen.[199] Approximately 45,000 computers between the television stations and banks had their operating systems removed and their hard drives erased.[200] The investigation found that the main access point was a patch management software that was used. Once the attackers had access to the management software they could bypass the user level on the systems and operate at the administrator level.[201] The attackers used the updates from the management software to hide their malware. The attackers had access to the systems for over a month before the final attack. During that month the attacker gathered all the information available.[202] The outcome of the attack was over $700 million in damages and the potential for unknown damage with the

---

[195] Elkind, "Hack of the Century," 74.

[196] Ibid.

[197] Ibid., 75.

[198] David M. Martin, "Tracing the Lineage of DarkSeoul," SANS Institute: InfoSec Reading Room, November 20, 2015, 2, https://www.sans.org/reading-room/whitepapers/warfare/tracing-lineage-darkseoul-36787.

[199] Ibid., 2-3.

[200] Ibid., 3.

[201] Ibid., 4.

[202] Ibid.

information that was stolen.[203] The fact that this previous attack had been linked to North Korea could have led Sony executives to give the threats more credibility.

Actor Seth Rogen also received warnings about a possible cyber-attack. He sought out Rich Klein, whose consulting firm in Washington, D.C., advises Hollywood on geopolitical problems. Once Klein was able to read the script for *The Interview* he advised Rogen to expect blowback from North Korea "possibly in the form of an electronic assault."[204] Klein also felt that North Korea might conduct a cyber-attack against the studio to prevent the release of the film.[205] Both of these warnings were passed onto Sony executives, but Sony denies having any knowledge or receiving any information on an imminent attack.

B. THE CYBER-ATTACK

On Monday November 24, 2014, at seven in the morning Sony Entertainment Pictures was the victim of a massive cyber-attack. When employees signed into their computers gunshots rang out from the speakers, and a picture of a skeleton appeared over the top two executive's heads which were made to look like zombies. Figure 1 shows a screenshot of what the employees saw.

[203] Elkind, "Hack of the Century," 75.

[204] Ibid., 76.

[205] Ibid.

Figure 1. Screenshot from Sony After the Cyber-Attack.[206]

1. Cyber-attack Damage

The attackers were able to take out approximately half of Sony's global network. Everything was erased from 3,262 company computers, as well as 6,797 personal computers. Reportedly, 837 of Sony's 1,555 servers were erased. Instead of just deleting information off the devices, the attackers had the data overwritten seven different times to ensure that the data could not be recovered. Before the data was destroyed, it was copied by the attackers. The last thing the attackers did was delete the operating system off all devices affected.[207] Sony's technology was set back decades, forcing the company to use fax machines, the postal service, and pay its employees by check for over a week, until it

[206] Source: Peter Elkind, "Inside the Hack of the Century," *Fortune*, July 2015, 67.

[207] Elkind, "Hack of the Century," 66.

could recover from the attack. As a precaution Sony shut down most of their computer systems across the world.[208]

The data that was stolen was made public over the next three weeks, in nine different batches. The stolen data included unfinished movie scripts, email exchanges, salaries, and over 47,000 Social Security numbers. Additionally, five different films were released to piracy websites for free viewing. Four of those five films had not yet been released by Sony. The hackers took things further by making threats for a 9/11 style attack if *The Interview* was released.

2. Media Coverage

In the aftermath of the Sony cyber-attack the news media did exactly what it is trained to do during a crisis: it wrote and discussed it. The news covered everything from what was happening, to speculating about who did it. They also published some of the information that the hackers had stolen and then leaked online. There is no way of knowing if the leaked information would have gotten out to as large of an audience if the news had not covered it. Multiple different news agencies published the personal emails from Sony executives and lists of salaries, however drew the line at releasing medical records or Social Security numbers.

By the middle of December Sony felt they needed to talk to an attorney about the stolen information. David Boies was hired and he warned over 40 different media organizations to stop using the stolen information or "they would be held 'responsible for any damage or loss.'"[209] Boies argued that the documents were protected under a variety of U.S. and international laws since they were private, confidential, or trade secrets.[210]

Aaron Sorkin, a screenwriter for Sony, wrote an OP-ED for *The New York Times* that explains what the news media was doing during the aftermath of the Sony cyber-

[208] David Robb, "Sony Hack: A Timeline," *Deadline*, December 22, 2014, http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/.

[209] Ibid., 83.

[210] Ibid.

attack. He says that they are "giving material aid to criminals."[211] Sorkin feels that the American news outlets provided the hackers an outlet for the stolen information.[212] The hackers did not have to do any work to ensure it would be seen by the masses; all they had to do was put it online and the news outlets would publish it and talk about it. The first release of private information was not done by the hackers but by the American news outlets. Sorkin writes he understands that stolen information is routinely used and sometimes should be published, such as the Pentagon Papers.[213] There is nothing in the stolen Sony documents that even comes close to the level of public interest that the Pentagon Papers did. The co-editor in chief of the magazine *Variety*; decided to publish the leaked information because he felt it was newsworthy.[214] Sorkin continues to say that every news outlet that published the information is "morally treasonous and spectacularly dishonorable."[215] He finishes his argument by saying that, "as demented and criminal as it is, at least the hackers are doing it for a cause. The press is doing it for a nickel."[216]

The FBI and Sony were attempting to contain the information that was stolen, and the media was thwarting that effort at every turn. The FBI and Sony took different approaches in an attempt to contain the stolen information. The FBI focused on people once they have accessed the stolen information by visiting people who had been linked to downloading a number of stolen files.[217] Sony's tactic was more focused on preventing the information from being accessed in the first place. Sony identified the websites that contained the stolen files for download, and then flooded those sites with random other

---

[211] Aaron Sorkin, "The Sony Hack and the Yellow Press," *New York Times*, December 15, 2014, http://www.nytimes.com/2014/12/15/opinion/aaron-sorkin-journalists-shouldnt-help-the-sony-hackers.html?_r=1.

[212] Ibid.

[213] Sorkin

[214] Ibid.

[215] Ibid.

[216] Ibid.

[217] Kashmir Hill, "Beware: Downloading the Hacked Sony Pictures Docs Could Bring the Feds to Your Door," *Fusion*, December 11, 2014, http://fusion.net/story/32988/beware-downloading-the-hacked-sony-pictures-docs-could-bring-the-feds-to-your-door/.

files.[218] This was an attempt to hide the stolen files in thousands of other files, and slow the download speeds to deter people from accessing the information.

C. AFTER THE CYBER-ATTACK

Within a couple of hours after the attack the FBI was notified. A team from the FBI Los Angeles cyber-squad was sent to start an investigation. Sony also hired its own private forensic expert to investigate, Kevin Mandia.[219] Four days after the attack the first of the stolen data was leaked to online file-sharing websites. The data consisted of five Sony films; *Fury, Annie, Mr. Turner, Still Alice,* and *To Write Love On Her Arms*. Of these five films *Fury* was the only movie to have been released and was still in theatres.[220] On December 1, the salaries of the top 17 Sony executives were leaked.[221] Many mainstream news outlets published the list. Every few days after this a new batch of information was leaked including; personal information, performance evaluations, medical records, background checks, disciplinary letters, passport information, and more salaries.[222] Personal emails from Sony's studio chief Amy Pascal were released, which included nasty comments about celebrities, and even racist banter about President Obama, insinuating that he preferred movies about black people.[223] This led Pascal to issue a public apology and many personal apologies as well.

In a press release on December 19, 2014, the FBI stated, "As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions."[224] The Guardians of Peace identified

---

218 Rick McCormick, "Sony Attacks Torrents to Prevent Spread of Stolen Data," *The Verge*, December 11, 2014, http://www.theverge.com/2014/12/11/7375617/sony-attacks-torrents-to-prevent-spread-of-stolen-data.

219 Ibid., 83.

220 Robb, "A Timeline."

221 Ibid.

222 Elkind, "Hack of the Century," 83.

223 Ibid.

224 "National Press Releases: Update on Sony Investigation," Federal Bureau of Investigation, December 19, 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

themselves as the attacker. This group had never been heard of before or since this cyberattack. The FBI released three reasons as part of the justification for naming North Korea. First, the technical analysis of the data deletion malware used was linked to additional malware that North Korea is known to have developed and used. Second, the FBI linked several Internet protocol (IP) addresses associated with North Korea to those IP addresses used in the attack. Third, the tools used had a stark resemblance to the ones used during the DarkSeoul attack that North Korea conducted against South Korea.[225] Later that same day North Korea publicly "denied any involvement in the attack, but praised the hackers … as having done a righteous deed."[226]

The FBI said that the cyber-attack conducted by North Korea was "intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves."[227] In a statement released on December 19, Secretary of Homeland Security Jeh Johnson said that the attack was not only against Sony but also against our freedom and way of life.[228] On December 22, 2014, a spokesperson for the State Department said, "we are considering a range of options in response. We aren't going to discuss publicly operational details about the possible response options."[229] The next day North Korea had a ten-hour Internet outage.[230] The United States did not take responsibility for this, but an unnamed official was quoted saying, "accidents can happen."[231] That quote led many to believe that the United States had caused the Internet outage in North Korea.

---

225 Update on Sony, FBI.

226 Mark E. Manyin et al., North Korea: Back on the State Sponsors of Terrorism List? (CRS Report No. R43865) (Washington, DC: Congressional Research Service, 2015), 9, https://www.fas.org/sgp/crs/row/R43865.pdf.

227 Ibid.

228 "Statement by Secretary Johnson On Cyber Attack On Sony Pictures Entertainment," U.S. Department of Homeland Security, December 19, 2014, http://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.

229 Kristina Daugirdas and Julian Davis Mortenson, "United States Responds to Alleged North Korean Cyber Attack on Sony Pictures Entertainment," *The American Journal of International Law* 109, no. 2 (2015): 420, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1717302701?accountid=12702.

230 Ibid.

231 Ibid.

On January 02, 2015, the White House issued additional economic sanctions against North Korea.[232] Admiral Rogers, Commander USCYBERCOM and Director NSA, feels that the U.S. needs to ensure the world knows that the cyber-attack on Sony crossed the line.[233] He said, "What concerned me was, given the fact that this is a matter of public record, if we don't publicly acknowledge it, if we don't attribute it and if we don't talk about what we're going to do in response to the activity ... I don't want anyone watching thinking we have not tripped a red line, that this is in the realm of the acceptable."[234] Even with their leader feeling that not enough has been done in response to the cyber-attack, neither USCYBERCOM nor NSA had a public role to play in the investigation. There were reports, however, that the NSA had successfully gained access to North Korea's computer systems recently, and some observers believed that should have allowed them to see the initial intrusion into Sony's network.[235]

The FBI Director, James Comey, made a statement saying that they believed the hackers gained access in September through a tactic called spear phishing.[236] Spear phishing is when massive amounts of emails are sent with encrypted links trying to get an employee to click on one that would allow the hackers to gain access. According to Sony's CEO, Michael Lynton, the company is a blameless victim, and Sony was prepared for conventional cybersecurity intrusions but that they had suffered "the worst cyber-attack in U.S. history."[237] FBI's Assistant Director, Joseph Demarest, agreed with Lynton and told the Senate that "the malware that was used would have slipped, probably would have gotten past 90% of the net defenses that are out there today in private industry, and I

---

[232] Exec. Order No. 13687, https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea.

[233] Joe Gould, "US Cyber Commander: Hackers Will Pay a Price," Defense News, May 11, 2015, http://www.defensenews.com/story/defense/policy-budget/cyber/2015/05/11/us-cybercom-rogers-cyber-deterrence/27140987/.

[234] Ibid.

[235] David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," January 18, 2015, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

[236] Elkind, "Hack of the Century," 80.

[237] Ibid., 67.

would challenge to even say government."[238] Even the spokesman for FireEye, a cybersecurity company, agreed stating that, "if a state actor wants to get in, he'll get in."[239] The attack on Sony was carefully planned and would have put the cybersecurity of the U.S. government to the test.

D. SUCCESS/FAILURE

In the aftermath of the attack, the U.S. government opened an investigation. In order to determine whether this investigation was successful, a definition of a successful investigation must be established. The goal of an investigation should be to identify the who, what, when, why, and how of the attack. In order to gain the most accurate information the first step must include putting the proper agency in charge.

The government is also interested in minimizing the effect of the attack, along with Sony. This requires the recovery of the information that was stolen and minimizing the distribution of what was not recovered. Additionally, the Sony case raises the issue of whether the government should work to close the security risk, ensuring that government systems would not be vulnerable to a similar attack, and coordinate with other companies to strengthen cybersecurity.

The FBI took on the lead role and carried out a successful investigation. According to government policy, the Secret Service should have been the lead investigator for the computer intrusion portion of the attack.[240] The FBI should have been the lead investigation for the copyright piracy and trade secret theft portion though.[241] According to the USA Patriot Act, the USSS is the primary agency for investigating cyber-attacks.[242] Primary jurisdiction for the three cyber-crimes was split between the Secret Service and the FBI, but the FBI conducted the investigation with little official

---

[238] Elkind, "Hack of the Century," 67.

[239] Ibid., 82.

[240] Reporting Computer, Internet-Related, or Intellectual Property Crime, U.S. Department of Justice, modified December 2015, https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime.

[241] Ibid.

[242] *USA PATRIOT Act,* Pub. L. No. 107-56, 115 Stat. 272 (2001).

help from any other agencies. The Sony case thus raises the issue of whether the investigation should have been more of a joint effort.

The next step for showing that the FBI conducted a successful investigation is to identify; the who, what, when, why, and how of the attack. The investigation carried out by the FBI identified all of these aspects in a timely manner with correct supporting evidence and updated the public with their findings.

The who portion is straightforward; identify the person or persons responsible. In this case the Guardians of Peace identified themselves as the attackers. The attackers provided their name but the FBI was able to trace the attack back to North Korea even though North Korea would not take responsibility for the attack.

The what is answered by looking at the attack itself and asking, what did it accomplish? The cyber-attack postponed the release and greatly reduced the profits made from the movie The Interview, and erased nearly half of Sony's computers, and servers.

The when is covered in the timeline, with the initial intrusion occurring in September 2014, through spear phishing, and the discovery of the attack on November 24, 2014. The FBI was able to identify the initial intrusion and follow what the hackers did once they had access to the network. The FBI traced what the hackers did, allowing the case to be studies by cybersecurity experts to formulate defenses against it.

The why, is the reasoning behind the attack. According to the FBI the attack was "intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves." As noted above, U.S. officials concluded that the intent of the attack was not to specifically harm Sony but to coercively obstruct exercise of the First Amendment by a foreign power.

The how portion of the investigation identified the initial access as a spear phishing attack in September and from there the attackers had access to the servers and the computers connected to those servers. Once the attackers had access all they had to do was avoid detection and carry out their plan.

This chapter has shown what happened leading up to, during, and after the cyber-attack conducted by North Korea against Sony. The executives at Sony disregarded multiple warnings and threats that a cyber-attack could happen. The Sony case, however, raises the question of whether the actual attack could have been prevented at the time, insofar as a nation such as North Korea will have more resources at its disposal than a company, even as large a one as Sony. The after effects on the attack caused more private companies to evaluate their own cybersecurity, and to make changes they deemed appropriate.

V. CONCLUSION, POLICY RECOMMENDATIONS, AND FURTHER RESEARCH

This thesis has discussed the available evidence to answer the question of whether the current cybersecurity responsibility allocation for DHS is optimal for achieving U.S. national cybersecurity objectives. This concluding chapter will offer a brief summary, followed by a discussion of possible policy recommendations for DHS, USSS, FBI, NSA/DOD, and DNI. The final section will identify areas that require further research to better understand the role of each of these organizations in cybersecurity.

A. CONCLUSION

This thesis examined the U.S. government's delineation for the roles and responsibilities of cybersecurity. The evolution of technology and the advances in cyberspace have made cybersecurity a vital interest for national security. Cyberspace provides a means for people to collaborate from across the world. That ease of communication is both advantageous and dangerous, which is why cybersecurity is so important. Proper cybersecurity can mitigate the dangerous side of cyberspace.

Chapter II identifies the evolution of cybersecurity laws and policies starting with the "Computer Security Act of 1987." The evolution starts with basic computer regulations and continues with the creation of multiple groups to further regulate or protect the growing cyber world. The National Security Telecommunications and Information Systems Security Committee is the first such group that was started in 1990. In 1998, with the signing of "PDD/NSC-63: Critical Infrastructure Protection," the physical protection of critical infrastructure was linked with protecting the same infrastructures from cyber-attacks.

The devastating terrorist attacks on September 11, 2001, changed the way the world viewed security at all levels. These attacks led directly to the passing of the Patriot Act, which expanded the roles and responsibilities of most government agencies for security, including cybersecurity. Another effect from the attacks was the creation of DHS in order to protect the U.S. from any future terrorist attack.

The establishment of the Comprehensive National Cyber Security Initiative (CNCI) in 2008 was the next major step forward for national cybersecurity. CNCI establishes a first line of defense against cyber-threats in order to strengthen the future of cybersecurity. CNCI also stressed the importance of collaboration between the government and private sector. This is further stressed in 2015, by "E.O. 13691: Encouraging Private-Sector Cybersecurity Collaboration," which identifies DHS as the liaison between the government and the private sector for cybersecurity and allows DHS to share classified information if deemed necessary.

Chapter II also outlines DHS's current cybersecurity mission along with the Secret Services mission under DHS. DHS is designated as the lead agency for national cybersecurity, and has established two main offices to support it. The Cyber Security Division focuses on collaboration and R&D to better secure the national computer network. The Office of Cybersecurity and Communications focuses on increasing the strength, resilience, and reliability of the national information infrastructure. The Secret Service has a cyber investigation mission. The mission is fulfilled through the Electronic Crimes Task Forces that are designed to identify, prevent, interrupt, and investigate any cyber-attacks of financial or critical infrastructure systems.

Chapter III briefly outlines the origin and the current cybersecurity missions for the FBI, NSA, DOD, and the DNI. The FBI is the primary agency for investigating cyber-crimes and cyber-attacks. The National Cyber Investigative Joint Task Force (NCIJTF) was established as the focal point for all cyber investigations. The NCIJTF also acts as a liaison between all levels of law enforcement and the Intelligence Community. In addition to NCIJTF, Cyber Task Forces were also established in order to better coordinate cyber investigations at both the local and national level.

The NSA and DOD cyber efforts are both led by the same person in a dual-hatted role. NSA's mission is two-fold: Signals Intelligence (SIGINT) and Information Assurance. SIGINT is the gathering, processing intelligence and advising the appropriate entity about threats. Information Assurance is preventing unauthorized access to the government's networks. Both of these mission support DOD's efforts to defend their and the United States' networks, and if necessary provide offensive cyber capabilities. The

intelligence for all cyber threats is fed to the Cyber Threat Intelligence Integration Center (CTIIC), which is led by the DNI. The DNI ensures that the intelligence that is received by CTIIC is processed and no link is missed and then provides that intelligence primarily to DHS, FBI, and DOD entities.

Chapter IV looks at the Sony Pictures Entertainment cyber-attack from 2014, in order to identify whether the current allocation of cyber responsibilities is appropriate. The attack caused Sony to lose approximately half of their information from personal computers, company computers and servers. The information that included movie scripts, email exchanges, salaries, and over 47,000 Social Security numbers, was only deleted after the attackers copied it. Within hours of the attack the FBI was notified and started the investigation. Portions of the stolen information were released over the next several months. In a press release the FBI identified the attack as originating from North Korea, and stated that the intent was to attack the freedom of speech provided by the First Amendment. The investigation of the attack was a success for the FBI, which identified the who, what, where, when, why, and how in a timely manner and provided updates on the investigation to the public.

B. POLICY RECOMMENDATIONS

While no single case study can be definitive, the research of this thesis offers insight into the policy changes that could be enacted in order to enhance the national cybersecurity effort. The discussion of this section offers proposals that merit further assessment on the basis of a wider range of cases.

1. DHS Cybersecurity Prevention Lead

The case of the Sony attack suggests that greater focus is needed on prevention and defensive operations. DHS is in the best position to be the lead agency for defensive cybersecurity. Under CSD and SECIR, DHS could continue to coordinate and promote cooperation between different government agencies and the private sector. As part of this, InfraGard could be transferred from the FBI to DHS's CSD. InfraGard is focused on preventing cyber-attacks and could be with the same entity that is in charge of preventing cyber-attacks.

The R&D section under CSD could expand its capabilities and continue its information sharing across government agencies and private industry lines. Cyber education could also become more of a priority to further cybersecurity and to assist in R&D.

The Network Security Deployment, under CS&C, could create a backup National Cybersecurity Protection System as a way to mitigate damages from a successful cyber-attack. To test this and to identify more issues FNR could develop a "Cyber Red-Team" that would continually test the cybersecurity across the government and provide a detailed weaknesses list up DHS chain of command and to the government entity that was identified. The red team reports would lead to best practices for prevention, identification, mitigation, and re-establishment of a network that can be shared through the government and to the private sector.

2. USSS Protection and Financial Missions

The Secret Service has a very broad set of responsibilities and their cyber investigation portion is not up to the standards set by the FBI. The Secret Service could focus its efforts on the protection and financial crimes missions. The protection mission does not allow a single mistake. If there is a mistake made under the protection mission, then one or more people may be killed. The cyber investigation mission that the Secret Service currently has is a distraction from their two primary missions. Cybersecurity should play a part in their protection mission, but the cybersecurity role could be limited to what affects the people the USSS is protecting. A special section needs to be developed that will deal with cybersecurity under the Secret Service. The same agents that are protecting people cannot be the agents that are responsible for cybersecurity. The cybersecurity agents need to be specially trained personnel who only focus on cybersecurity. If there is a cyber-attack against a protected person, then the Secret Service should assist the FBI in the investigation.

The financial mission is the founding mission for the Secret Service. They are the proven specialists in the financial crimes spectrum. Over 150 years has been dedicated to making the Secret Service the best financial investigation organization in the world. The

evolving cyber aspect of finances has made finances and cyber intertwined. The Secret Service needs to better develop financial cyber agents that can track down criminals in cyberspace. The existing ECSAP can be expanded to include two different tracks to develop cyber agents for protection and financial specialties.

3. FBI Lead Cyber Investigator

As seen in the Sony case, the FBI can conduct a successful national level investigation. The FBI's NCIJTF is already the focal point for cyber investigations, because along with the 56 CTFs, NCFTA, and iGuardian, the FBI is the best established to be the lead investigation agency for all cyber-attacks and cyber-crimes. The laws and policies need to be updated so that the FBI is the lead investigation entity for cyber issues, and they would have the authority to investigate any crime associated with cyberspace. The ECTF from the Secret Service could be moved under NCIJTF to expand the capabilities. The FBI must also expand their training pipeline to better develop cyber specific agents. The cyber agents must be proficient in cybersecurity, and investigations.

The agents working at CTFs must continually strive to further their cyber education for a better understanding of the crimes they investigate. CTFs serve as liaisons between local entities and national level entities for cybersecurity. This is a good arrangement, but they must remember to only focus on investigating cyber-crimes and not on preventing them, since DHS covers that portion.

The FBI will also assist the Secret Service as requested for their cyber protection and financial missions. The cyber protection portion can be either preemptive or as part of an investigation. The financial collaboration would be for an investigation that needs both the Secret Service's financial expertise and the FBI's cyber expertise.

4. NSA/DOD Maintain Mission and Expand Capabilities

As seen in Chapter III the NSA and DOD are the main entities that look out towards other countries as their primary focus. They are focused on intelligence gathering, and defensive and offensive cyber operations against foreign entities. This could remain the case, and neither entity should shift their focus to domestic

cybersecurity. The DOD should be primarily focused on other countries' governmental and military cyber capabilities, and how to mitigate or interrupt them. The DOD should be the only cyber entity that will have offensive capabilities. The NSA and DOD should both focus on expanding their capabilities to ensure that they are ahead of our adversaries.

5. DNI Expand CTIIC

The DNI's role in cybersecurity started little more than a year ago and is contributing to increasing the national cybersecurity objectives. The CTIIC has been a great start for its purpose, but it could easily provide more actionable intelligence. It is designed to process and disseminate intelligence, primarily to NCCIC, NCIJTF, and USCYBERCOM. Right now this is a one-way stream of information, but it needs to flow both ways. The CTIIC could not only receive information from the IC but could also receive information from its three main consumers. Additionally, a feedback system needs to be established for the main consumers to provide constructive criticism in order to make CTIIC better.

C. FURTHER RESEARCH RECOMMENDATIONS

The cyber world is constantly evolving, and will not stop changing. This means that current research will always be needed for cyber issues. Our adversaries are probing for our weaknesses and are developing new ways to exploit them through cyberspace. In order to expand our understanding of cybersecurity and to prevent our adversaries from getting an upper hand, further research is needed. The R&D that is being conducted for cyber capabilities needs to be better integrated. The possible ways to do this needs to be identified and best practices need to be established for sharing R&D information but also preventing that same information from getting into the hands of our enemies.

Additional research is needed to determine the advantages and disadvantages in setting up an international cybersecurity sharing initiative. If the advantages outweigh the disadvantages, then how can it be established and governed? Should it be under the United Nations or is that too large of a group for honest sharing?

Cyber investigations need further research as well. How do they differ from other investigations? Is a cyber-crime always a federal investigation or what would make it a local or state level investigation and how should we develop the necessary cyber capabilities at the different levels?

Finally, the role of USCYBERCOM should be evaluated to see if it can offer improved support in cases such as the Sony hack. Current debates over whether it should remain where it is under U.S. Strategic Command or become its own combatant command offer a timely opportunity to evaluate its interagency role.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Asllani, Arben, Charles Stephen White, and Lawrence Ettkin. "Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. " *Journal of Legal, Ethical and Regulatory Issues* 16, no. 1 (2013): 7–14. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1370351181?accountid=12702.

Blue, Violet. "New Report: DHS is a Mess of Cybersecurity Incompetence." *ZDnet*, January 14, 2015. http://www.zdnet.com/article/new-report-the-dhs-is-a-mess-of-cybersecurity-incompetence/.

Boyd, Aaron. "DNI Clapper: Cyber Bigger Threat Than Terrorism." *Federal Times*, February 4, 2016. http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/.

Castelli, Christopher J. "DHS Official Downplays Potential for Sony Hacking to Spur Cybersecurity Changes." *Inside Cybersecurity* (Dec 16, 2014). http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1636659052?accountid=12702.

Crabtree, Susan. "DHS' Johnson: Sony Hack a Wake-up Call for Business." *Washington Examiner* (Dec 19, 2014). http://www.washingtonexaminer.com/dhs-johnson-sony-hack-a-wake-up-call-for-business/article/2557657.

Curran, John. "U.S. Should Clarify Leadership Roles in Cybersecurity, Sen. Mikulski Says." *Cybersecurity Policy Report* (Aug 02, 2010): 1. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/746442266?accountid=12702.

"Cyber-Security Group Pushes 12-Point Plan on White House." TechWeb (Dec 08, 2004): 1. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/201528422?accountid=12702.

Daugirdas, Kristina and Julian Davis Mortenson. "United States Responds to Alleged North Korean Cyber Attack on Sony Pictures Entertainment." *The American Journal of International Law* 109, no. 2 (04, 2015): 419–422. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1717302701?accountid=12702.

Doyle, Charles. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (CRS Report No. 97–1025). Washington, DC: Congressional Research Service, 2010. https://www.fas.org/sgp/crs/misc/97-1025.pdf.

Elkind, Peter. “Inside the Hack of the Century.” *Fortune*, July 2015. http://nics.syr.edu/wp-content/uploads/2016/04/Inside-the-Hack-of-the-Century.pdf.

Executive Office of the President of the United States. *Communications Intelligence.* National Security Council Intelligence Directive No. 9. Washington, DC: Executive Office of the President of the United States, 1952. http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa02b.pdf.

———. *Critical Infrastructure Protection.* Presidential Decision Directive/NSC-63. Washington, DC: Executive Office of the President of the United States, 1998. http://fas.org/irp/offdocs/pdd/pdd-63.htm.

———. *Critical Infrastructure Identification, Prioritization, and Protection*. Homeland Security Presidential Directive No. 7. Washington, DC: Executive Office of the President of the United States, 2003. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf.

———. *Critical Infrastructure Security and Resilience*. Presidential Policy Directive 21. Washington, DC: Executive Office of the President of the United States, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

———. *Establishment of the Cyber Threat Intelligence Integration Center*. Presidential Memorandum. Washington, DC: Executive Office of the President of the United States, 2015. https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

———. *National Policy for the Security of National Security Telecommunications and Information System.* National Security Directive 42. Washington, DC: Executive Office of the President of the United States, 1990. http://fas.org/irp/offdocs/nsd/nsd42.pdf.

———. *The Comprehensive National Cybersecurity Initiative*. Washington, DC: Executive Office of the President of the United States, 2008. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Field, Joeli R. “Cybersecurity: Division of Responsibility in the U.S. Government.” working paper, American Military University, Interagency Operations, Charles Town, WV, 2010. http://www.nsci-va.org/CyberReferenceLib/2010-09-18-Cybersecurity-Division%20of%20Responsibility%20in%20the%20US%20Government-Joeli%20Field.pdf.

Franke, Ulrik, and Joel Brynielsson. “Cyber Situational Awareness - A Systematic Review of the Literature.” *Computers & Security* 46, (10, 2014): 18–31. doi: http://dx.doi.org/10.1016/j.cose.2014.06.008. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1642269155?accountid=12702.

Gould, Joe. “US Cyber Commander: Hackers Will Pay a Price.” *Defense News*, May 11, 2015. http://www.defensenews.com/story/defense/policy-budget/cyber/2015/05/11/us-cybercom-rogers-cyber-deterrence/27140987/.

Goutam, Rajesh Kumar. “Importance of Cyber Security.” *International Journal of Computer Applications* 111, no. 7 (2015). doi: http://dx.doi.org/10.5120/19550-1250. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1677936364?accountid=12702.

Greenemeier, Larry. “Federal Role in Ensuring Cybersecurity Isn’t Clear.” *InformationWeek* no. 1023 (Jan 24, 2005): 41. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/229160173?accountid=12702.

Gruenwedel, Erik. “FBI Doubles Down on North Korean Ties to Sony Cyber Attack. “ *Home Media Magazine* 37, no. 1 (Jan 12, 2015): 1–1,21. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1647424635?accountid=12702.

Hathaway, Melissa E. “Leadership and Responsibility for Cybersecurity.” *Georgetown Journal of International Affairs*, Special Issue (2012). http://belfercenter.ksg.harvard.edu/files/71-80-hathaway.pdf.

Hill, Kashmir. “Beware: Downloading the Hacked Sony Pictures Docs Could Bring the Feds to Your Door.” *Fusion*, December 11, 2014. http://fusion.net/story/32988/beware-downloading-the-hacked-sony-pictures-docs-could-bring-the-feds-to-your-door/.

InfraGard. “InfraGard: Partnership for Protection.” Accessed May 13, 2016. https://www.infragard.org/.

“Is Kim Jong Un Innocent?; Cyber-Security.” *The Economist* 414, no. 8919 (Jan 03, 2015): 22. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1641939004?accountid=12702.

Johnson, Ted. “Hack Aftermath.” *Variety* 327, no. 11 (Apr 14, 2015): 43–44. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1675636219?accountid=12702.

Joint Chiefs of Staff. “Adm. Winnefeld’s Remarks at the West Point Cyber Conference.” May 14, 2015. http://www.jcs.mil/Media/Speeches/tabid/3890/Article/ 589135/adm-winnefelds-remarks-at-the-west-point-cyber-conference.aspx.

Lie, Eric, Rorry Macmillan, and Richard Keck. “Cybersecurity: The Role and Responsibilities of an Effective Regulator.” Paper presented at 9th International Telecommunications Union Global Symposium for Regulators, Beirut, Lebanon, November 2009. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

Manyin, Mark E., Emma Chanlett-Avery, Dianne E. Rennack, Ian E. Rinehart, John W. Rollins. *North Korea: Back on the State Sponsors of Terrorism List?* (CRS Report No. R43865). Washington, DC: Congressional Research Service, 2015. https://www.fas.org/sgp/crs/row/R43865.pdf.

Martin, David M. “Tracing the Lineage of DarkSeoul.” *SANS Institute*. November 20, 2015. https://www.sans.org/reading-room/whitepapers/warfare/tracing-lineage-darkseoul-36787.

McCormick, Rick. “Sony Attacks Torrents to Prevent Spread of Stolen Data.” *The Verge*, December 11, 2014. http://www.theverge.com/2014/12/11/7375617/sony-attacks-torrents-to-prevent-spread-of-stolen-data.

Myers, Elizabeth A. “Cyber as a ‘Team Sport: Operationalizing a Whole-of-Government Approach to Cyberspace Operations.” Master’s thesis, Joint Forces Staff College, 2011. http://www.dtic.mil/dtic/tr/fulltext/u2/a545638.pdf.

National Archives and Records Administration. “Records of the U.S. Secret Service [USSS]: Record Group 87, 1863–1988.” Accessed April 15, 2016. http://www.archives.gov/research/guide-fed-records/groups/087.html#87.1.

National Security Agency. “Cyber.” Modified May 3, 2016. https://www.nsa.gov/what-we-do/cyber/.

———. “Frequently Asked Questions.” Modified May 3, 2016. https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml.

Newmeyer, Kevin P. “Who should Lead U.S. Cybersecurity Efforts?” *Prism: A Journal of the Center for Complex Operations* 3, no. 2 (03, 2012): 115–126. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1011482876?accountid=12702.

Nielsen, S. C. “Pursuing Security in Cyberspace: Strategic and Organizational Challenges.” *Orbis* 56, no. 3: 336–356. doi: http://dx.doi.org/10.1016/j.orbis.2012.05.004. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1034349334?accountid=12702.

Office of the Director of National Intelligence. “History.” Accessed May 13, 2016. https://www.dni.gov/index.php/about/history.

———. “Mission, Vision & Goals.” Accessed May 13, 2016. https://www.dni.gov/index.php/about/mission.

———. “Office of the Director of National Intelligence.” Accessed May 13, 2016. https://www.dni.gov/index.php.

Parrish, Karen. “Privacy or Security in Cyber? Both, NSA Chief Says.” U.S. Department of Defense. March 2, 2016. http://www.defense.gov/News-Article-View/Article/684015/privacy-or-security-in-cyber-both-nsa-chief-says.

Partnership for Public Service, and Booz Allen Hamilton. *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce*. McLean, VA. Booz Allen Hamilton, 2009. https://www.boozallen.com/content/dam/boozallen/media/file/CyberIn-Security_2009.pdf.

Partnership for Public Service, and Booz Allen Hamilton. *Cyber In-Security II: Closing the Federal Talent Gap*. McLean, VA. Booz Allen Hamilton, 2015. http://ourpublicservice.org/publications/viewcontentdetails.php?id=504.

“Preventing 9/11 in the Cyber World.” *Information Management* 47, no. 3 (May, 2013): 18. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1430501590?accountid=12702.

Reese, Shawn. *The U.S. Secret Service: History and Missions* (CRS Report No. RL34603). Washington, DC: Congressional Research Service, 2014. https://fas.org/sgp/crs/homesec/RL34603.pdf.

Robb, David. “Sony Hack: A Timeline.” Deadline, December 22, 2014. http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/.

Roesener, August G, PhD., U.S.A.F., Carl Bottolfson U.S.A.F., and Gerry Fernandez U.S.N. “Policy for U.S. Cybersecurity.” *Air & Space Power Journal* 28, no. 6 (Nov, 2014): 38–54. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/1652188677?accountid=12702.

Sanger, David E., and Martin Fackler. “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say.” *New York Times*, January 18, 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

Schwartz, Mathew J. “FBI Defends Cyber Investigation Skills.” *InformationWeek* no. 1300 (May 16, 2011): 19. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/871111525?accountid=12702.

Secretary of Defense. *The Department of Defense Cyber Strategy*. DOD Cyber Strategy. Washington, DC: Secretary of Defense, 2015.

———. *The National Security Agency and the Central Security Service*. DOD Directive S-5100.20. Washington, DC: Secretary of Defense, 1971.

Shackelford, Scott J., and Richard B. Andres. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. " *Georgetown Journal of International Law* 42, no. 4 (Summer, 2011): 971. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/897838433?accountid=12702.

Soergel, Andrew. "Sony Says It's Not Curtains for 'The Interview' After All." *U.S. News*, December 24, 2014. http://www.usnews.com/news/newsgram/articles/2014/12/24/seth-rogens-and-james-francos-the-interview-back-on-says-sony.

Sorkin, Aaron. "The Sony Hack and the Yellow Press." *New York Times*, December 15, 2014. http://www.nytimes.com/2014/12/15/opinion/aaron-sorkin-journalists-shouldnt-help-the-sony-hackers.html?_r=1.

U.S. Army Cyber Command. "The Facts: Cyber Mission Force." March 2, 2016. http://www.arcyber.army.mil/fact_sheets/ARCYBER%20fact%20sheet%20-%20Cyber%20Mission%20Force%20(2March2016).pdf.

U.S. Department of Defense. "Remarks by Secretary Carter to U.S. Cyber Command Workforce at Fort Meade, Maryland." March 13, 2015. http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/607024.

———. "Statement by Pentagon Press Secretary Peter Cook on DOD's 'Hack the Pentagon' Cybersecurity Initiative." March 2, 2016. http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

U.S. Department of Energy. "Cybersecurity Is Every Citizen's Responsibility." October 2013. http://energy.gov/articles/cybersecurity-every-citizens-responsibility.

U.S. Department of Homeland Security Science and Technology Directorate. An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States. Edited by Mathew H. Fleming, Eric Goldstein, and Robert Tuohy. Arlington, VA, May 24, 2011. http://www.homelandsecurity.org/docs/reports/MHF-and-EG-Analysis-of-authorities-supporting-efforts-of-DHS-to-secure-cyberspace-2011.pdf.

———. "About the National Cybersecurity and Communications Integration Center." Modified September 22, 2015. http://www.dhs.gov/national-cybersecurity-communications-integration-center.

———. "Creation of the Department of Homeland Security." Modified October 2014. http://www.dhs.gov/creation-department-homeland-security.

———. “Cyber Security Division.” Modified August 2015. http://www.dhs.gov/science-and-technology/cyber-security-division.

———. “Cybersecurity: A Shared Responsibility.” October 2013. https://www.dhs.gov/blog/2013/10/18/cybersecurity-shared-responsibility.

———. “Federal Network Resilience.” Modified September 22, 2015. http://www.dhs.gov/federal-network-resilience.

———. “Network Security Deployment.” Modified September 22, 2015. http://www.dhs.gov/network-security-deployment.

———. “Office of Cybersecurity and Communications.” Modified July 2015. http://www.dhs.gov/office-cybersecurity-and-communications.

———. “Office of Emergency Communications.” Modified September 23, 2015. http://www.dhs.gov/office-emergency-communications.

———. “Stakeholder Engagement and Cyber Infrastructure Resilience.” Modified September 23, 2015. http://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience.

———. “Statement by Secretary Johnson On Cyber Attack On Sony Pictures Entertainment.” December 19, 2014. http://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.

———. “U.S. Secret Service Electronic Crimes Task Forces.” Accessed April 15, 2016. https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf.

U.S. Department of Justice. “Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section Criminal Division.” January 14, 2015. http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

———. “Reporting Computer, Internet-Related, or Intellectual Property Crime.” Modified December 2015. https://www.justice.gov/criminal-ccips/reporting-computer-Internet-related-or-intellectual-property-crime.

U.S. Federal Bureau of Investigation. “A Brief History of the FBI.” Accessed May 13, 2016. https://www.fbi.gov/about-us/history/brief-history.

———. “Cyber Task Forces.” Accessed May 13, 2016. https://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1.

———. “iGuardian: The FBI’s Industry-Focused Cyber Intrusion Reporting Platform.” Accessed May 13, 2016. https://www.fbi.gov/stats-services/iguardian.

———. “National Cyber-Forensics & Training Alliance.” Accessed May 13, 2016. https://www.fbi.gov/about-us/investigate/cyber/national-cyber-forensics-training-alliance.

———. “National Press Releases: Update on Sony Investigation.” December 19, 2014. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

———. “Ten Years After: The FBI Since 9/11-Cyber.” Accessed May 13, 2016. https://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber.

U.S. Secret Service. “The Investigative Mission: Cyber Operations.” Accessed April 15, 2016. http://www.secretservice.gov/investigation/.

———. “USSS History.” Accessed April 15, 2016. http://www.secretservice.gov/about/history/events/.

U.S. Strategic Command. “U.S. Cyber Command.” Modified March 2015. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

Vijayan, Jaikumar. “Cybersecurity Official Says White House should Lead.” *Computerworld* 43, no. 16 (2009): 6. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/34185659?accountid=12702.

Wagner, Thomas D. “Sharing Cyber Intelligence in Trusted Environments: A Literature Review.” working paper, School of Computing Telecommunications and Networks, Faculty of Computing Engineering and the Built Environment, Birmingham City University, Birmingham, England. Accessed May 20, 2016. https://www.bcu.ac.uk/Download/Asset/633bd91b-4d73-e511-80ce-005056831842.

White House. “Fact Sheet: Cyber Threat Intelligence Integration Center.” February 25, 2015. https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

“White House, Congress Flunk on Cyber Security, CSIA Says.” *TechWeb* (Dec 14, 2005): 1. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/201509659?accountid=12702.

Wilshusen, Gregory C. *Critical Infrastructure Protection: Measures Needed to Assess Agencies’ Promotion of the Cybersecurity Framework* (GAO-16-152). Washington, DC: U.S. Government Accountability Office, 2015. http://www.gao.gov/assets/680/674300.pdf.

Young, Mark D. “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power.” *Journal of National Security Law and Policy* 4, no. 173 (2010). http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California