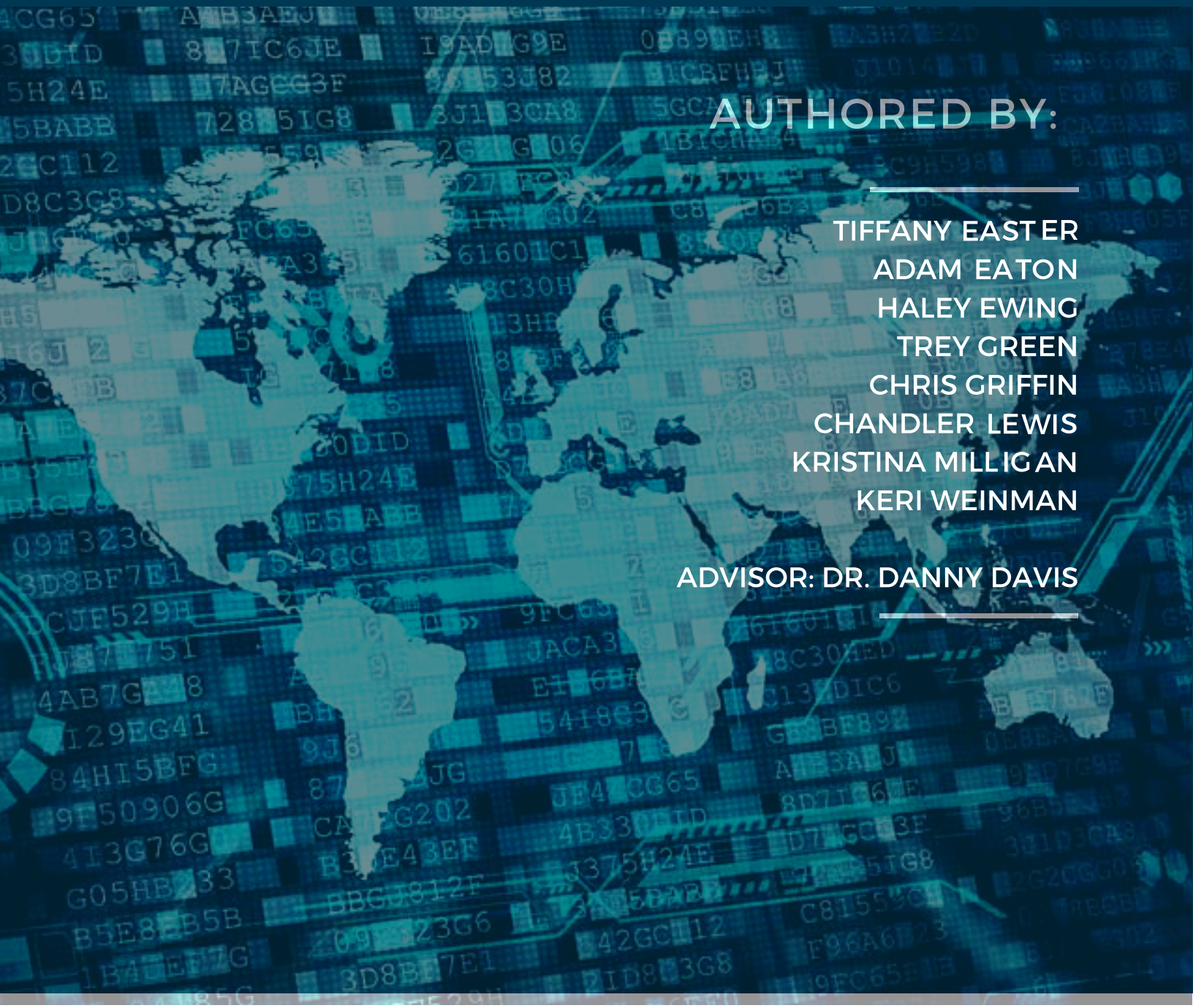


AUTHORED BY:

TIFFANY EASTER
ADAM EATON
HALEY EWING
TREY GREEN
CHRIS GRIFFIN
CHANDLER LEWIS
KRISTINA MILLIGAN
KERI WEINMAN

ADVISOR: DR. DANNY DAVIS

2018-2019 CAPSTONE PROJECT
CLIENT: POINTSTREAM, INC.

COMPREHENSIVE U.S. CYBER FRAMEWORK

KEY ASPECTS OF CRITICAL INFRASTRUCTURE, PRIVATE SECTOR, AND PERSONALLY IDENTIFIABLE INFORMATION

The Bush School
OF GOVERNMENT & PUBLIC SERVICE
TEXAS A&M UNIVERSITY

2018 – 2019 Capstone Team
The Bush School of Government and Public Service, Texas A&M University
Advisor: Danny W. Davis, Ph.D.

About the Project

This project is a product of the Class of 2019 Bush School of Government and Public Service, Texas A&M University Capstone Program. The project lasted one academic year and involved eight second-year master students. It intends to synthesize and provide clarity in the realm of issues pertaining to U.S. Internet Protocol Space by demonstrating natural partnerships and recommendations for existing cyber incident response. The project was produced at the request of PointStream Inc., a private cybersecurity contractor.

Mission

This capstone team analyzed existing frameworks for cyber incident response for PointStream Inc. in order to propose a comprehensive and efficient plan for U.S. cybersecurity, critical infrastructure, and private sector stakeholders.

Advisor

Dr. Danny Davis - Associate Professor of the Practice and Director, Graduate Certificate in Homeland Security

Capstone Team

Tiffany Easter - MPSA 2019
Adam Eaton - MPSA 2019
Haley Ewing - MPSA 2019
Trey Green - MPSA 2019
Christopher Griffin - MPSA 2019
Chandler Lewis - MPSA 2019
Kristina Milligan - MPSA 2019
Keri Weinman - MPSA 2019

Acknowledgement

The Capstone Team would like to express gratitude to COL Phil Waldron, Founder and CEO of PointStream Inc., for this opportunity and invaluable support throughout the duration of this project. We would also like to thank the Bush School Faculty and Staff and the various contributors to our project, LTG (Ret.) Kevin McLaughlin, Dr. Stephen Cambone, and BG (Ret.) Leesa Papier.

Table of Contents

Acronym List

ACs	**Advisory Councils**
ACI	**American Cyber Institute**
AI	**Artificial Intelligence**
APT	**Advanced Persistent Threat**
ARPA	**Advanced Research Projects Agency**
CD	**Cybersecurity Division**
CIA	**Central Intelligence Agency**
CISA	**Cybersecurity and Infrastructure Security Agency**
CNA	**Computer Network Attacks**
CND	**Computer Network Defense**
CNE	**Computer Network Exploitation**
CNO	**Computer Network Operations**
CSIRT	**Computer Security Incident Response Team**
DAFB	**Dyess Air Force Base**
DARPA	**Defense Advanced Research Projects Agency**
DCI	**Defense Critical Infrastructure**
DDoS	**Distributed Denial of Service**
DHS	**Department of Homeland Security**
DHS CS	**Department of Homeland Security Cyber Strategy**
DIA	**Defense Intelligence Agency**
DIB	**Defense Industrial Base**
DNS	**Domain Name System**
DOC	**Department of Commerce**
DoD	**Department of Defense**
DoD CS	**Department of Defense Cyber Strategy 2018**
DoDM	**Department of Defense Manual**
DOE	**Department of Energy**

Acronym List

DOI	**Department of the Interior**
DOJ	**Department of Justice**
DOS	**Department of State**
DOT	**Department of Transportation**
DSCA	**Defense Support for Civilian Authorities**
DSS	**Defense Security Services**
ECD	**Emergency Communication Division**
EO	**Executive Order**
EPA	**Environmental Protection Agency**
ERCOT	**Electric Reliability Council of Texas**
EU	**European Union**
FBI	**Federal Bureau of Investigation**
FBI IC3	**Federal Bureau of Investigation Internet Crime Complaint Center**
FCC	**Federal Communications Commission**
FEMA	**Federal Emergency Management Agency**
FISA	**Foreign Intelligence Surveillance Act**
FSRAs	**Federal and State Regulatory Agencies**
FTC	**Federal Trade Commission**
GAO	**Government Accountability Office**
GDPR	**General Data Protection Regulation**
GLBA	**Gramm-Leach-Bliley Act**
GSA	**General Services Administration**
HHS	**Department of Health and Human Services**
HIPAA	**Health Insurance Portability and Accountability Act**
HPSCI	**House Permanent Select Committee on Intelligence**
IC	**Intelligence Committee**
InfraGard	**Federal Bureau of Investigation InfraGard program**

Acronym List

IP	**Internet Protocol**
IPTF	**Infrastructure Protection Task Force**
ISACs	**Information Sharing and Analysis Centers**
ISD	**Infrastructure Security Division**
IT	**Information Technology**
IoT	**Internet of Things**
JCS	**Joint Chiefs of Staff**
JP	**Joint Publication**
LFA	**Lead Federal Agency**
LGs	**Local Governments**
NCCIC	**National Cybersecurity and Communications Integration Center**
NCIRP	**National Cyber Incident Response Plan**
NCS	**White House National Cyber Strategy**
NEW	**Network-enabled Electronic Warfare**
NGOs	**Non-Governmental Organizations**
NIPP	**National Infrastructure Protection Plan**
NIST	**National Institute for Standards and Technology**
NPPD	**National Protection and Programs Directorate**
NRC	**Nuclear Regulatory Commission**
NRF	**National Response Framework**
NRMC	**National Risk Management Center**
NSA	**National Security Agency**
NSS	**White House National Security Strategy**
ODNI	**Office of the Director of National Intelligence**
OFAs	**Other Federal Agencies**
OMB	**Office of Management and Budget**
OPM	**Office of Personnel Management**

Acronym List

RADICS	**Rapid Attack Detection, Isolation and Characterization Systems**
PEs	**Private Entities**
PII	**Personally Identifiable Information**
PPD	**Presidential Policy Directive**
SCADA	**Supervisory Control and Data Acquisition**
SEC	**Securities and Exchange Commission**
SECDEF	**Secretary of Defense**
SIGINT	**Signals Intelligence**
SLTT	**State, Local, Tribal, and Territorial Governments**
SNRA	**Strategic National Risk Assessment**
SSCI	**Senate Select Committee on Intelligence**
STT+IAGs	**State, Tribal, Territorial, and Insular Area Governments**
TCSSP	**Texas Cybersecurity Strategic Plan**
TDIR	**Texas Department of Information Resources**
USCYBERCOM	**U.S. Cyber Command**
U.S.C.	**United States Code**
US-CERT	**U.S. Computer Emergency Readiness Team**
USDA	**Department of Agriculture**
USDT	**Department of the Treasury**
USNORTHCOM	**U.S. Northern Command**
USPI	**U.S. Persons Information**
WMD	**Weapons of Mass Destruction**
UK	**United Kingdom**
USSR	**Union of Soviet Socialist Republics**

Executive Summary

While the societal, governmental, and economic benefits of a technologically-connected global community are potentially substantial, so too are the risks associated with protecting data and securing cyberspace against malicious activity. Providing security in cyberspace has generated the need for a new technology discipline: cybersecurity. The continuing proliferation and sophistication of cyber threats will allow for cyber actors at many levels, from simple hackers to antagonistic nation-states, to utilize them against U.S. interests. The U.S. must therefore be equipped both technologically and administratively to address these threats. This report examines the issues surrounding U.S. capabilities in providing cyber response, focusing on the federal level but including considerations for state and local governments as well as the private sector, in order to provide recommendations for developing a comprehensive, national cyber framework.

Any discussion of a national cyber framework begins with identifying the role of the Federal Government and the current laws, strategies, plans, and frameworks that dictate how the Federal Government responds to a cyberattack against critical infrastructure. The various and often overlapping governance and guidance documents increases the complexity of cyber response. Alleviating this complexity requires first understanding the fundamental structure of U.S. critical infrastructure and the current capabilities of the Federal Government to respond to a cyberattack. An evaluation of the governance and guidance documents outlines the roles and responsibilities of each various Federal, state, and local governments, as well as private sector entities and identifies overlaps and potential deficiencies in guiding response capabilities.

Understanding the role that the private sector can assume in cybersecurity is important when developing a national cyber framework. Since the majority of U.S. critical infrastructure is owned or operated by private sector entities, the capabilities and deficiencies in current private sector cybersecurity and cyber defense systems will have an impact on concerns for national security. The lack of comprehensive laws and policies to regulate cybersecurity cyber defense standards in the private sector has created vulnerabilities within cyberspace. These vulnerabilities are amplified due to a lack of a streamlined reporting process between the private sector and the government, as well as issues surround response jurisdiction and capabilities. Despite these issues, the private sector can still take on a vital role to complement or supplement government

cyber capabilities, and the establishment of a public-private partnership for cyber response can be a powerful tool to include in a national cyber framework.

Considerations for protecting the constitutionally-guaranteed right to privacy must also be included in any discussion of cybersecurity in the context of national defense and security. This includes determining the existence of any restrictions or over-restrictions on government capabilities, particularly those of the Department of Defense, when operating within U.S. Internet Protocol space for national defense. The right to privacy under the Fourth Amendment has been established through historic case law, with more recent Supreme Court rulings extending protections for personal privacy to cyberspace. However, the current legal structure of defense operations under the U.S. Code allows for the Department of Defense to operate within U.S. Internet Protocol space, with some restrictions. The capability to conduct national defense and security operations within cyberspace can be further strengthened by utilizing the private sector, which does not face the same restrictions as the government.

Introduction

The United States (U.S.) Constitution elucidates the responsibility of the Federal Government to provide for the national defense and to safeguard the individual's right to privacy: The former is defined explicitly in Article One, Section Eight and Article Four, Section Four,[1,2] while the latter has been established under precedents formed through case law interpretation of the Fourth Amendment (see Chapter 3 of this report). While these may be considered to be mutually exclusive under the conventional understanding of national defense, e.g. the Army does not need to enter an individual's home or ask for personal information to adequately defend the nation, changes in how warfare is defined and conducted, coupled with advances in technology, have blurred the lines and called into question the ability to defend and guarantee, in whole, a right to privacy.

At the turn of the 21st century, the U.S. military had established near-supremacy in conducting 20th century conflict by employing the latest in military technology. Utilizing the latest advancements in satellite technology, using precision (aka "smart") bombs, and fully grasping the military capabilities of information technology (IT), the U.S. was able to conduct conventional warfare on the terms of the more advanced Western military strengths.[3] Key to this was the expansion of capabilities for electronic warfare, which has existed since the military began utilizing advancements in radio technology in the early 20th century, for exploitation and control of the battlefield.[4] During the first decades of the 21st century, however, conflict began shifting to the irregular and the U.S. found itself increasingly engaged in asymmetric warfare, especially against terrorist and non-state actors in Afghanistan and Iraq.[5,6,7] Asymmetric warfare comprises a "disproportionate distribution of power" between adversaries, with the less militarily-equipped (i.e. weaker) force utilizing tactics that undermine the military advantage of the stronger force.[8] The use of cyberspace to conduct asymmetric warfare is likely to increase as the resources needed to carry out a cyberattack are relatively low, and these tactics are readily available.[9] The U.S. has made strides to improve capabilities to engage in such conflict through strategies like network-enabled electronic warfare (NEW), which utilizes the growing networks of interconnected and adaptive systems that have developed in tandem with the growth and proliferation of cyberspace.[10] However, the U.S. military will need to find new methods to conduct intelligence preparation of the battlefield to contend with both the complexities of cyberspace and the nature by which asymmetric actors operate.[11,12]

This changing conduct of warfare, coupled with globalization and advancements in communication technologies, has led to a struggle to balance national defense and individual freedom, particularly privacy. The U.S. has spent approximately $80 billion dollars on increasing and enhancing counterterrorism measures, both domestic and abroad.[13] The struggle to find this balance is compounded by how tightly the global community is connected electronically. Even in the physical realm, questions have arisen as to how much of the rights to free speech, due process, and privacy can be sacrificed in the name of national defense against terrorism.[14] However, these questions rise beyond defending only against terrorism. The extensive growth of the Internet and cyberspace, and the more recent hyper-connectivity brought on by the Internet of Things (IoT), which by their nature are open and connected and promote freedom of expression, have created a vast new space in which malicious actors can operate in near complete anonymity. It is these potential threats that exist in this vast, open cyberspace which the nation must defend against.

Cyberspace and the Internet

In order to understand the challenges faced to defend against malicious activity within cyberspace, it is important to briefly describe the principles of cyberspace and the Internet and the distinction between them.

The Internet is the culmination of the continuous development of wireless technologies, beginning with the early mathematical models of James Clerk Maxwell in the middle of the 19th century through the U.S. patent of Marconi's wireless telegraph at the turn of the century. In attempting to improve upon the existing technology and beat the Union of Soviet Socialist Republics (USSR) after the launch of Sputnik in 1957, the Advanced Research Projects Agency (ARPA) was tasked with advancing U.S. capabilities in all areas of technological advancement.[15] The simultaneous research being conducted by the RAND Corporation and in universities into wireless communication, and that of the U.S. defense industry into satellite technologies and computer-to-computer communication, culminated in the development of ARPANET. The original purpose of ARPANET was to link research institutions funded by the Pentagon over telephone lines.[16] ARPANET ultimately served as the catalyst for the development of what eventually became the Internet, and industry and academic researchers during the 1980s further

advanced the principles of ARPANET to create a technological interface to provide human-to-human interaction. This led to the creation of the computing discipline by which the Internet was allowed to flourish.[17,18,19] Kleinrock describes the Internet as "the current manifestation of (community of users, merging of analog and digital technologies, and voice, data, video, text, image, fax, graphics, and streaming media) and the vortex around which an accelerating wave of change and improvement is taking place, not only in infrastructure, but also in the applications, users, services, and innovations of the technology."[15]

Cyberspace, as defined by the U.S. Joint Chiefs of Staff (JCS) is the "domain within the interdependent network of IT infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[20] Under this definition, the Internet is understood as one distinct facet of cyberspace, while cyberspace comprises all aspects of IT and includes the data collected, stored, and transmitted by users. However, when compared with Kleinrock's definition of the Internet given previously, it could be viewed that cyberspace and the Internet are synonymous. Colonel Suzanne Nielsen, currently the head of the Social Sciences Department and formerly the director of the International Relations Program at West Point, uses "cyberspace" and "Internet" as distinct terms and defines cyberspace as "the globally connected networks of hardware, software, and data, as well as the people who interact with them,"[21] indicating that cyberspace exists at a higher order than the Internet. Further examination into the literature regarding cybersecurity (to which this report belongs) discusses cyberspace as distinct from the Internet, and for the purposes of this report the discussion will center on cyberspace, which will be assumed to include the Internet. Specific references may be made to the Internet for purposes of discussion where considering the entirety of cyberspace is not appropriate.

The Internet of Things and Big Data

The growth of cyberspace after the turn of the 21st century has given rise to new ways in which humans can utilize technology to shape the environment around them. Already the world is experiencing the next phase in the evolution of computing as the world has moved and continues to move further away from the traditional desktop and into a reality where the digital network connects the objects around us.[22] Cloud computing can provide the ability to perform distributed

or parallel computing, in order to improve computing efficiency through scaling complex processes. This form of computing can allow for the dynamic sharing, selection, and aggregation of resources distributed across various geographic locations.[23,24] This transition from using the Internet to connect end-user devices to using it to connect physical objects that identify, communicate, and interact with each other humans gives rise to the Internet of Things (IoT).[25] Machine-to-machine interaction in the IoT will occur over both wired and wireless technology, which can allow for a vast network of objects of all sizes and uses to communicate.[26] It is predicted that by 2020, up to 28 billion devices will be connected to the Internet, two-thirds of which will be represented by previously unconnected devices including household appliances, thermostats, automobiles, and sensors.[27] The continued proliferation of the IoT will support the further development and enhancement of "smart cities," or cities where infrastructure, city management systems, and other basic functions are conducted by objects connected to the network.[28]

These new, expansive networks and smart cities will require the collection, processing, and storage of large amounts of data generated by the connected machines and the human users that interface with the machines. Whereas in the past data analysis was more structured and conducted in a more static environment, technological advances and a move toward the widespread implementation of IoT applications has made big data collection and analysis a dynamic and evolutionary process.[29] The amount of big data collected can be so large that ordinary software technology cannot process all of it,[30] requiring alternative means for storage and handling of this data until it is needed for processing. Cloud computing provides a useful tool, as it has almost unlimited processing and storage capabilities.[31] Coupling big data with artificial intelligence (AI) is allowing computers to process this vast amount information faster, while increasing the ability for machines to make real-time decisions and develop solutions to complex problems faster than humans.[32] Further advances in quantum computing, which will outperform current and future supercomputing capabilities, will also speed up computational processes using big data.[33,34]

While the potential benefits of this technological interconnectivity and use of big data are enormous, the potential threats must also be considered. Any entity that collects, processes, or stores digital data puts that data at risk of unauthorized access, corruption, or theft. Wireless

connections can also be exploited, allowing for access to control of critical infrastructure, networks, and systems by virtually anyone with a computer and an Internet connection. Malicious actors that threaten the security of data and connected systems are numerous, and the tools they use can be simple and crude, or complex and sophisticated.

Cybersecurity and Cyber Threats

The ability to protect IT systems has become critical, as these elements have become ubiquitous in modern society and government.[35] This is not a new phenomenon, however; the practice of protecting digital networks extends back to the 1980s and early 1990s.[36] But as the Internet becomes more sophisticated and cyberspace continues to expand to include new elements, so too will the associated threats continue to grow and become more advanced. The technological advancements associated with cyber threats have reduced the amount of resources required to perpetrate some types of attacks. This increases the availability of such tools to a number of different malicious cyber actors. And those actors with significantly more technological and financial resources can utilize more sophisticated types of threats.

There are various actors that conduct malicious cyber activities. These include hacktivists, insider threats, nation-states, cyber terrorists, and cyber criminals. Each of these actors have different motivations for carrying out a cyberattack. And each have different levels of sophistication and resources with which to launch a specific type of attack. Hacktivists are in essence activists that operate, either independently or under a wider organizational structure, within cyberspace to achieve or further their specific agenda.[37] This agenda is often political, religious, or social in nature.[38] The main goal of cyber criminals, similar to criminals in the physical world, is to steal things from others; in cyberspace, this is typically sensitive information that can be used for financial gain.[39] Cyber terrorists are also similar to their counterparts in the physical world in that they seek a political or ideological end through their actions, though cyber terrorists operate in the anonymous and borderless realm of cyberspace.[40] The Federal Bureau of Investigation (FBI) defines cyber terror as "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information."[41]

Perhaps most alarming is the way in which nation-states are using cyberspace and the Internet to conduct malicious and subversive activities against other nations to steal classified information, disrupt the operation of critical infrastructure, or subvert the social, economic or governmental processes.[42] Russia has utilized cyber incursions to intimidate, as in Ukraine in 2015, create fear, as in Georgia in 2008, and attempt to destabilize, as in Estonia in 2007.[43,44,45] Files stolen from the German Parliamentary Committee in 2015 were attributed to Russia or an actor with support from Russia, as were the misinformation campaigns in Syria and the Crimea.[46] While Russian cyber activity against the U.S. has historically been smaller scale, beginning in 2014 Russian hacks into U.S. government computers became more complex, even going so far as to attack cyberattack alert systems.[47]

China too has engaged in malicious cyber activity, both economic and military. Chinese economic expansion over the last decades of the 20th and into the 21st century has been attributed to intellectual property theft, using the Internet to steal technologies from foreign firms as an alternative to domestic innovation.[43] The country's most recent *Military Strategic Guidelines* place on emphasis on "informatization" of the military and an increase in the capabilities for asymmetric warfare.[48] Chinese cyber incursions against the U.S. began around 2005 to collect intelligence, spot vulnerabilities, and insert trapdoors into U.S. military systems.[49] The Edward Snowden leaks revealed that in 2010, Chinese hackers conducted over 30,000 cyber incursions against the networks of the Pentagon and other intelligence agencies to steal information.[50]

Smaller, less developed states are also engaging in malicious cyber activity. North Korea employs large numbers of government hackers, both internationally and domestically, as a military strategy and to provide a government revenue stream.[51] Although its cyber infrastructure is considered rudimentary, North Korea has utilized sophisticated cyber tactics, including advanced persistent threats, against both South Korea and the U.S.[52] Iran has been building its cyber capabilities as a way to establish dominance in the Persian Gulf and compete against more powerful opponents internationally.[53] In the wake of Stuxnet, Iran has engaged in a build-up of cyber capabilities in direct competition with Israel.[54]

Malicious cyber threats can be used in an attack against a network or system in order to accomplish a number of goals. The National Institute of Standards and Technology (NIST)

provides the following as definitions for an attack within cyberspace.[55] The specific NIST documents in which these definitions are found are included in parentheses.

- An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality (NIST SP 800-82 Rev. 2);
- Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself (CSSNI 4009-2015, NIST SP 800-12 Rev. 1, NIST 800-30 Rev. 1);
- The realization of some specific threat that impacts the confidentiality, integrity, accountability, or availability of a computational resource (NIST SP 800-28 Ver. 2);
- An unauthorized entity's attempt to fool a Verifier or RP into believing that the unauthorized individual in question is the subscriber (NIST SP 800-63-3).

The Department of Defense (DoD), under Joint Publication (JP) 1-02 "Department of Defense Dictionary of Military Terms and Associated Terms", previously used the term "computer network attack" (CNA) to describes activities to "alter, disrupt, deceive, degrade, or destroy computer systems or networks," and the term "computer network exploitation" (CNE) to describe "activities taken to penetrate computer systems or networks by an adversary in order to obtain information resident on or transiting through these systems or networks. However, JP-3-13 "Information Operations" approved their removal from JP-1-02 in November 2012. They are still used throughout the literature.[56,57,58] For the purposes of this report, the terms "attack" and "cyberattack" are used to indicate an incident that occurs within cyberspace using any form of the methods described below, in accordance with the NIST definitions provided above. The term "hack" is used to identify an attack that results only in an unauthorized breach, in accordance with the fourth definition provided by NIST above. This type of attack is not intended to collect, disrupt, deny, degrade, or destroy.

In 2005, the U.S. Government Accountability Office (GAO) released Report 05-434: Critical Infrastructure Protection that included what were at the time identified as the current threats used to carry out a cyberattack. The methods and tactics used to carry out a cyberattack include the basic and familiar, such as worms, viruses, or malware, to the more sophisticated, including

exploit tools and sniffers, to those that require more time and effort to create and implement, namely phishing or advanced persistent threat (APT).[59] The FBI's Internet Crime Complaint Center (IC3) collects information related to Internet crime complaints and analyzes and disseminates that information to other law enforcement agencies as well as the general public.[60] The 2016 Internet Crime Report identified compromise of business email, ransomware, tech support fraud, elder fraud, and extortion as the major then-current crime trends.[61] Emerging threats in 2019 include formjacking, where cybercriminals use malicious code in retailers' websites to steal customer credit card information, and the continued use of social media for election interference.[62]

Worms and viruses are utilized by other attack methods to access the target system or network. While they achieve similar functions, worms can autonomously replicate while viruses require user action (opening an email, clicking a link) to propagate.[63] Phishing and spear phishing are social engineering methods used to extract sensitive personal information, usually in the form of an email request or an online form. While phishing is a broad threat that is sent to a large number of targets, spear phishing is used to target a smaller range of victims and has a higher rate of success.[64] Other threats identified in the GAO report include:[59]

- Exploit tools: publicly-available tools used by actors of varying levels of technical proficiency to locate vulnerabilities for entry in target systems or networks;
- Logic bombs: inserted code that causes a program to perform a destructive action when a specifically triggered;
- Sniffers: programs that are used to intercept and examine routed data to search for information transmitted in clear text, such as passwords;
- Trojan horses: useful or apparently useful software programs that conceal harmful code that when triggered executes a harmful function;

One of the more disruptive cyber threats is distributed denial of service (DDoS). The main intent of a DDoS attack is to utilize a large number of computers (referred to as botnets[65]) to overload a network with requests for information, in order to disrupt overall system performance.[66] One of the most vulnerable targets of a DDoS attack is the Domain Name System (DNS), the complex, global distributed database that is a vital for Internet functionality.[67] Because the DNS handles

such massive amounts of Internet "traffic," identifying and separating legitimate users from potential DDoS incursions is critical but time consuming.[68] Perpetrators of a DDoS incursion do not need to recruit large numbers of individual users to initiate the attack; instead, they utilize a worm or virus, often unknown to the infected machine and user, to infect other computers which are then used to carry out the incursion by requesting information from the targeted site.[66]

Another type of cyber threat that has the potential for increased malicious activity is the zero-day exploit. This type of threat targets a security flaw that exists within installed software, that the vendor may or may not know exists, but for which there is no current security patch available to address the vulnerability.[69] An exploit of a zero-day vulnerability thus takes advantage of the fact that the vulnerability may not have been previously identified. After that point, the system is already comprised and an attempt to eliminate the vulnerability would not address the infection already in the system.[70] As software vendors and users have become more aware of the potential existence of zero-day vulnerabilities within their systems, malicious actors have recently begun using computer worms that can autonomously change their sequence after a successful infection, which makes them more difficult to locate using standardized defensive software or fixes.[71]

Perhaps the most sophisticated current cyber threat is the advanced persistent threat (APT), where an unauthorized access is used to gain entry into a network or system, and the user remains in that system undetected for an extended period.[72] This type of threat is designed specifically for the systems against which it is intended to be used.[73] The nature of an APT attack requires significant resources, both technical and financial, which means these threats are more likely associated with nation-states than with other malicious cyber actors.[37] The term "advanced persistent threat" was first used as early as 2006 as what was then an unclassified means of describing cyber intrusions that originated in China, and between 2005 and 2013 there were 37 reported APT intrusions attributed to China including APT10 Menupass Team in 2009 and APT12 Calc Team in 2012.[74] While the targets of these intrusions were initially government entities or defense contractors, around the year 2010 APT intrusions specifically used against commercial targets increased.[75] One of the most famous, and dangerous, APT attacks is the Stuxnet attack against the Iranian nuclear program. Hoffman equates this type of attack with a biological virus; the computer virus or worm penetrates the host system and can remain dormant and undetected until it activates and causes the harm for which it was created[76].

Despite its immense military defensive capabilities, the U.S. is just as vulnerable to malicious cyber actors and activities as any other country. There is constant fear that a coordinated and concentrated attack against U.S. critical infrastructure is just beyond the horizon. This so-called "digital Pearl Harbor" would have catastrophic consequences.[77] The suspected Russian interference in the 2016 elections brings the threat to a more personal and pernicious level.[78] This was a campaign of misinformation and personal persuasion, targeting individual voters on both sides of the political spectrum to influence the election and drive.[79,80] The real and lasting damage goes beyond the results of that one election, however, as the specter of foreign interference influencing or changing the outcome of an election significantly undermines the foundation of our democratic processes and institutions.[36] The new cold war of cybercrime and cyber espionage activities both domestically and abroad, as well as the continued advance of cyber capabilities by China, Russia, North Korea, and Iran, will continue to heighten fears of a cyber crisis in the U.S., whether under an actual attack or a fear that one has or may occur.[81,82]

Federal Disaster Response

Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988 (the Stafford Act), which amended the Disaster Relief Act of 1974, the Federal Emergency Management Agency (FEMA), and by extension the Department of Homeland Security (DHS), has oversight of implementation for federal disaster relief assistance and the allocation of federal resources for relief.[83,84] However, real-time responsibility for incident response originates at the local level, with state and Federal assistance provided after local resources are determined to be insufficient or have been overwhelmed.[85] This "federalist" approach to emergency response can complicate authority when multiple jurisdictions are involved, or when attempting to determine when the disaster has grown beyond the classification of a localized incident.[85]

The overall language of the Stafford Act narrows the scope of Federal emergency response to natural disasters or incidents where property damage or significant loss of life has occurred. In addition to its use in natural disaster response, the Stafford Act was used in response to the Oklahoma City bombing in 1995, the 9/11 Attacks, and the Boston Marathon bombing in 2013.[84] The nature of cyberattacks, in that they have historically, in the U.S., caused non-physical damage and have not resulted in a loss of life, may not rise to the level of requiring a

comprehensive Federal response in the immediate aftermath, and would thus not fall under the jurisdiction of the Stafford Act. However, a concentrated cyberattack does have the potential to cause significant damage, even physical damage, to the nation's critical infrastructure (see the discussion in Chapter 1 of this report). If this type of incident, or worse, was to occur, immediate Federal response would be necessary, which will require the existence of a national policy framework by which this response can be conducted.

Basis of Research

Understanding that securing cyberspace is a complex issue, that cyber threats are an ever-present and continuously advancing reality, and that the current Federal emergency response law is not directly applicable to a cyberattack response, the authors of this report conducted research on the current state of cybersecurity and cyberattack response in the U.S., focusing on the Federal level but with consideration for lower levels of government as well as the private sector, to determine what frameworks, strategies, or guidance currently exist, and to assess their perceived adequacy in addressing cyberattacks. The research focuses on addressing the following statement:

> "The Department of Homeland Security (DHS) has responsibility for securing the nation's public and private cyberspace. However, it is the Department of Defense (DoD) that possesses the preponderance of cyber tools to combat attacks. The DoD operates under many restrictions when operating within the geographic borders of the U.S. The rules under which DoD operates in cyberspace were established based on historical signal intelligence (SIGINT) collection and Computer Network Exploitation, Computer Network Defense, and Cyber Network Attacks. These rules are meant to protect the privacy of U.S. citizens and entities and to place controls on exploitation and offensive operations. The separate states' National Guards under U.S. Code Title 32 have been assigned a cyber protection role for their state. This is similar to the long-standing operation of National Guard units in response to natural disasters found under the Stafford Act. Due to this, much has to be coordinated among the various federal and state/local government agencies and private sector elements. The current rules in

> place to defend our nation and private entities against a cyberattack or in response to a cyberattack are very restrictive."

Addressing this statement requires answering the following two questions:

1. Does current law over-restrict DoD in conducting national defense operations within Internet Protocol (IP) space?
2. What is the appropriate framework for government entities to coordinate with each other and with the private sector to respond to a cyberattack, while respecting the privacy of U.S. citizens?

It is important to distinguish the terminology used in the problem statement and the research questions. First, as discussed previously, the term "cyberattack" is used colloquially to refer to any incident that could be defined under the NIST definitions of an attack within cyberspace. In the instance of an incursion that does not collect, disrupt, deny, degrade, or destroy, the term "hack" may be used. Second, with respect to the first research question, this research focuses specifically on IP space, as opposed to all of cyberspace, as it considers the use of the communication network specifically, but not to include the use of infrastructure or data more broadly.

Limitations and Assumptions

The most up-to-date and leading-edge data and information regarding the U.S. government's activities concerning cybersecurity and cyberspace are assumed to be classified. This research was therefore limited to unclassified material that was available in the open-source literature, discoverable through online databases. This material was also limited in the time in which the research could be conducted: Some of the reference material may be from 2018 or 2019, but analyses on laws and regulations passed after November 2018 were not included, though these may be referenced in passing. There is a lack in consistency with what documentation is available, what is included in that documentation, and even the terminology used within that documentation, particularly between the various Federal agencies and entities. Every effort has been made to coordinate and correlate across the research material to create a level of consistency for this report. Additionally, cyber-specific policies will continue to change as new

types of threats and actors appear within the cyber realm, and as cyber technology continues to advance. These policies will also change in conjunction with changes at the Federal level. New presidential administrations will have differing policy objectives regarding cybersecurity, and changes in the composition of Congress will impact how successful a president can be at achieving specific policy objectives. Finally, the research is limited in that the findings and recommendations are tailored to include defensive cyber capabilities only.

The research was conducted under the following assumptions, as found in the open-source literature:

- All parties, including Federal agencies and entities, operate within their jurisdiction as prescribed by law;[86,87,88]
- DHS has the overriding authority regarding the protection of critical infrastructure;[89,90,91]
- The majority of critical infrastructure is owned and/or operated by the private sector. The exact amount ranges between 80% and 90% in the literature and what FEMA has reported;[92,93]
- There currently is no clear, singular, comprehensive federal framework for responding to cyber incidents. As such, we assume that this type of framework is necessary.[58,59,60,61]

Additionally, the research was conducted under the following assumptions that cannot be verified in the literature due to the classified nature of government operations. However, for the purpose of answering the research questions for this paper, these two assumptions are essential:

- DoD is currently restricted from effectively combating cyber threats through information and data gathering;
- DoD possess the preponderance of capabilities to combat cyber threats.

Structure of Report

This report is divided into three chapters. Chapter 1 focuses on the response mechanisms and frameworks that are currently in place to respond in the event of a cyber incident. This chapter examines the current structure of critical infrastructure and discusses cyber incidents that have occurred within critical infrastructure around the world. The chapter evaluates each of the

primary plans, strategies, frameworks, and partnerships, developed by a variety of departments, agencies, and documents. This evaluation outlines the roles and responsibilities of each entity in the event of a cyber incident. The overlap of these documents and agencies are presented and analyzed through a scorecard that identifies which authority has responsibility over specific response activities. The chapter concludes with recommendations on how the Federal Government should move forward to better streamline cyber incident response mechanisms.

Chapter 2 focuses on cybersecurity within the private sector, identifying the laws that govern how private sector entities operate within cyberspace. This chapter discusses the current state of cybersecurity regulation for the private sector and identifies the deficiencies in incident reporting to the Federal Government, as well as issues surrounding government jurisdiction over private industry and cyberspace. This chapter examines the relationship and interaction between the private sector and the government, and proposes a path forward for a more cooperative relationship regarding cybersecurity through public-private partnerships and cyber insurance. The chapter also discusses how the private sector can be utilized to address deficiencies in Federal Government cyber capabilities, including providing innovation and overcoming governmental restrictions for operating in cyberspace.

Chapter 3 concentrates on the personal information of private American citizens, the rights that protect that information, and the implications of cybersecurity on these rights. This chapter defines what comprises personal identifiable information and identifies the laws and regulations in place to protect this information, and then provides recommendations for how DoD can engage in cybersecurity without infringing on those rights through partnering with private industry or DHS. This chapter also provides clarity on how DoD is restricted when operating in U.S. IP space, specifically regarding the protection and usage of private information.

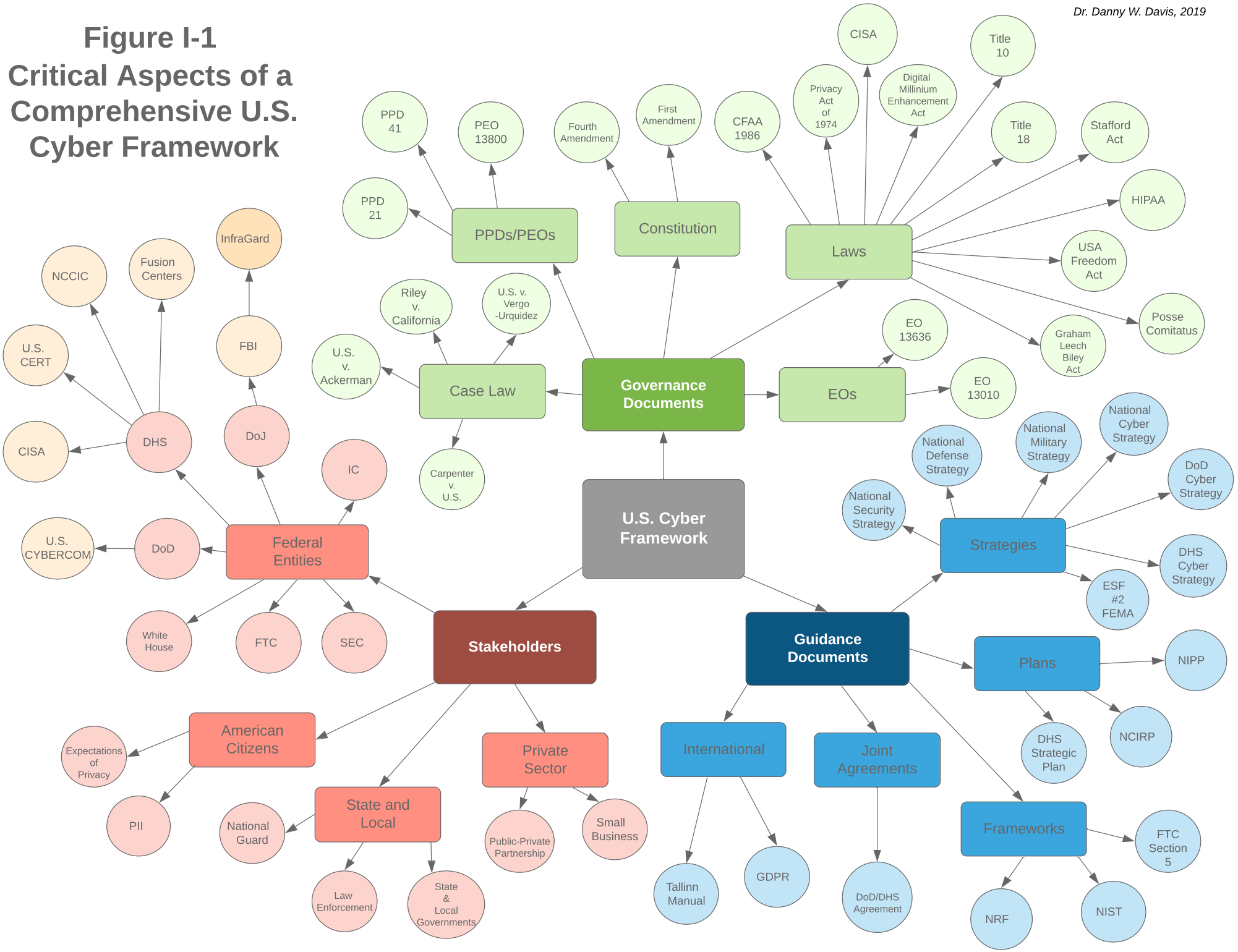
The final section provides the overarching recommendations for elements to be included in a comprehensive federal cyber framework, how the government and private industry can create a partnership to implement that framework, how the private industry can be included in that framework, and how that framework can allow DoD to operate within IP space to provide for national security while maintaining individual rights.

Annex A attached to this report applies the concepts and recommendations presented herein to a hypothetical cyberattack scenario, which the authors created. This scenario includes specifics of the attack, the effects of the attack on the community in which the attack occurs, and the response of state, local, and Federal Government authorities. The Annex will document the timeline of both the attack and the response, and will provide an overview of how and when the various guidance and governance documents are executed.

Figure I-1 presents a visual representation of the critical aspects of a comprehensive U.S. cyber framework. Included in the graphic are the relevant governance and guidance documents that address U.S. cybersecurity and cyber incident response. These include Federal laws, Constitutional amendments, Executive Branch directives, and agency-specific and interagency documents. Also included in the graphic are the stakeholders impacted by a U.S. cyber framework, spanning both the public and private sectors. All of these documents and stakeholders play a critical role in cybersecurity and cyberattack response, and therefore must be considered in any comprehensive Federal framework. This graphic was used as a strategic outline to guide and define the scope of the report to answer the research questions.

Figure I-1
Critical Aspects of a Comprehensive U.S. Cyber Framework

Dr. Danny W. Davis, 2019



References

1. Meese III, Edwin. 2011. "Who is responsible for America's security?" Heritage Foundation. https://www.heritage.org/the-constitution/report/who-responsible-americas-security
2. Talent, Jim. 2010. "A Constitutional Basis for Defense." The Heritage Foundation. https://www.heritage.org/defense/report/constitutional-basis-defense
3. Ucko, David. H., and Thomas A. Marks. 2018. "Violence in context: Mapping the strategies and operational art of irregular warfare." *Contemporary Security Policy* 39(2): 206-233.
4. Spezio, Anthony E. 2002. "Electronic warfare systems." *IEEE Transactions on Microwave Theory and Techniques 50*(3): 633-644.
5. Ahrari, Ehsan. 2010. "Transformation of America's military and asymmetric war." *Comparative Strategy 29*(3): 223-244.
6. Brzica, Nikola. 2018. "Understanding Contemporary Asymmetric Threats." *Croatian International Relations Review 24*(83): 34-51.
7. Yun, Minwoo. 2010. "Insurgency warfare as an emerging new mode of warfare and the new enemy." *The Korean Journal of Defense Analysi*, *22*(1): 111-125.
8. Long, David E. 2008. "Countering asymmetrical warfare in the 21st century: A grand strategic vision." *Strategic Insights 7*(3).
9. Chansoria, Monika. 2012. "Defying borders in future conflict in East Asia: Chinese capabilities in the realm of information warfare and cyber space." *The Journal of East Asian Affairs 26*(1): 105-127.
10. Liang, Qilian, Xiuzhen Cheng, and Sherwood W Samn,. 2010. "NEW: network-enabled electronic warfare for target recognition." *IEEE Transactions on Aerospace and Electronic Systems 46*(2): 558-568.
11. Carter, Donald P. 2016. "Clouds or clocks: The limitations of intelligence preparation of the battlefield in a complex world." *Military Review 96*(2): 36-41.
12. Chase, Eric C. 2009. "Intelligence preparation of the (asymmetric) battlefield." *Marine Corps Gazette, 93*(2), 20-23.
13. Rubin, David, Kim Lynch, Jason Escaravage, & Hillary Lerner. 2014. "Harnessing data for national security." *The SAIS Review of International Affairs* 34(1): 121-128.
14. Bendix, William, and Paul J. Quirk. 2016. "Introduction: Governing the security state." *Journal of Policy History* 28(3): 399-405.
15. Kleinrock, Leonard. 2008. "History of the Internet and its flexible future." *IEEE Wireless Communications* 15(1): 8-18.

16. Featherly, Kevin. 2016. “ARPANET.” Encyclopædia Britannica, https://www.britannica.com/topic/ARPANET (March 28, 2019).

17. Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimutha Palaniswami. 2013. “Internet of Things (IoT): A vision, architectural elements, and future directions.” *Future Generation Computer Systems* 29(7): 1645-1660.

18. Campbell-Kelly, Martin, and Daniel D. Garcia-Swartz. 2013. “The history of the internet: the missing narratives.” *Journal of Information Technology* 28(1): 18-33.

19. Mincu, Constantin. 2016. “Cyber Attacks, Major Threats and Vulnerabilities against States, Organizations and Citizens.” Annals: Series on Military Sciences 8(1): 3-15.

20. Joint Chiefs of Staff. 2018. “Joint Publication 3-12: Cyberspace Operations.” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

21. Nielsen, Suzanne C. 2012. Pursuing security in cyberspace: Strategic and organizational challenges. Orbis, 56(3), 336.

22. Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimutha Palaniswami. 2013. “Internet of Things (IoT): A vision, architectural elements, and future directions.” *Future Generation Computer Systems* 29(7): 1645-1660.

23. Weiss, Aaron. 2007. “Computing in the clouds.” *Networker 11*(4):16-25.

24. Buyya, Rajkumar, Yeo, Chee Shin, Venugopal, Srikumar, Broberg, James and Brandic, Ivona. 2009. “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility.” *Future Generation computer systems 25*(6): 599-616.

25. Miorandi, Daniele, Sabrina Sicari, Francsco De Pellegrini, and Imrich Chlamtac. 2012. “Internet of things: Vision, applications and research challenges.” *Ad Hoc Networks* 10(7): 1497-1516.

26. Borgia, Eleonora. 2014. “The Internet of Things vision: Key features, applications and open issues.” *Computer Communications* 54: 1-31.

27. Banafa, Ahmed. 2015. “Internet of Things (IoT): More than Smart ‘Things.’” Datafloq. https://datafloq.com/read/internet-of-things-more-than-smart-things/1060 (March 27, 2019)

28. Li, Zhen, and Qi Liao. 2018. “Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets.” *Government Information Quarterly* 35(1), 151-160.

29. Ju, Jingrui, Luning Liu, and Yuqiang Feng. 2018. “Citizen-centered big data analysis-driven governance intelligence framework for smart cities.” *Telecommunications Policy* 42(10): 881.

30. Liu, Yu-Li, Yuntsai Chou, and Chih-Liang Yeh. 2018. “Big data, the internet of things, and the interconnected society.” *Telecommunications Policy* 42(4): 277.

31. Botta, Alessio, De Donato, Walter, Persico, Valerio and Pescapé, Antonio. 2016. "Integration of cloud computing and internet of things: a survey." *Future generation computer systems 56*: 684-700.

32. Williams, Peter 2019. "Does competency-based education with blockchain signal a new mission for universities?" *Journal of Higher Education Policy and Management* 41(1): 104-117.

33. Giles, Martin. 2019. "Explainer: What is a quantum computer?" MIT Technology Review. https://www.technologyreview.com/s/612844/what-is-quantum-computing/ (March 27, 2019)

34. Bishwas, Arit K., Mani, Ashish, and Palade, Vaslie. 2018. "An all-pair quantum SVM approach for big data multiclass classification." *Quantum Information Processing 17*(10): 282.

35. Wirtz, Bernd W., and Jan C. Weyerer. 2017. "Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats." *International Journal of Public Administration* 40(13): 1085-1100.

36. Rid, Thomas, and Ben Buchanan. 2018. "Hacking democracy." *The SAIS Review of International Affairs* 38(1): 3.

37. Rudner, Martin. 2013. "Cyber-threats to Critical National Infrastructure: An Intelligence Challenge." *International Journal of Intelligence and CounterIntelligence* 26(3): 453-481.

38. Kenney, Michael. 2015. "Cyber-terrorism in a post-Stuxnet world." *Orbis* 59(1): 111-128.

39. Maimon, David, and Eric R. Louderback. 2018. "Cyber-Dependent Crimes: An Interdisciplinary Review." *Annual Review of Criminology* 2:191-216.

40. Tehrani, P Pardis Moslemzadeh, Nazura Abdul Manap, Hossein Taj. 2013. "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime." *Computer Law & Security Review* 29(3): 207-215.

41. Tafoya, William L. 2011. "Cyber Terror." Federal Bureau of Investigation Law Enforcement Bulletin https://leb.fbi.gov/articles/featured-articles/cyber-terror (March 27, 2019)

42. Osawa, Jun. 2017. "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?" *Asia-Pacific Review* 24(2): 113-131.

43. Flournoy, Michèle and Michael Sulmeyer. 2018. "Battlefield internet: A plan for securing cyberspace." *Foreign Affairs* 97(5) 40-46.

44. Hughes, Rex. 2010. "A treaty for cyberspace." *International Affairs (London) 86*(2): 523-541.

45. Payne, Christian and Finlay, Lorraine. 2017. “Addressing obstacles to cyber-attribution: a model based on state response to cyber-attack.” *The George Washington International Law Review 49*(3): 535-568.

46. Shah, Shabaz H. and Verma, Sudheer S. 2018. “The US and Russia: Politics of spheres of influence in the 21st century.” *IUP Journal of International Relations 12*(4): 7-20.

47. Softness, Nicole. 2017. “How should the U.S. respond to a Russian cyber attack?” *Yale Journal of International Affairs 12*(1): 99.

48. Johnson, James S. 2018. China's vision of the future network-centric battlefield: Cyber, space and electromagnetic asymmetric challenges to the United States. *Comparative Strategy, 37*(5), 373-390.

49. Thomas, Timothy L. 2008. “China's electronic long-range reconnaissance.” *Military Review 88*(6): 47-54.

50. Reimann, Jakob. 2019. *China is flooding the Middle East with cheap drones.* Washington: Inter-Hemispheric Resource Center Press. (pg number)

51. Stent, Dylan. 2018. “The great cyber game.” *New Zealand International Review 43*(5): 6.

52. Boo, Hyeong-wook. 2017. “An assessment of North Korean cyber threats.” *The Journal of East Asian Affairs 31*(1): 97-117.

53. Lewis, James A. 2014. *Cybersecurity and stability in the Gulf*. Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-and-stability-gulf

54. Netolická, Veronika and Mares, Miroslav. 2018. “Arms race "in cyberspace" - A case study of Iran and Israel.” *Comparative Strategy 37*(5): 414-429.

55. National Institute of Standards and Technology. 2019. “Glossary: attack.” NIST Computer Science Resource Center, https://csrc.nist.gov/glossary/term/attack (March 28, 2019)

56. National Institute of Standards and Technology. 2019. “Glossary: computer network attack.” NIST Computer Science Resource Center, https://csrc.nist.gov/glossary/term/attack (March 28, 2019)

57. National Institute of Standards and Technology. 2019. “Glossary: computer network exploitation.” NIST Computer Science Resource Center, https://csrc.nist.gov/glossary/term/attack (March 28, 2019)

58. Lin, Herbert. 2012. “A virtual necessity: Some modest steps toward greater cybersecurity.” *Bulletin of the Atomic Scientists 68*(5): 75-87.

59. Government Accountability Office. 2005. *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*. https://www.gao.gov/new.items/d05434.pdf

60. Federal Bureau of Investigation. 2019. “About IC3.” Federal Bureau of Investigation Internet Crime Complaint Center (IC3) https://www.ic3.gov/about/default.aspx (March 27, 2019)

61. Federal Bureau of Investigation. 2017. “2016 Crime Report.” Federal Bureau of Investigation https://www.fbi.gov/news/stories/ic3-releases-2016-internet-crime-report (March 27, 2019)

62. Symantec. 2019. “Internet Security Threat Report: Executive Summary.” https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf (March 27, 2019)

63. Srinivas, Jangirala., Ashok Kumar Das, and Neeraj Kumar. 2019. “Government regulations in cyber security: Framework, standards and recommendations.” *Future Generation Computer Systems* 92: 178-188

64. Burns A.J., M. Eric Johnson, and Deanna D. Caputo. 2019. “Spear phishing in a barrel: Insights from a targeted phishing campaign.” *Journal of Organizational Computing and Electronic Commerce* 29(1): 24-39.

65. Alexander, Dean. 2012. “Cyber Threats in the 21st Century.” *Security* 49(9): 70-76.

66. Ammori, Marvin, and Keira Poellet. 2010. “Security versus Freedom" on the Internet: Cybersecurity and Net Neutrality.” *SAIS Review of International Affairs* 30(2): 51-65.

67. Wang, Zheng. 2019. “An elastic and resiliency defense against DDoS attacks on the critical DNS authoritative infrastructure.” *Journal of Computer and System Sciences* 99: 1-26.

68. Ahmed, Muhammad Ejaz, Saeed Ullah, and Hyoungshick Kim. 2019. “Statistical Application Fingerprinting for DdoS Attack Mitigation.” *IEEE Transactions on Information Forensics and Security* 14(6): 1471-1484.

69. Kaur, Ratinder, and Maninder Singh. 2014. “A survey on zero-day polymorphic worm detection techniques.” *IEEE Communications Surveys & Tutorials* 16(3): 1520-1549.

70. Wang, Lingyu., Sushil Jajodia, Anoop Singhal, Pengsu Cheng, and Steven Noel. 2014. “k-Zero Day Safety: A Network Security Metric For Measuring The Risk Of Unknown Vulnerabilities.” *IEEE Transactions on Dependable and Secure Computing* 11(1): 30-44.

71. Wang, Lanjia., Zhichun Li, Zhi Fu, and Xing Lu. 2010. “Thwarting zero-day polymorphic worms with network-level length-based signature generation.” *IEEE/ACM Transactions on Networking (TON)* 18(1): 53-66.

72. Lord, Nate. 2018. “What is an Advanced Persistent Threat? APT Definition.” Digital Guardian, https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition (March 27, 2019)

73. DeVore, Marc R., and Sangho Lee. 2017. "APT(Advanced Persistent Threat)S and influence: cyber weapons and the changing calculus of conflict." *The Journal of East Asian Affairs* 31(1): 39-64.

74. Fire Eye. 2019. "Advanced Persistent Threat Groups." Fire Eye https://www.fireeye.com/current-threats/apt-groups.html (March 28, 2019).

75. Lindsay, Jon R. 2015. "The impact of China on cybersecurity: Fiction and friction." *International Security* 39(3): 7-47.

76. Hoffman, David E. 2011. "The New Virology." *Foreign Policy* 185: 77-80

77. Goodman, Seymour E, Jessica C. Kirk, and Megan H. Kirk. 2007. "Cyberspace as a medium for terrorists." *Technological Forecasting and Social Change* 74(2): 193-210.

78. Kriner, Douglas, and Schickler, Eric. 2018. "The Resilience of Separation of Powers? Congress and the Russia Investigation." *Presidential Studies Quarterly 48*(3): 436-455.

79. Kornbluh, Karen. 2018. "The internet's lost promise: And how america can restore it." *Foreign Affairs 97*: 33-38.

80. Chertoff, Michael and Rasmussen, Anders F. 2019. "The unhackable election: What it takes to defend democracy." *Foreign Affairs 98*: 156.

81. Jensen, Benjamin. 2018. "The Cyber Character of Political Warfare." *The Brown Journal of World Affairs* 24: 159-171.

82. Libicki, Martin C. 2012. "Crisis and escalation in cyberspace." The RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf

83. Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988. Pub. L. No. 100-707; amending Pub. L. No. 93-288. Codified at 42 U.S.C. §§ 5121-5207.

84. Lindsay, Bruce R. 2017. "*Stafford Act Assistance and Acts of Terrorism*." Congressional Research Service. https://fas.org/sgp/crs/homesec/R44801.pdf

85. Brown, Jared T, and Bruce R. Lindsay. 2018. "*Congressional Primer on Responding to Major Disasters and Emergencies."* Congressional Research Service. https://fas.org/sgp/crs/homesec/R41981.pdf

86. Carter, David L. 2009. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies.* Department of Justice: Office of Community Oriented Policing Services. https://fas.org/irp/agency/doj/lei.pdf (March 19th, 2019).

87. City of Arlington, Texas, et al. v. Federal Communications Commission et al. 2013. 569 U.S. 290.

88. Cooper, Roy. 2014. *Mutual Aid Agreements Between Law Enforcement Agencies in North Carolina.* North Carolina Department of Justice. https://ncsheriffs.org/wp-content/uploads/2015/01/Mutual_Aid_Agreements-Oct2014.pdf (March 19th, 2019).

89. Department of Homeland Security. 2019. “Cyber and Infrastructure Security Agency.” https://www.dhs.gov/CISA (March 19th, 2019).

90. Wortzel, Larry. 2003. “Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security.” The Heritage Foundation. https://www.heritage.org/homeland-security/report/securing-americas-critical-infrastructures-top-priority-the-department (March 19th, 2019).

91. Department of Homeland Security. 2013. *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*. https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (March 19th, 2019).

92. Chen, Thomas M. 2014. “Cyberterrorism after Stuxnet.” Strategic Studies Institute. https://ssi.armywarcollege.edu/pdffiles/PUB1211.pdf

93. Federal Emergency Management Agency. 2011. *Strategic Foresight Initiative*. https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf

94. Simon, David. 2017. “Raising the Consequences of Hacking American Companies.” The Center for Strategic & International Studies. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/171012_Simon_RaisingConsequencesOfHacking_Web.pdf (March 19th, 2019).

95. O’Connor, Nuala. 2018. “Reforming the U.S. Approach to Data Protection and Privacy.” Council on Foreign Relations. https://www.cfr.org/report/reforming-us-approach-data-protection (March 19th, 2019).

96. Wheeler, Tarah. 2018 “In Cyberwar, There are No Rules.” Foreignpolicy.com. https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ (March 19th, 2019).

97. Fischer, Eric A., Liu, Edward C., Rollins, John W. & Theohary, Catherine A. 2014. “The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress.” Congressional Research Service. https://fas.org/sgp/crs/misc/R42984.pdf (March 19th, 2019).

Chapter 1

Cyberattacks and Critical Infrastructure

Understanding the measures necessary to protect the United States (U.S.) and its critical infrastructure from cyberattacks first requires determining how the nation's critical infrastructure is defined. The definition of critical infrastructure has been formed over time by presidential decree. President Clinton's Executive Order (EO) 13010 established the President's Commission on Critical Infrastructure Protection and included language that specified how infrastructure is identified as "critical:" "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[1] The "certain national infrastructures" considered as vital included electrical power systems, communication services, finance, transportation, emergency services, water supply systems, and continuity of government.[2] It is important to note here that while the sectors of critical infrastructure now fall under the Department of Homeland Security (DHS), at the time this EO was established DHS did not exist. The current placement of critical infrastructure under DHS authority, established through the Homeland Security Act of 2002, shows an important evolution in the structure of homeland security within the U.S.

In 2013 President Obama issued an EO on Improving Critical Infrastructure Cybersecurity, EO 13636, to address threats posed by cyberattacks that could disrupt the nation's power, water, communication, or other critical systems. EO 13636 further defines critical infrastructure as the "systems and assets, whether physical of virtual, so vital to the United States that the incapacity or destruction of [such] would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3,4]

Section 4 of EO 13636 requires the Attorney General, the Secretary of Homeland Security, and the Director of Office of the Director of National Intelligence (ODNI) to produce unclassified reports of current cyber threats. Under this section, the Department of Justice (DOJ), DHS, and ODNI are given their first role in merging cyber threats with the vulnerabilities of critical infrastructure. Section 4, subsection c, requires coordination between DHS and the Department of Defense (DoD) by mandating that together they "establish procedures to expand the Enhanced Cybersecurity program to all critical infrastructure sectors."[4] The Enhanced Cybersecurity program was one of the first to establish a working partnership between the public and private sectors regarding classified cyber matters. This was important to create due to the close contracting between public and private and the need-to-know of vulnerabilities. Additionally,

this EO provided direction for cybersecurity considerations that culminated in the creation of the National Institute for Standards and Technology (NIST) framework that establishes best practices for cybersecurity that public and private entities are encouraged to follow.

"Critical infrastructures" as defined under both EO 13010 and 13636 encompass a wide range of organizations and structures that are vital for the uninterrupted operation of American society. Additionally, each individual element of these organizations and structures must be maintained, protected, and managed in order to function properly. Presidential Policy Directive 21 (PPD-21), entitled Critical Infrastructure Security and Resilience and implemented in 2013 in conjunction with EO 13636, established sixteen distinct sectors of critical infrastructure.[5] PPD-21 assigned a Sector-Specific Agency (SSA) to each sector of critical infrastructure, and each SSA is individually responsible for a portion of the financial, industrial, security, public health, communication, technological, and other critical functions of our nation. These SSAs include the DHS, the DoD, the Department of Energy (DOE), the Department of the Treasury (USDT), the U.S. Department of Agriculture (USDA), the Department of Health and Human Services (HHS), the General Services Administration (GSA), the Department of Transportation (DOT), and the Environmental Protection Agency (EPA). While the head of each SSA is responsible for developing and maintaining cyber defense strategies and plans specific to their sector, DHS coordinates efforts between all sectors and directs the Federal Government's overall protection and security of all critical infrastructure.[6] **Figure 1-1** shows each the critical infrastructure sectors, provides a description of each sector, and indicates the designated SSA for each sector.

Figure 1-1 Critical Infrastructure Sectors[7]

Various laws and legislation have been developed to assist in the protection of critical infrastructure from the cyber threats of the modern world. In May 2017, Presidential Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (PEO 13800) was created to implement "The Framework for Improving Critical Infrastructure Cybersecurity" produced by NIST, while also modernizing the cyber defense plans formed under the mandate included in PPD-21.[8] PPD-41, issued in 2016, focused on the cybersecurity elements contained within the nation's National Preparedness Goals by creating principles that guide the Federal Government's response to any cyberattack involving government or private sector critical infrastructure entities. These principles dictate that in response to any cyberattack,

Federal agencies shall undertake three simultaneous lines of effort: Threat response, asset response, and intelligence support and related activities. Achieving all three of these lines of effort is meant to facilitate more adequate protection against cyberattacks.[8]

On November 16, 2018, President Trump signed the Cybersecurity and Infrastructure Security Agency Act of 2018 into law. This act elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS through the establishment of the Cybersecurity and Infrastructure Security Agency (CISA). CISA was created to "defend critical infrastructure against the threats of *today*, while working with partners across all levels of government and in the private sector to secure against the evolving risks of *tomorrow*."[9] CISA has been officially tasked with protecting the nation's critical infrastructure from both physical attacks and cyberattacks, which will require the effective coordination and collaboration of various government and private sector organizations.[9]

Cyberattacks and Critical Infrastructure

Although the majority of the nation's critical infrastructure and resources are owned by the private sector, the government has a vested interest in addressing any potential vulnerabilities that such infrastructure and resources have to an attack, particularly when government entities are involved.[10] Addressing potential vulnerabilities becomes increasingly difficult and complex when considering that these infrastructures and resources are susceptible to not only physical attacks, but also to constantly evolving cyber threats. The following are examples of how real cyberattacks have exposed inadequate protective measures for some of the largest infrastructure sectors in the U.S.

Stuxnet

One of the most prolific and malicious cyberattack methods is the Stuxnet computer worm, first publicly deployed in 2010. Stuxnet was developed to sabotage the Iranian nuclear program by targeting Programmable Logic Controllers (PLCs) and other machines within nuclear facilities that were using Microsoft Windows software.[11,12] The attack physically damaged the nuclear reactors, demonstrating that a cyberattack could be used as a war tactic that can cause physical damage and exposed new vulnerabilities for critical infrastructure.[13,14] The implications of

Stuxnet go beyond the potential for use as a weapon of war. When it was used against the Iranian nuclear reactors, the worm targeted the supervisory control and data acquisition (SCADA) systems of the reactors, as well as other systems that were used to directly control reactor operations. SCADA systems have been used for years across multiple sectors of critical infrastructure, including oil and gas refineries as well as electrical grids.[15,16] The proliferation of SCADA systems throughout critical infrastructure networks and their susceptibility to the Stuxnet attack expose a substantial vulnerability that must be addressed. Although it is not certain who developed Stuxnet, many believed that the U.S. and Israel worked together to develop the worm.[17,18]

Rye, NY Attack

A smaller but no less concerning cyberattack occurred in the New York City suburb of Rye. A hacker gained access to the control system of the Bowman Avenue Dam in 2013, though the hack was not discovered until two years later in 2015. Responsibility for the hack was eventually claimed by SOBH Cyber Jihad, an Iranian hacktivist group; the group claimed they maintained their silence about the hack for two years in accordance with a "state-level" warning not to go public about the hack.[19] However, the attack and the group's responsibility were never acknowledged by the Iranian government.[20]

Although the Bowman Avenue Dam itself is a relatively smaller dam and the attack did not affect many people at that time, the reality that the hack was able to occur revealed wider implications for vulnerabilities in a massive sector of critical infrastructure, including the fact that the hack was not discovered until two years after it occurred. Senator Charles Schumer of New York said that the revelation of the attack "should be a wakeup call that the nation's critical infrastructure is too vulnerable to 'evil-doers' toiling away at keyboards."[20] Under normal conditions, the hackers should have been able to use the remote access to release water from behind the dam; however, the dam was undergoing maintenance at that time and the sluice gate was manually disconnected, preventing electronic control.[21] This event is specifically considered a hack as it was only intended as an undetected intrusion, but was not intended to physically damage the structure.[22]

Ukrainian Power Grid Attack

On December 23, 2015 an electric company in western Ukraine reported power outages due to illegal activity detected within the company's SCADA systems perpetrated by a then-unknown actor.[23] In a report released by DHS, attribution for the attack was not officially determined; however, per information obtained from DHS's Industrial Control Systems Cyber Emergency Response Team and the U.S. cyber intelligence firm iSight, the attack was linked back to "Sandworm," a known Russian hacking group.[24,25,23]

In total, three Ukrainian electrical distribution groups experienced coordinated cyberattacks that occurred within thirty minutes of each other. Initially, it was estimated that 80,000 customers were affected, but detailed reports of the incident later indicated that the total number of affected customers was closer to 225,000.[25,23] The power outages lasted for several hours, but were eventually restored.

This attack is significant in that it was the first publically-acknowledged cyberattack that resulted in power outages due to a targeted attack on SCADA systems within a nation's critical infrastructure.[25,26]. Additionally, it brought to light the importance of understanding the ability of foreign adversaries to attack power grids and potentially damage a nation's critical infrastructure. The threat of a power outage on the scale of the Ukraine attack goes beyond its effect on large-scale critical infrastructure. Such an attack would also have significant effects on everyday life, as the loss of electronic devices, appliances, and systems such as powering refrigerators, ovens, cell phone and mobile computer charging, and access to electronic medical records can cause harm to individuals and pose a threat to national security.[26]

Atlanta Ransomware Attack

A January 2018 audit of the City of Atlanta's information technology (IT) infrastructure identified between 1,500 and 2,000 vulnerabilities, confirming previous criticisms that the city had not been spending enough to adequately upgrade the city's internal systems.[27] Two months later, on March 22, a massive SamSam ransomware attack struck the city's internal systems, locking files and demanding a ransom of approximately $50,000 in bitcoin.[28,29] The SamSam ransomware is unique from other forms of ransomware in that it does not rely on phishing to

achieve its goal; instead, it uses a "brute-force attack" to guess individual passwords until a match is found.[30,31] Since Atlanta is a hub for transportation, health, and economics, the incident received attention nationwide and brought to light cyber vulnerabilities within one of the largest cities in the nation, with real-time and lasting effects.

As the SamSam attack spread throughout the city's IT infrastructure, it affected many of the city's programs and services, including parking, utility, and court services.[31,29] Additionally, many legal documents and years of police dash-cam videos were permanently deleted. City employees were not able to return to their computers for another five days and many systems have still not recovered.[28]

On November 26, 2018 a U.S. grand jury indicted two Iranian hackers for the attack who the DOJ alleged are part of the SamSam group.[32] The group, based in Iran but with no known affiliation with the Iranian government, is known for choosing targets that are most likely to consent to ransom demands as well as finding and locking up the victims' most valuable information.[30,32] The attack is currently the largest successful breach of security for a major American city by ransomware and affected up to 6 million people. The SamSam attack has prompted many cities across the nation to examine the security of their infrastructure systems and evaluate the availability of resources to address a cyber incident of similar severity were it to happen to them.[29,27]

These examples demonstrate the current existence of vulnerabilities in critical infrastructure networks, and how a directed cyberattack against even one of these vulnerable networks can bring the operations of an entire city to a standstill, or physically damage structures. Had any of these attacks escalated further, it could have ultimately led to loss of life, potentially even as significant as nuclear meltdown or dam failure. **Table 1-1** lists additional cyberattacks that have occurred across the world. The Stuxnet attack and the attack on the Ukrainian power grid are included in this table, while the Rye, NY and Atlanta Ransomware attacks are not. Recognizing the continued proliferation of cyberattacks is vital to understanding the implications of future attacks and the need for adequate cybersecurity measures to address potential attacks on U.S. critical infrastructure. A clear understanding of the frameworks and roles of cyber response and preparedness currently in place is vital to successful prevention and mitigation in the event of a

cyberattack. As such, the development of a universal response framework will provide both government and private sector entities the ability to adequately respond to such attacks. This framework could generate more productive response measures and hopefully decrease the amount and severity of damage, especially when critical infrastructure is targeted.

Table 1-1 Notable Cyberattacks

Incident	Country of incident	Year incident began	Impact	Attribution in the Public Domain
Lawrence Berkeley National Laboratory	United States	1986	Intrusion and sensitive data exfiltration	Criminal trial in West Germany, 1990
Titan Rain	United States	2003	Exfiltration of sensitive data from organizations including NASA, Lockheed Martin, Sandia National Laboratories, and the FBI, as well as U.S. and British defense departments	Widely attributed to China by government and private sources in news outlets in 2005; dissent by Chinese state
Estonian DDoS	Estonia	2007	Large-scale DDoS attack of Estonian websites in the context of tensions with Russia	Accusations by Estonian government to Russian state actors; Russia blamed attack on pro-Kremlin youth movement—not state-sponsored actors
Stuxnet Worm	Iran	2010	Physical damage to Iranian centrifuges; worldwide computer infection	Widely attributed to the United States and Israel; leaks by U.S. officials
DDoS attacks on U.S. banks	United States	2012	DDoS attacks on more than 46 major U.S. financial institutions	Widespread perception of Iranian state sponsorship; initial U.S. government leaks and eventual indictment of Iranian state actors in March 2016

Adapted From: Davis, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. 2017. Stateless Attribution: Toward International Accountability in Cyberspace. Rand Corporation. https://www.rand.org/pubs/research_reports/RR2081.html

Table 1-1 Notable Cyberattacks

Incident	Country of incident	Year incident began	Impact	Attribution in the Public Domain
Saudi Aramco	Saudi Arabia	2012 and 2016	Wiped or destroyed 35,000 Saudi Aramco computers; similar attack in late 2016	In 2012, U.S. officials link attack to Iran in news media
Associated Press Twitter account	United States	2013	Compromised Associated Press Twitter account and tweeted false news of an attack on the White House, leading to sharp stock market declines	Attack claimed by Syrian Electronic Army
White House and State Department	United States	2014	Significant intrusion in unclassified computer systems	Widely attributed to Russia but no official attribution by U.S. government
Sony Pictures	United States	2014	Sensitive data stolen and leaked; significant business disruption	Attributed to North Korean state actors by U.S. President in December 2014 and to Lazarus by Operation Blockbuster in 2016
GitHub	United States	2015	Large and persistent DDoS attack on software development collaboration site	Widely attributed to Chinese state actors by private firms and researchers
TV5Monde	France	2015	18-hour TV network outage; false flag leads to false attribution to ISIS	FireEye attributed to Russian hacking group APT28 in June 2015

Adapted From: Davis, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. 2017. Stateless Attribution: Toward International Accountability in Cyberspace. Rand Corporation. https://www.rand.org/pubs/research_reports/RR2081.html

Table 1-1 Notable Cyberattacks

Incident	Country of incident	Year incident began	Impact	Attribution in the Public Domain
OPM	United States	2015	Exfiltration of 21.5 million personnel records of U.S. government employees	Widely attributed to China although never officially attributed by U.S. government
German Parliament	Germany	2015	Exfiltration and release of 2,420 sensitive files belonging to German Christian Democratic Union	BfV attribution to APT28 in news outlets in May 2016
Ukraine power grid	Ukraine	2016	Loss of power for several hours across regional power distribution plants, affecting 225,000 customers	Ukrainian officials accused Russia; private firms suggest possible state actors and/or cyber criminals
Democratic National Committee (DNC)	United States	2016	Exfiltration and release of DNC and campaign documents; interference with 2016 U.S. presidential election	CrowdStrike (June 2016) and DNI report (January 2017) attributed to Russian state actors
Bangladesh Central Bank	Bangladesh	2016	Successful bank heist of $81 million from Bangladesh Central Bank account at the Federal Reserve Bank of New York using Society for Worldwide Interbank Financial Telecommunication (SWIFT) banking system	Symantec report links to Lazarus May 2016; U.S. intelligence agencies report link to North Korea state news outlets in March 2017

Adapted From: Davis, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. 2017. Stateless Attribution: Toward International Accountability in Cyberspace. Rand Corporation. https://www.rand.org/pubs/research_reports/RR2081.html

Table 1-1 Notable Cyberattacks

Incident	Country of incident	Year incident began	Impact	Attribution in the Public Domain
Mossack Fonseca	Panama	2016	11.5 million leaked documents representing more than 214,488 “offshore entities," leading to numerous tax evasion and corruption charges	No attribution to date; possible hacktivists and/or insiders
Dyn	United States	2016	DDoS attack using a botnet of Internet of Things devices against Dyn, a domain name system (DNS) provider, disabling a significant number of websites	No official attribution; widely believed to be a hacktivist organization such as Anonymous, New World Hackers, or SpainSquad
WannaCry	Worldwide	2017	Ransomware attack affecting health care, transportation, and telecommunications infrastructure worldwide	No official attribution; some private firms suggest links to Lazarus Group; Russia blamed the United States for creating exploit that enables WannaCry

Adapted From: Davis, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. 2017. Stateless Attribution: Toward International Accountability in Cyberspace. Rand Corporation. https://www.rand.org/pubs/research_reports/RR2081.html

Government Agencies and Responsibilities for Cybersecurity

Per **Figure I-1** in the Introduction, there are many guiding agencies, policies, and coordination agreements that must be considered regarding critical infrastructure and cyberattack response mechanisms. While they all play an important role in coordinating a response, each is guided by different authorities. Due to critical infrastructure falling under the umbrella of DHS, but touching multiple other industries and agencies such as DoD and DOJ as well as the individual SSAs, response planning mechanisms are not easy to establish. Throughout this section, a variety of the most important response and authorization documents are analyzed. These documents include the National Cyber Incident Response Plan (NCIRP), the National Infrastructure Protection Plan (NIPP), the DHS Cybersecurity Strategy, the National Response Framework (NRF), CISA, the DoD Cyber Strategy (DoD CS), InfraGard, EO 13010, EO 13636, PPD-21, PPD-41, PEO 13800, the DoD-DHS Cyber Coordination Agreement, the National Cyber Strategy (NCS), and the National Security Strategy (NSS). These documents will be used to identify any overlaps and evaluate any vulnerabilities in the current state of cyberattack response mechanisms for critical infrastructure entities. Though the following sections are categorized by the major agencies involved (DHS, DoD, and DOJ), there are overlaps within these sections as some documents under a certain agency have equal or interconnected responsibilities within a different agency.

Department of Homeland Security (DHS)

The official mission of DHS is to "prevent terrorism and enhance security, manage borders administer immigration laws, secure cyberspace, and ensure disaster resilience."[33] Specific authority is granted to DHS to achieve this mission through PPDs issued by the President and conducted through the strategies and plans produced by the separate departments within DHS. This section will focus on the portion of the mission that "secures cyberspace," particularly as it relates to critical infrastructure, within the documents indicated by the black squares in **Table 1-2**.

Table 1-2 DHS Cyber Response Guidance Documents

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
DHS															

Cybersecurity and Infrastructure Security Agency (CISA)

CISA, as discussed previously, is housed under DHS. It is structured into four divisions: Cybersecurity; Infrastructure Security; Emergency Communications; and the National Risk Management Center (NRMC). Each of these divisions is tasked with different priorities, some of which are meant to mitigate and some to adapt. The main goal of the Cybersecurity Division (CD) is to assist in safeguarding the ".gov" network that facilitates the day to day function of the government network. The Infrastructure Security Division (ISD) coordinates security and resilience efforts through public-private partnerships and delivers technical assistance if called upon. The Emergency Communications Division (ECD) is responsible for ensuring the function of interoperable communications across all facets of government. Finally, the NRMC works with all entities involved in securing critical infrastructure by "identify[ing], analyz[ing], prioritiz[ing], and manag[ing]" the most strategic risks to critical functions of the nation.[34]

DHS Cybersecurity Strategy

The DHS Cybersecurity Strategy (DHS CS), released in November of 2018 under the Trump Administration, directly discusses critical infrastructure under Pillar 2, Goal 3: Protect Critical Infrastructure. As previously discussed, critical infrastructure is vital to the overall function of the nation as it controls national security, public health and safety, and economic security, and an attack against any sector could therefore endanger public safety and potentially lead to loss of life. Pillar 2, Goal 3 outlines three primary objectives for cybersecurity of critical infrastructure, with each objective requiring the engagement of a variety of both government and nongovernmental actors.[35] These objectives are:

- Objective 3.1: Maturing cyber security offerings and engagements to address national risks to critical infrastructure

- Objective 3.2: Expand and improve sharing of cyber threat indicators, defensive measures, and other cybersecurity information
- Objective 3.3: Improve cybersecurity capabilities and resources available to sector-specific agencies, regulators, and policymakers

Despite the inclusion of the Defense Industrial Base (DIB), which is controlled by DoD, the DHS CS does not mention any roles for agencies that are not DHS. The only instance in which another agency is specifically mentioned by name is through a footnote on page 8, which provides a caveat that DHS leads the effort in Federal cyber hygiene with the exception of national security systems and some DoD and intelligence community systems. It does not, however, explicitly specify what comprises national security or DoD and intelligence community (IC) systems.

National Response Framework (NRF)

The process by which disaster response is conducted in the U.S., as stipulated in the Stafford Act (see discussion in the Introduction), is outlined in the National Response Framework (NRF). This framework, issued by DHS in 2013 under the Obama Administration, describes the roles, responsibilities, and structures "of a threat or hazard, in anticipation of a significant event, or in response to an incident."[36] The NRF outlines a tiered structure that facilitates a "bottom-up" approach for disaster response,[37] emphasizing that the NRF can be partially or fully implemented for a scaled incident response. Implementation of the NRF will vary depending on the size, severity, and scope of the incident. Cybersecurity is explicitly identified as a response core-capability of the NRF, based on the results of the Strategic National Risk Assessment (SNRA), as threats and hazards related to "malicious cyber activity can have catastrophic consequences."[36]

Under the NRF, the Secretary of Homeland Security is designated as the principal incident manager for domestic incidents and is tasked with providing an overall architecture for domestic incident management and coordination of Federal emergency response. The Federal emergency response requiring coordination with other Federal agencies to create a unified response to domestic incidents. The heads of other Federal agencies are tasked with other responsibilities;

specifically, the Assistant Secretary for Cybersecurity and Communications coordinates the response of significant cyberattacks. Additionally, under the NRF it is the responsibility of DHS to re-establish critical communications and coordinate communications support within response efforts.[36] This task is #2 within the 15 NRF Emergency Support Functions.

National Cyber Incident Response Plan (NCIRP)

Building off the response structures and procedures outlined in the NRF, the National Cyber Incident Response Plan (NCIRP), authorized in 2016 by the Obama Administration, defines similar, comprehensive mitigation, response, and recovery procedures for cyberattacks.[38] The NCIRP was developed in accordance with the principles of PPD-41, articulating the "roles and responsibilities, capabilities, and coordinating structures" for response and recovery from cyber incidents affecting critical infrastructure.[38] Like the NRF, the NCIRP stresses that cyberattack response is a unified effort of all levels of government as well as the private sector and the general public. The NCIRP differs from the NRF in that the NCIRP does not represent an operational plan for cyberattack response. Instead, the NCIRP serves as a guiding document for the development of organization-specific operational plans, as implemented by government agencies or private sector entities.[38]

Cooperation between government and the private sector to develop and implement robust cybersecurity strategies is vital for the protection of critical infrastructure, due to the majority of critical infrastructure being owned by the private sector. The development of such strategies will be conducted in accordance with industry standards put forth by NIST, which focus on a risk-based framework to provide cybersecurity resilience of critical infrastructure.[39] This may require government intervention if private sector cybersecurity implementation is deemed inadequate.[40] Under the NCIRP, the Federal Government and the private sector work concurrently to provide threat and asset response capabilities.[38] In another departure from the NRF, the NCIRP does not designate DHS as the sole lead Federal agency (LFA) for response coordination between government and the private sector when there is a cyberattack primarily involving the private sector. Instead, the LFA will depend on the response activities being performed: DOJ serves as the LFA for coordinating threat response; DHS serves as the LFA for coordinating asset response; and ODNI serves as the lead in coordinating intelligence support.[38]

DHS does coordinates asset response through the National Cybersecurity and Communications Integration Center (NCCIC). The primary role of asset response is to support technical assistance to affected entities, mitigate vulnerabilities, and assess the risk of said vulnerabilities. Specifically, if a Federal Government system is affected by a cyberattack, a U.S. Computer Emergency Readiness Team (US-CERT), under the authority of DHS, must be notified within one hour of the attack being officially confirmed by the Computer Security Incident Response Team (CSIRT). Additionally, US-CERT plays a role in assisting local government with resources and capabilities to address and respond to the attack.

The National Infrastructure Protection Plan (NIPP)

The National Infrastructure Protection Plan (NIPP), created in 2013 under the Obama Administration, is another DHS guidance document that plays a major role in cybersecurity efforts, specifically regarding critical infrastructure. It is the principal document required for critical infrastructure preparedness and protection to ensure secure and resilient critical infrastructure networks. The NIPP accomplishes this through establishing a framework in which the public and private sectors cooperate to disseminate information, communicate, and prepare for attacks.

The NIPP includes the following ten key concepts:

- Provides an updated approach to critical infrastructure security and resilience;
- Recommends greater focus on integration of cyber and physical security efforts;
- Fosters closer alignment to national preparedness efforts;
- Increases focus on cross sector and jurisdictional coordination to achieve results;
- Recognizes integration of information-sharing as an essential component of the risk management framework;
- Recognizes the key role and knowledge of critical infrastructure owners and operators;
- Integrates efforts by all levels of government, private, and nonprofit sectors by providing an inclusive partnership framework and recognizing unique expertise and capabilities each participant brings to the national effort;

- Reflects today's integrated all-hazards environment;
- Remains grounded in business principles and existing policy;
- Drives action toward long-term improvement

Each concept is equally important as together they provide comprehensive guidance and direction for all levels of government and the private sector to synchronize their efforts in the event of an attack against critical infrastructure.[41]

Sector Specific Agencies

As previously mentioned, SSAs were assigned to each of the sixteen sectors of critical infrastructure through PPD-21 to ensure proper oversight and guidance through DHS. The roles and responsibilities of the SSAs in critical infrastructure protection are outlined throughout various documents and agency strategies, as indicated in **Table 1-3**.

Table 1-3 SSA Cyber Response Guidance Documents

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
SSA															

NCIRP

The NCIRP places specific responsibilities on each SSA, such as increased communication with privately owned critical infrastructure that fall under their specific control. NCIRP also states that the main role of each SSA is to coordinate the efforts of the Federal Government if an attack takes place within their specific sector of critical infrastructure.

NIPP

The NIPP stresses the need for coordination and communication between each SSA and the organizations, both federally- and privately-owned, that are included in their specific sector. The methods by which this coordination should occur is not specifically outlined in the NIPP;

instead, each SSA and their respective administrations are responsible for developing these methods.

DHS Cybersecurity Strategy

The DHS CS explains that SSAs have an important role in the coordination and oversight of each sector of critical infrastructure. It also puts a great emphasis on the relationship between SSAs and other agencies.

DoD Cyber Strategy

The DoD CS makes only one mention of SSAs, when describing the roles of the Defense Critical Infrastructure (DCI) and the DIB within DoD. The SSAs play a small role in helping protect DoD critical infrastructure, as it is primarily protected by DoD itself.

EO 13010

EO 13010 created the President's Commission on Critical Infrastructure Protection and placed two members of each SSA on the Commission.

EO 13636

EO 13636 fails to provide guidance for the SSAs regarding cyber protection of critical infrastructure due to its vague reference to coordination that must take place without prescribing how this coordination should be conducted.

PPD-41

PPD-41 provides more detailed responsibilities for the SSAs regarding the protection of critical infrastructure, specifically that of the private sector. It states that "[t]he relevant [SSA] will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyberattack on private sector critical infrastructure."

Department of Defense (DoD)

DoD plays a vital role in protecting critical infrastructure, particularly the DIB. However, this role becomes a little less clear as many of the strategies and frameworks list DoD as solely a supporting actor to DHS. The documents below discuss the supporting role that DoD plays, as indicated in **Table 1-4**.

Table 1-4 DoD Cyber Response Guidance Documents

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
DoD															

DoD Cyber Strategy

In September 2018, DoD released its new Cyber Strategy (DoD CS). Though the full document is classified, an unclassified summary has been made available to the public. The strategy is comprised of four pillars and five lines of effort to help execute the DoD CS. The four pillars are:

1. Protecting the American people, the homeland and the American way of life by safeguarding networks, systems, functions, and data;
2. Promoting American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
3. Preserving peace and security by strengthening the ability of the U.S., its partners and allies to deter and punish those who use cyber maliciously;
4. Advancing American influence to extend the key tenants of an open, interoperable, reliable, and secure internet.

The five lines of effort to help execute these pillars are as: build a more lethal force; compete and deter in cyberspace; strengthen alliances and attack new partnerships; reform the department; and cultivate talent.

For strategic competition in the cyber realm, DoD's first high-level priority is ensuring their ability to fight and win wars in any domain. Fulfilling this mission completely requires protecting the nation's critical infrastructure, as the DIB and non-DoD operated critical infrastructure are imperative to the success of DoD fighting and winning wars. It is important to note that the DoD CS specifically states that DoD should be prepared to defend "when directed," including to defend networks and systems that are not operated by DoD nor are part of the DIB.

The DoD CS also establishes the role of DoD within critical infrastructure as an entity that is charged with preempting and deterring malicious cyber actors from targeting critical infrastructure as a whole. This is an important distinction because it is a role that DHS currently is not playing. Deterring and preempting is currently purely under the purview of DoD.[42]

The second line of effort to pursue the four pillars requires DoD to compete and deter within cyberspace to increase the resilience of critical infrastructure within the U.S. This requires that DoD partners with other agencies and entities within the Federal Government to streamline information sharing.

NIPP

While DoD is mentioned throughout the NIPP, its primary role is defined as the SSA for the DIB. Any responsibilities beyond this role will be exercised only at the request of another Federal agency. The NIPP is specific about this when it is discussing SSAs: Footnote c on page 43 expressly states that any provisions included in the plan do not supersede or affect the authority of DoD entities or their chain of command.

NCIRP

For response to a cyberattack, the DoD performs a similar role as it would for other national emergencies: Namely, defense support of civil authorities (DSCA). DoD resources and capabilities can be utilized to assist with response efforts of other government agencies or entities when requested by DHS, and/or when authorized by the President or the Secretary of Defense (SECDEF).[43] Under the NCIRP, DoD has the specific responsibility for threat and asset response when DoD assets and the DoD Information Network (DoDIN) are affected, with

cooperation from both DOJ and DHS.[38] Within the NCIRP, DoD's primary task is to handle all matters dealing with the DIB. Other Federal agencies will become involved if called upon by DoD.

NRF

Within the NRF, it is stated that DoD resources can be committed to respond when requested by another Federal agency, or when directed by the President.

EO 13010

Under this EO, the SECDEF, along with the heads of other agencies, should nominate two full-time members to be on the commission that reports to the President. An Infrastructure Protection Task Force (IPTF) was to be established to include DoD as a member. The IPTF was charged with providing and coordinating the provision of critical infrastructure as well as issuing notifications of potential cyber threats and issuing direct warnings in the event of an attack.

EO 13636

Under this EO, the SECDEF was ordered to collaborate with the heads of other Federal departments to incorporate security standards and information sharing requirements in order to provide classified information to critical infrastructure partners on a need-to-know basis.

DHS - DoD Agreement

As discussed previously, CISA has been established as the new primary agency dedicated to coordinating cyberattack response. However, two days prior to the announcement of creation of his agency, DHS and DoD signed an agreement, authorized under the NPPD, that solidified interagency cooperation and specifically outlined the roles, responsibilities, and authorities of each agency for joint cybersecurity efforts. While reaffirming that DHS remains the LFA regarding all cybersecurity efforts to protect critical infrastructure, the agreement also recognized that in order for DoD to fulfill its mission, including waging and winning wars, critical infrastructure must remain intact and provide the necessary resources.[44]

The agreement based the coordination between DHS and DoD on three primary objectives. The first objective is that both agencies will adopt a "threat-informed, risk-based approach" to ensure the delivery and function of critical infrastructure.[44] This approach will streamline the mutual understanding between the two agencies to determine what constitutes a threat, why the threat is important, and the associated risks and how they should conduct the proper response. This mutual understanding will increase the efficiency and efficacy of resiliency and planning for defense against cyberattacks.

The second objective requires DHS and DoD, with the assistance of the Federal Bureau of Investigation (FBI) and the IC, to develop a common understanding of existing threats and disseminate this information to the owners and operators of critical infrastructure, which will allow the owners and operators to increase their own capacity for resilience and preparation against cyberattacks. Establishing this repository for information on existing threats and current capabilities, with the understanding that it was developed using language and facts that were agreed upon by all contributing parties, and providing the ability to access the information in a timely manner will allow for more confidence within critical infrastructure sectors.[44]

The third objective is that DHS and DoD will each incorporate the individual strengths of the other agency, as necessary and appropriate, to supplement their own individual agency mission and provide for a more coordinated overall resilience. For example, the expertise that DHS has with respect to domestic response capabilities allows them to provide DoD with valuable information to inform DoD of the specific types of threats they could potentially encounter. Likewise, the new "defending forward" objective of the 2018 National Cyber strategy allows DoD to inform DHS on potential adversarial activity they could potentially face, specifically regarding critical infrastructure.[44]

Department of Justice (DOJ)

DOJ plays a variety of roles in cyberattack response and coordination. While DOJ does not assume the lead role in many of the documents that have been discussed, they do play a supporting role as outlined blow. **Table 1-5** identifies the guidance documents under which DOJ has been given some level of authority for response to cyberattacks.

Table 1-5 DOJ Cyber Response Guidance Documents

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
DoJ															

InfraGard

Within the DOJ, the FBI plays the most prominent role in the protection of critical infrastructure through their InfraGard program. InfraGard is a partnership between the FBI (which falls under the DOJ) and members of the private sector. It is the responsibility of the DOJ to administer this program and stimulate public-private collaboration. As of November 2018, there were approximately 50,000 members of the InfraGard program, comprising representatives from all sixteen sectors of critical infrastructure.[45]

Through this program, members of the private sector are afforded the opportunity to learn about current and emerging cyber threats that have been previously identified as the most serious for critical infrastructure, as well as those threats that are intensifying and require increased attention. This learning opportunity includes educational seminars and workshops, information-sharing through federal government reports and assessments, threat advisories, vulnerability reports, and intelligence bulletins. Not only does this collaborative effort provide private entities a chance to streamline their information gathering processes, it also provides government entities a chance to review data and analysis from the private sector as well.

NCIRP

The NCIRP states that when an attack response is initiated, DOJ, through the FBI, is the LFA. Attack response activities can include investigative, forensic, and analytical activities, as well as the conducting of appropriate law enforcement and national security investigative activities. The DOJ offices of U.S. attorneys and criminal and National Security divisions work with Federal law enforcement agencies and use their authorities to disrupt and apprehend malicious cyber actors.

NIPP

The DOJ, including the FBI, is tasked with leading counterterrorism and counterintelligence investigations and related law enforcement activity across all sectors of critical infrastructure. It is the job of DOJ to investigate, disrupt, and prosecute threats or attempted attacks against the nation's critical infrastructure.

E0 13010

Under this EO, the head of DOJ along with the heads of other Federal agencies should nominate two full time members to be on the commission that reports to the President. An IPTF within the DOJ was to be established, and to be chaired by the FBI. The IPTF was tasked with providing and coordinating the provision of critical infrastructure as well as issuing notifications of potential cyber threats and issuing direct warnings in the event of an attack.

PPD-21

Under PPD-21, DOJ was assigned to lead investigations and related law enforcement activities across all sectors of critical infrastructure. They are provided the same responsibilities as mentioned under the NIPP.

PEO 13800

PEO 13800 does not explicitly mention DOJ, but it does include the FBI. Under this PEO, the FBI is tasked with aiding in identifying the authorities and capabilities that agencies could employ to support cybersecurity efforts, as well as providing a report to the President that includes findings and recommendations for better supporting the cybersecurity risk management efforts of Section 9 entities. Additionally, the FBI should consult with other SSAs regarding cyber threat information sharing, response, capacity building, and cooperation.

Office of the Director of National Intelligence

ODNI oversees intelligence support and asset protection in the event of a cyberattack. Additionally, ODNI acts as the principal advisor to the President in many of the frameworks

currently in place for critical infrastructure protection. **Table 1-6** identifies the frameworks under which ODNI has been specified direct responsibilities for response to cyberattacks.

Table 1-6 ODNI Cyber Response Guidance Documents

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
ODNI															

NCIRP

Under the NCIRP, ODNI is designated as the LFA for intelligence support regarding cyberattack response, and is tasked with providing intelligence support to Federal agencies. If a cyberattack affects IC assets, ODNI manages the threat and asset response.

NIPP

Under the NIPP, the IC, led by ODNI, should use their authorities and mechanisms to assess threats to critical infrastructure and coordinate on intelligence and other information related to critical infrastructure. They should also oversee information security policies, guidelines and standards, and directives for safeguarding national security systems as directed by the President.

NRF

The NRF designates ODNI to serves head of the IC and act as the principal advisor to the President regarding intelligence matters.

E0 13636

This EO requires ODNI as well as others to issue instructions about their specific authorities regarding cyber threats. The instructions will address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

PPD-21

PPD-21 requires the Director of National Intelligence to use the authorities and appropriate coordination mechanisms to provide intelligence assessments regarding threats to critical infrastructure.

PEO 13800

PEO 13800 requires that for any National Security System, ODNI should work with other SSAs to provide a report and identify authorities and capabilities that agencies could use to support cybersecurity efforts. This document also requires ODNI to examine the capability of the U.S. to manage the potential consequences of an attack while identifying any potential gaps and shortcomings.

State, Local, Tribal, and Territorial Governments

State, local, tribal, and territorial (SLTT) governments form the backbone of the U.S. administrative power that coincides with the Federal Government. In the world of cybersecurity, SLTT governments play a key role in the protection of critical infrastructure. In most cases, SLTT governments act as first responders in the event of a cyberattack and do as much as they are able using their own resources, until the Federal Government is called upon to intercede. SLTT governments are cited in a variety of documents and agency missions that involve the protection of critical infrastructure, as outlined in **Table 1-7**.

Table 1-7 SLTT Government Cyber Response Guidance Documents

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
SLTT															

NCIRP

The NCIRP stresses the importance of the cohesion between the Federal Government and SLTT governments regarding cybersecurity. The need for cohesion is exemplified within one of its

guiding principles, “Unity of Government Effort.” The plan places substantial focus and detail on SLTT governments, explaining their role in threat response, asset response, intelligence support, affected entity response, coordinating structures, and cyber operations.

NIPP

The NIPPP also focuses on the collaboration between SLTT governments, the Federal Government, and the private sector. The goals and expectations of SLTT governments are included throughout the document, detailing what they need to complete in order to protect critical infrastructure during a cyberattack.

PPD-21

PPD-21 establishes a need for partnership between all levels of government, but fails to provide SLTT governments with specific directions due to the document focusing more on the Federal Government.

PPD-41

PPD-41 makes even less mention of SLTT governments than PPD-21; they are only cited when the guiding principles and the effort to coordinate government actions are outlined.

Guidance Document Analysis Scorecard

In order to begin to understand the roles of the various government agencies and entities that are tasked with cybersecurity responsibilities for critical infrastructure, an analysis and understanding of current government documents that address these response mechanisms to a cyberattack is important. Throughout this chapter, each of the primary entities that play a role in protecting critical infrastructure have been outlined and analyzed under the documents in which they are referenced. Although this chapter only explicitly discusses six such entities, **Table 1-8** provides a comprehensive guide that identifies **all** the agencies, departments, and entities that play a role in cybersecurity for critical infrastructure and the governance and guidance documents in which they are included. This guide provides a visible representation of the overlap

between and the involvement within individual entities regarding cybersecurity and the lack of coordination between roles and responsibilities defined under the separate guidance documents.

Due to the federalist structure of the U.S. government and the interconnection with the capitalist structure of the private sector, entities at all levels of government participate in a shared responsibility for ensuring the protection of the nation's critical infrastructure. This includes federal entities, tribal and territorial entities, public and private owners, and operators.

Table 1-8 Guidance Document Analysis Scorecard

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
DoD															
DHS															
DoJ															
ODNI															
SLTT															
SSAs															
DoS															
DoI															
DoC															
GSA															
NRC															
FCC															
FSRAs															
ACs															
PEs															
NIST															
NGOs															
LGs															

Table 1-8 Guidance Document Analysis Scorecard

	NCIRP	NIPP	DHS CS	NRF	CISA	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
STT+ IAGs				■											
CD					■										
ECD					■										
ISD					■										
NRMC					■								■		
FPS					■										
OFAs						■									
NSA								■							
Acs		■						■	■						
FBI								■							
CIA								■							
FEMA								■							
IPTF								■							
OMB									■			■			
NSC											■				
NCCIC													■		
NRMC					■								■		
FAV														■	■

Limitations and Recommendations

One of the primary issues that the government must address regarding its role in cybersecurity is a lack of consistency between the various strategies, plans, and documents that guide cybersecurity efforts. Each government agency has been tasked with a specific mission to protect critical infrastructure and must assume a different, unique role in attack response. However, in the event of a cyberattack all agencies will be required to work together in order to address the attack, mitigate the potential damages, and provide recovery assistance. The NCIRP clearly outlines the roles for threat and asset response. However, the NIPP also outlines threat response roles for attacks that target critical infrastructure. The NIPP is not discussed or mentioned in the NCIRP, and the NCIRP is not mentioned in the NIPP. Since both are guidance documents, as opposed to official government statutes, there arises the potential issue for determining which document supersedes the other during attack response, and therefore the distinct and unique roles and responsibilities of the participating agencies for a single, fully coordinated attack response has not been established. This presents the potential for confusion in the event of a cyberattack.

The current NIPP outlines the collaboration between government and private sector entities that are involved directly with critical infrastructure to manage risks and meet security or resilience goals with respect to cybersecurity. However, the "current" NIPP was issued in 2013 and is considered out-of-date compared to the reality of the state of current cyber threats and the relationship between the agencies that have tasked with protecting critical infrastructure. Also, the NIPP is the only strategy developed to specifically protect critical infrastructure.[41] This changed after the passage of the Cybersecurity and Infrastructure Security Agency Act in November 2018.[9] The new agency that was created through this act, CISA, is directed to lead the national effort to protect critical infrastructure while working with government and private sector partners. However, with this being a relatively new agency, all aspects of its functions and operations have not yet been finalized.

It must also be acknowledged that the current cyberattack response frameworks, strategies, and guidance documents were developed under different presidential administrations, which means they will likely reflect different administrative goals, aspirations, strategies, and plans for cybersecurity. The NRF, NCIRP, and NIPP were all issued during the Obama Administration,

while the most recent DHS CS was developed by the Trump Administration. Competing domestic and international policies, including those for defense and attack response, will result in language changing between similar documents released under different administrations, especially administrations of different political parties. The language of newer documents may completely contradict that of older documents. When new frameworks, strategies, and guidance documents are developed without clear reference to previous, similar documents, an issue arises of which document should take precedence during an attack. If the language is directly contradictory, this will further complicate the ability for adequate response.

Based on the research conducted on the current laws, policies, strategies, frameworks, and guidance documents that discuss cybersecurity and cyber incident response, the primary recommendation of this chapter of the report is for CISA to create a single, comprehensive plan/strategy for cyberattack response regarding critical infrastructure that supersedes all other critical infrastructure cyberattack response guidance documents. Due to the establishment of CISA as the new central agency that handles cyber infrastructure matters exclusively, this agency should be responsible for producing a guiding document for cyberattack response and mitigation. This document should include an attack handbook that aligns with the 2018 National Cyber Strategy and the 2018 National Security Strategy and should be continuously updated to include the most accurate data and information for effective cyberattack response.

Additionally, each SSA will be required to update their individual cyberattack response plans to reflect and expand upon what is included in the new CISA document. This puts each individual sector of critical infrastructure in concurrence with the direction of the central authority and streamlines the individual response mechanisms for each sector. Lastly, through incorporating the updates and changes issued by CISA, the cyber infrastructure sections in each of the existing guidance documents should be completely removed or updated to reflect what is included in the new document.

References

1. Executive Order No. 13010. Federal Register, vol. 61, no. 138, p. 37347-37350 (1996).
2. Moteff, John. Claudia Copeland, and John Fischer. 2003. "*Critical Infrastructures: What Makes an Infrastructure Critical?"*. Congressional Research Service. https://fas.org/irp/crs/RL31556.pdf
3. Weed, Scott A. 2017. "U.S. Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure." Air Force University Research Institute. *https://www.hsdl.org/?abstract&did=803892*
4. Executive Order No. 13636. Federal Register, vol 78, no. 33, p. 11739-11744 (2013).
5. Department of Homeland Security. 2015. *Presidential Policy Directive 21.* https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf
6. Department of Homeland Security. 2019. "Infrastructure Security". https://www.dhs.gov/topic/critical-infrastructure-security
7. Government Accountability Office. 2005. Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. https://www.gao.gov/new.items/d05434.pdf
8. Presidential Policy Directive No. 41. Weekly Comp. Pres. Doc. DCPD-201600495. (2016).
9. Department of Homeland Security. 2018. "Cybersecurity and Infrastructure Security Agency: About CISA". https://www.dhs.gov/cisa/about-cisa.
10. Federal Emergency Management Agency. 2011. *Strategic Foresight Initiative*. https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf
11. North Atlantic Treaty Organization. 2013. "The History of Cyber Attacks - a Timeline.". https://www.nato.int/docu/review/2013/cyber/timeline/en/index.html
12. Lachow, Irving. 2011. "The Stuxnet Enigma: Implications for the Future of Cybersecurity." *Georgetown Journal of International Affairs* 2011: 118-126.
13. Chen, Thomas M. 2014. "Cyberterrorism after Stuxnet." Strategic Studies Institute. https://ssi.armywarcollege.edu/pdffiles/PUB1211.pdf
14. Jabbour, Kamal, and Erich Devendorf. 2017. "Cyber Threat Characterization." *The Cyber Defense Review* 2(3): 79-94.
15. Dickman, Frank. 2013. "Hacking The Industrial SCADA Network II Latest Threats To Pipeline, Production And Process Management Systems." https://www.automation.com/pdf_articles/SCADA_Threat_Assessment_Hacking_SCADA_Network_II.pdf

16. Porche III, Isaac R., Jerry M. Sollinger, and Shawn McKay. 2011. *A Cyberworm That Knows No Boundaries*. RAND Corporation: National Defense Research Institute. https://www.rand.org/pubs/occasional_papers/OP342.html

17. Holloway, Michael. 2015. "Stuxnet Worm Attack On Iranian Nuclear Facilities". http://large.stanford.edu/courses/2015/ph241/holloway1/

18. Trautman, Lawrence J. and Peter C. Ormerod. 2018. "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things." *University of Miami Law Review* 72(3): 761–826.

19. Carlin, John P. 2016. "Assistant Attorney General John P. Carlin Delivers Remarks at Press Conference Announcing Seven Iranians Charged for Conducting Cyber Attacks against U.S. Financial Sector." The United States Department of Justice. https://www.justice.gov/opa/speech/assistant-attorney-general-john-p-carlin-delivers-remarks-press-conference-announcing

20. Connor, Tracy, Tom Winter, and Stephanie Gosk. 2015. "Iranian Hackers Claim Cyber Attack on New York Dam." NBCNews.com. https://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611

21. Thompson, Mark. 2016. "Iranian Cyber Attack on New York Dam Shows Future of War." Time Magazine. http://time.com/4270728/iran-cyber-attack-dam-fbi/

22. Trautman, Lawrence. 2016. "Is Cyberattack the Next Pearl Harbor?" *North Carolina Journal of Law & Technology* 18(2): 233-289.

23. Park, Donghui., Julia Summers, and Michael Walstrom. 2017. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." University of Washington: The Henry M. Jackson School of International Studies. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

24. Volz, Dustin. 2016. "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage." Reuters. https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K

25. Lee, Robert M., Michael J. Assante, Tim Conway. 2016. "TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid." SANS Industrial Control Systems | Electric Information Sharing and Analysis Center. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

26. Sullivan, Julia E., and Dmitriy Kamensky. 2017. "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid." *The Electricity Journal* 30(3): 30-35.

27. Newman, Lily. 2018. "The Ransomware that hobbled Atlanta will strike again" Wired.com. https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/

28. Techcrunch. 2018. “Atlanta Cyberattack.” *https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/*

29. National Public Radio. 2018. “Atlanta Paralyzed For More Than A Week By Cyber Attack.” https://www.npr.org/2018/03/30/598386485/atlanta-paralyzed-for-more-than-a-week-by-cyber-attack

30. Blinder, Alan, and Nicole Perloth. 2018. “A Cyberattack Hobbles Atlanta, and Security Experts Shudder.” The New York Times. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

31. Grinberg, Emanuella. 2018. “The FBI is investigating a ransomware attack on the city of Atlanta.” Cable News Network. https://www.cnn.com/2018/03/22/us/atlanta-ransomware-attack/index.html

32. Sebenius, Alyza. 2018. “Iran-Based Hackers indicted in March Cyberattack on Atlanta.” Bloomberg. https://www.bloomberg.com/news/articles/2018-12-06/iran-based-hackers-indicted-in-march-cyberattack-on-atlanta

33. Department of Homeland Security. 2016. “Mission.” https://www.dhs.gov/mission.

34. Cybersecurity and Infrastructure Security Agency. 2018. *National Risk Management Fact Sheet.* https://www.dhs.gov/sites/default/files/publications/NRMC%20100%20Days%20Fact%20Sheet%2020181115_CISA%20v2.pdf

35. Department of Homeland Security. 2018. *Department of Homeland Security Cybersecurity Strategy*. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

36. Department of Homeland Security. 2016. *National Response Framework.* https://www.fema.gov/media-library-data/20130726-1914-25045-8516/final_national_response_framework_20130501.pdf

37. Brown, Jared T, and Bruce R. Lindsay. 2018. “*Congressional Primer on Responding to Major Disasters and Emergencies.”* Congressional Research Service. https://fas.org/sgp/crs/homesec/R41981.pdf

38. Department of Homeland Security. 2016. *National Cyber Incident Response Plan.*. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

39. National Institute of Standards and Technology. 2017. “*Framework for Improving Critical Infrastructure Cybersecurity.”* https://www.nist.gov/cyberframework

40. Bajramovic, Eedita. 2015. “Cyber Security in Private Industry Critical Infrastructure.” *International Journal of Economics and La, 5*(13): 9.

41. Department of Homeland Security. 2013. *National Infrastructure Protection Plan.* https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

42. Department of Defense. 2018. *Summary: Department of Defense Cyber Strategy.* https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

43. Ozment, Andy, Tom Atkin, Eric Goldstein and Scott Mann. 2015. *Critical Partnerships: DHS, DoD, and the National Response to Significant Cyber Incidents. Department of Defense.* Department of Defense. https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/DOD-DHS-Cyber_Article-2016-09-23-CLEAN.pdf

44. National Protection and Programs Directorate. 2018. "Written testimony of NPPD for a House Homeland Security Subcommittee on Cybersecurity & Infrastructure Protection and House Armed Services Subcommittee on Emerging Threats & Capabilities hearing regarding Interagency Cyber Cooperation." https://www.dhs.gov/news/2018/11/14/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity

45. Department of Justice. 2018. *InfraGard: Connect to Protect.* https://www.infragard.org/Files/INFRAGARD_Factsheet_10-10-2018.pdf

Chapter 2

The Private Sector's Role in Cybersecurity

Acknowledging the importance of the government's role in securing the nation's critical infrastructure while understanding that most of this infrastructure is privately owned and/or operated is the first step in developing an appropriate national framework for comprehensive cybersecurity. A private sector entity is any organization or business that is not directly under government control; however, this can include government contractors or universities that do receive government funding.

A vital aspect of the current environment of cybersecurity requires understanding the role that the private sector has in this development. The government has historically outsourced the provision of public services to the private sector in an effort to be more cost effective and to provide higher quality services.[1] The use of public-private partnerships as a form of outsourcing began in the late 18th and early 19th centuries when the United States (U.S.) government sought to increase private sector participation in the development of public roads.[1] Additionally, growing discontent with the government during the 1960s increased privatization for other public services as well, including prisons, charter schools, and information technology (IT) services.[2] Similar to the provision of other public goods, such as the Internet, the private sector can be utilized to outsource "cyber maintenance" for the government. In fact, the Department of Defense (DoD) has already started this trend: DoD spent approximately $390 million in 2015 to outsource the creation of new cyber weapon technology to government contractors.[3,4] Utilizing the private sector for innovation and security is becoming more important due to the vulnerabilities of critical infrastructure as a result of the interconnectedness of the Internet.

This chapter discusses the crucial position both the government and private sector occupy in providing cybersecurity for critical infrastructure. Each has instituted different standards for protecting against, mitigating the impact of, and assessing the potential for cyberattacks. These differences demonstrate a need for a more unified approach to cybersecurity, to benefit the private sector as well as the government. Additionally, different levels of cyberattack reporting and the variety of stakeholders in the private sector make up an overarching theme of a public-private partnership, demonstrating the complexity and difficulty of the current process. This chapter will further examine the unique situations that the private sector experiences when defending against cyber threats, considering both small and large businesses, and discusses potential conflicts regarding jurisdiction and cyberattack reporting that exist between the private

sector and the government. These issues have the potential to disrupt effective, unified cybersecurity; this chapter reviews these issues and recommends solutions.

The Private Sector and Critical Infrastructure

The private sector in the U.S. comprises over 30 million companies that employ 91% of American workers, and 99% of these companies are small businesses with less than 500 employees.[5] Regardless of the size, function, or mission of each organization, cybersecurity constitutes a concern for every business in the private sector. Private sector organizations are increasingly using the advantages of the digital world to collect, process, and store large amounts of data, including employee records, customer information, and internal operations information. While the benefits of cyber technologies have allowed private sector organizations to capitalize on advancements, including the Internet of Things (IoT), big data, cloud services, and other emerging technologies, it has also led to the development of a new set of security concerns that companies were not previously prepared to address.[6] The proliferation and increasing sophistication of cyber criminals and malicious actors increases the vulnerability of digital data to cyberattacks, and companies must consider the practical and economic considerations for mitigating the risk to digital data storage.

Within this context, it is important to reiterate that the majority of critical infrastructure is owned and/or operated by private sector organizations.[7] This is important as the practical and economic considerations for cybersecurity within the private sector must account for protecting data and information that belong to private organizations as well as for those elements of critical infrastructure over which the government has a vested interest in protecting. Private sector organizations are involved in the ownership and operation of every sector of critical infrastructure including major soles in the financial, energy, communications, food, and agriculture, and healthcare sectors.[7]

Protocol for Data Security

The major authority for the regulation of data storage and cybersecurity in the U.S. resides within the guidelines promulgated by the Federal Trade Commission (FTC). Section 5 of the Federal Trade Commission Act gave the FTC the authority to investigate “unfair and deceptive

acts and practices in or affecting commerce," which the FTC has interpreted to include data security and protection.[8] This has allowed the FTC to exercise authority in monitoring the security of data stored within private sector organizations.[9] Using this authority, the FTC has promulgated documents that guide private sector organizations to implement data storage and cybersecurity measures; however, these documents do not constitute enforceable requirements. Specifically, the FTC has provided a series of recommendations for data security that encourage businesses to protect customer data that include: establishing a secure, robust cybersecurity system; implementing relevant cybersecurity protocol training for employees; emphasizing the importance of not sharing passwords; and creating internal cybersecurity and data security manager position.[10] While implementing these recommendations will no doubt improve cybersecurity none are legally mandatory.[10]

One area for which the Federal Government has specific laws regarding data protection is for healthcare. Under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Federal Government officially recognized the sensitive nature of personal health data by instituting enforceable regulations to address the proper and secure storage and handling of this type of data.[11] HIPAA was enacted in response to the emergence of technologies that could allow medical records to be portable through electronic means.[12] This portability was intended to allow for easier sharing of information among the various health care providers and institutions a patient may visit. A second important aspect of HIPAA was a guarantee for the security of a patient's medical records.[13] Increasing the electronic portability of patient records created the potential for an increased risk of unauthorized access. The provisions contained within HIPAA require that patient records be made more easily accessible, but also more secure. The Act also requires that explicit permission is required for any individual, other than the individual to whom that information belongs, to access that information, and outlines the protocol for addressing any breach or other unauthorized access of the information.[11] The proliferation of the Internet and the prevalence of cyber threats has further required HIPAA to be used as the legal authority that requires medical information to be protected against cyberattacks.

Similar Federally-mandated data protection requirements have been established for the financial sector as well. Under the Financial Modernization Act of 1999, commonly referred to as the Gramm-Leach-Bliley Act (GLBA), financial institutions are required to provide a "reasonable

level of security" for data and to define the process by which a data breach must be reported.[14] The provisions of the GLBA were intended, in part, to ensure that financial institutions were protecting the confidentiality of their customer's personal information.[15] However, the act is not specifically tailored to the capabilities of modern technology, because technology has advanced to include capabilities that were not even imagined when the act was drafted. Additionally, the act is vague in defining what constitutes a "reasonable level of security," ultimately allowing financial institutions to adopt security measures they consider "reasonable."[15] Additionally, the breach reporting mechanism established by the act has proven hard to enforce due to companies not sharing when a breach has occurred. While the act was a step in the right direction when it was introduced, it lacks the technical details required to adapt to evolving data security concerns.[15]

In addition to HIPAA, GLBA, and the FTC guidelines, there are some state laws that address cybersecurity and data protection. Currently, 24 states have passed legislation affecting the private sector that require some form of data protection.[16] Each state legislation has different requirements and focuses on different aspects within the field of data protection. For instance, in Texas, Business & Commerce Code § 521.052 requires business and nonprofit sports associations that collect personal data to provide "reasonable procedures" to protect this data. In California, Civil Code § 1798.91.04 requires manufacturers of connected devices to equip these devices with reasonable security features to protect any data they may collect, contain, or transmit against unauthorized access, destruction, use, modification, or disclosure. In Colorado, House Bill 18-1128 requires entities that collect data to develop written policies for the disposal of personal information when it is no longer needed. While there is a general principle for requiring businesses to implement and maintain reasonable cybersecurity procedures and provide an avenue for legal corrective action, the specific requirement differences between individual state legislation showcase the lack of uniformity between states.[16] Additionally, the number of states with legislation specifically requiring data security has doubled between 2016 and 2018 showing an increased focus on this type of legislation, and that more is likely to come in the future.[16]

While data protection laws in the U.S. remain limited and vague, the European Union (EU) has made strides to strengthen cybersecurity and data protection measures and to provide more strict

enforcement for failing to comply. The most recent, and comprehensive, of these efforts is the EU's General Data Protection Regulation (GDPR), which was passed into law in 2016 and became enforceable in 2018.[17] The GDPR establishes that the right to personal data collected by companies belongs to the individual from whom that data is collected, and requires entities that collect, process, or disseminate that data to provide appropriate security measures to safeguard the confidentiality, integrity, and availability of the data.[18] The law sets a fine of 20 million euros or 4% of an entity's global sales, whichever is greater, for violation or noncompliance.[19]

Though the GDPR is an EU law, its jurisdiction extends beyond the physical borders of the EU. Any company in the world that collects data on an EU citizen and fails to comply with the regulation can be prosecuted by the EU.[19] Thus, the law directly affects U.S. organizations that collect data when an individual visits the organization's website. Many companies that reach international customers have updated their privacy statements to comply with the provisions of the GDPR.[17] And while most large businesses have not experienced compliance issues and have deemed the required changes to be reasonable, small business have struggled due to the complexity of the regulation and the additional need for understanding the impacts of storing data now complicated by the geographic locations of users.[17] While the disparity in data storage policies has decreased by an estimated 20%, there still remains a large disparity between the current outcomes and the intention of increasing the security of customer data.[18] It remains to be seen if the GDPR will result in the implementation of increased levels of security in the private sector.

In addition to the regulations discussed above, private sector organizations that contract or intend to contract with any part of the Federal Government have additional regulations with which they must comply. The Defense Security Service (DSS) was developed to foster partnerships and innovation between the Federal Government and the private sector by providing security risk management and professional development.[20] The DSS evaluates contractors who apply for government contracts and determines if they meet the security requirements to do government work. To qualify for basic consideration, the contractor and all of their subcontractors must comply with Defense Federal Acquisition Regulation 252.204-7012, which requires contractors to implement data security in accordance with the standards provided in the National Institute for Standards and Technology (NIST) Special Publication 800-171. These standards provide the

"basic" security controls for contractor information systems.[20] The policy further details the conditions that a contractor must pass to be considered eligible for government work. These requirements ensure that a private sector contractor that may be granted access to controlled government information is following proper data security.

Data Security Disparities

The differences between large and small businesses, particularly financial differences, require different considerations for cybersecurity. Small businesses are categorized as those that have fewer than 500 employees and/or make less than $7.5 million in average annual receipts.[21] Due to the limited resources of many small businesses, they are inhibited from investing in the same types of cybersecurity measures that large businesses can afford to purchase or create in-house. However, despite the lack of resources, small businesses must protect their data in the same manner as large businesses. This has allowed for a market to open for the sale of a range of cyber defense systems that companies can purchase and implement, as opposed to creating in-house systems.

Implementation of cybersecurity systems is not normally a concern for small business owners when they first start their business, so many have no form of cyber defense systems, and those that do generally use generic systems available on the free market.[22] This becomes an issue when a small business experiences a data breach. Studies show that 31% of cyberattacks target small businesses, and 60% of those that suffer a data breach fail within six months because they cannot make up the damages.[23] Unless there is an increased focus on investing cybersecurity systems, small businesses may find it difficult to endure as cyberattacks become more prolific and severe.

By contrast, large businesses, especially technology companies, possess the assets and capabilities to develop their own cyber defense systems, and most deploy these systems for data protection. However, while large businesses do have the capacity to protect their data, the current economic incentive system does not necessarily incentivize them to do so.[22] In a 2014 attack, suspected to have been conducted by North Korea in response to the film *The Interview*, Sony spent approximately $35 million to address the attack and recover lost property.[23] The attack consisted of a worm that was designed to listen to and extract data from private phone

conversations that were happening within the company, access employees' personal information, and copy and destroy company records.[24] After accounting for cyber insurance payments to compensate for the losses and advertisement revenues from the film (which grossed more than $40 million), the overall impact of the attack was minuscule considering that Sony's annual revenue is estimated around $68 billion.[23,25]

This outcome was similar for the 2013 Target and Home Depot data breaches. Both Target and Home Depot lost less than 2% of their profits: Target lost $105 million compared to $72.5 billion in sales, while Home Depot lost $28 million compared to $17.7 billion in profit.[26,27] The Target attack occurred due to a heating, ventilating, and air conditioning subcontractor that had been the target of a malware intrusion that allowed hackers to collect personal information and credit card numbers from transactions as customers check-out.[28] The Home Depot attack occurred in a similar manner, despite the fact that Home Depot had an opportunity to learn from the Target attack to consider its own potential vulnerabilities. In this instance, the breach occurred due to the theft of third-party vendor credentials that allowed access to credit card information during check-out transactions.[29] Ultimately, the "loss" that each of these companies suffered was minimized by cyber insurance claims and the enormous profit-to-loss ratio.

This financial "resilience" of large businesses against cyberattacks creates a disincentive to commit a substantial investment in cybersecurity. JPMorgan Chase reportedly spends $250 million on data security each year, which represents only 0.35% of the company's annual expenses.[22] As a banking and investment firm, where protecting customer information and money is vital for business operations, spending such a small portion of the budget on cybersecurity illustrates that large businesses may not currently consider cyber threats as a significant business concern. However, this is not uncommon: Bank of American spends $400 million on cybersecurity, which is less than 1% of their operating budget.[30,31] Even Microsoft, a company specifically devoted to producing computer technology, spends just $1 billion on cybersecurity, which comprises approximately 6% of their operating budget.[32,33] These expenditures indicate that the incentive for large companies to invest more in cyber defense systems is limited as cyberattack have demonstrated minimal potential impact to overall profits. These companies may also not consider cybersecurity a major investment need as they possess the financial capacity to recover after a major breach.

Reporting Cyber Incidents and Public-Private Relations

In April 2018, the governments of the U.S. and the United Kingdom (UK) jointly issued a warning of Russian efforts into malicious cyber activities, which was disseminated among government agencies as well as to the private sector. Many of the potential targets of these efforts were assumed to be critical infrastructure.[34] The cyberattack reporting protocol between the private sector and the government is neither cohesive nor straightforward. Open-source research has yielded very little published information regarding the historic reporting structure or jurisdictional boundaries between the government and the private sector specifically for cybersecurity. However, due to an increase in cyberattacks specifically targeting the private sector, establishing a formal reporting structure and the jurisdictional boundaries for cybersecurity is vital to protect U.S. activities in cyberspace.

Private-to-Federal Reporting Protocol

One of the most significant issues that the private sector faces after a cyberattack has occurred is the lack of a formal protocol by which to report the incident to the Federal Government. While the U.S. government provides the private sector with guidance and advice, most companies either do not know how to correctly report an incident or choose not to report.[35,36] Each individual Federal agency has a different way in which they request the private sector reports an incident.

The U.S. Computer Emergency Readiness Team (US-CERT) requests that private sector organizations submit reports of cyberattacks to the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC evaluates the attack for functional, informational, and potential impact, recoverability, location of observed activity, actor characterization, and cross-sector dependency.[37] Since the NCCIC serves as the national hub for cybersecurity and is located within the Department of Homeland Security (DHS), they currently report attacks to the appropriate government agency responsible for each sector of critical infrastructure.

DHS also accomplishes reporting with the private sector by utilizing Information Sharing and Analysis Centers (ISACs). ISACs are nonprofit organizations, comprising members of the private sector including critical infrastructure owners and operators, that are tasked with

information sharing processes with the government.[38] ISACs can improve cybersecurity within the private sector by increasing cyber resiliency through sharing best practices, joint research, and increase project funding.[39] While ISACs help with information sharing, their utilization does not necessarily increase reporting of cyber incidents. DHS also has a unified guideline for when and to whom the private sector should report a cyberattack. This guideline encourages the private sector to report the cyberattack to Federal authorities if the attack:[40]

- Results in a significant loss of data, system availability, or system control;
- Impacts a large number of victims;
- Indicates unauthorized access to or malicious present within critical infrastructure technology systems;
- Affects critical infrastructure or core government functions;
- Impacts national security, economic security, or public health and safety.

The DHS cyberattack reporting guideline is similar to the cybersecurity guidelines developed by the Department of Justice (DOJ), which focus primarily on prevention. However, in the event of a cyberattack, DOJ has implemented an easy-to-follow reporting procedure that requires private sector organizations to make initial assessment, implement measures to minimize damage, record and collect information, and notify within the organization as well as to federal responders.[41] Within DOJ, the Federal Bureau of Investigation (FBI) is specifically responsible for combatting foreign cyberattacks and threats. The FBI currently disseminates information of potential threats or targets to the private sector, but is seeking to have an embedded information sharing system with the private sector.[42] Moving forward, more thorough cooperation between federal authorities and the private sector is essential for reporting cyber issues.

In 2011, the U.S. Securities and Exchange Commission (SEC) became the first government entity to officially advise private sector organizations on how to properly report cyberattacks by recommending that these organizations advise their investors when an attack occurs. As a result, twenty-four organizations reported cyberattacks to the SEC in 2017, though it is estimated that nearly 5,000 experienced some form of a cyberattack in the same period.[35] In 2018 the SEC further advised companies to also publicly disclose any information regarding cyberattacks.[35,43] However, publicly disclosing that a cyberattack has occurred could display a company's internal

vulnerabilities, thereby providing competitors with the opportunity to address any cybersecurity system failures without displaying their own vulnerabilities.[44] Thus, companies are reluctant to report cyberattacks for fear of losing customers or investors, of facing legal liability, or of the potential damage to their stock value, or simply because they deem it to not be in the company's best interest to report.[45,44]

Despite the reluctance to report a cyberattack, the private sector believes it is more equipped to defend against cyberattacks than the government; consequently, the government outsources much of its cybersecurity to the private sector, which in turn makes the private sector a more susceptible target for cyberattacks.[46,47] Some within the private sector believe that government should not restrict the private sector in how they respond to cyber incidents.[48,49] Not only do large businesses in the private sector possess a preponderance of tools to protect themselves, they are also capable of a more rapid response, including the ability to more quickly and accurately identify those responsible for the attack.[48]

Private to State/Local Reporting Protocol and Capabilities

Similar to the jurisdictional structure for emergencies and natural disasters specified in the National Response Framework (NRF) (discussed in Chapter 1), state and local governments have the initial responsibility for response in the event of a cyberattack. State and local governments can request assistance from the Federal Government if their own resources are insufficient to provide an adequate response. Private sector organizations report an attack to either state or local authorities, who in turn report the incident to the appropriate Lead Federal Agency (LFA).[50] However, state and local governments often lack the adequate tools and resources to rapidly address cyber incident response, losing valuable time as the information moves slowly up the chain of command.[51,52] Some states have created a central state agency that works with both internal and external stakeholders to combat cyberattacks, while other states are simply outsourcing cyber-related issues, including reporting, to contractors in the private sector.[53] This model is common among states with established programs, including Arizona, California, Michigan, New Jersey, New York, Texas, Virginia, and Washington.[54] While establishing a central agency for state and local governments can be beneficial, there is currently no clear path

that allows state and local governments to work directly with the private sector to respond to a cyberattack.

As of late 2018, the cyber capabilities of individual states have been expanded to meet emerging cyber threats.[54] However, most of the expanded capabilities are still in the preliminary stage. States have traditionally combated these threats primarily through assets like security tools and technology plans.[54] However, only 17-21% of state and local government executives believe that they have the tools necessary to detect cybersecurity issues or adequately trained staff to respond to them.[55] Moreover, 25% of local executives believe they are lacking the funding to ensure their own security.[55] This leads to the current reporting structure between state and local governments and the private sector not being conducive to the nature of cyberattacks.

Cyberattack Response Issues: Jurisdiction and Capabilities

The government is frequently confronted with an inability to properly respond to cyberattacks due to jurisdictional issues, the timeliness required for an adequate response, or issues relating to attribution. In instances where the government is unable to provide an adequate response to a cyberattack, the private sector may question the government's cybersecurity capabilities and may instead attempt to address the attack themselves. For example, utilizing the hacking back tactic allows private companies to hack the malicious cyber actor(s) who are hacking their system, in real time, to either retrieve stolen data or to retaliate. This can be accomplished using cybersecurity personnel or through software that is designed to hack back when it senses a threat.[56,57]

However, using hacking back as a defensive tactic presents the potential for serious issues between the U.S. and its allies or adversaries. If a private U.S. company hacked back in response to a cyberattack, and in the process encountered sensitive information or destroyed connections that belong to a foreign government entity, there could be substantial diplomatic repercussions. It is currently illegal for the private sector to hack back, due to a large margin of error on locating the hacker.[58]

Additionally, there is the potential that hacking back could itself be used maliciously; a private company could hack a competitor under the false pretense that they were utilizing hacking back

as defense against a cyber incident.[58] These issues demonstrate the need for the government and the private sector to jointly develop a more coordinated and effective system with which to respond to cyberattacks against the private sector. While it is still illegal for private companies to hack back, legislation to allow private sector organizations to actively defend themselves against cyber threats, using tactics similar to hacking back, is continually (but thus far unsuccessfully) introduced in Congress.[59] The Pentagon has warned that the private sector should not have the ability to conduct offensive hacking; however, the DoD is open to the private sector having more robust cyber defense systems. This can become contentious when determining which capabilities are considered *defensive* and which are considered *offensive*.[60] With the right defense systems and personnel in place, both the government and the private sector can be adequately equipped to defend their respective systems against cyberattacks.

Another problem the government faces regarding cybersecurity is an inability to recruit and retain qualified employees. DoD often trains employees who after a time leave to join the private sector for higher paying jobs. As a result, DoD fills these much-needed positions with underqualified or under skilled candidates.[61] A former Chief Architect and Special Advisor for Cybersecurity for DHS describes the recruitment process for cybersecurity as slow-moving and flawed in enticing qualified people to apply for the positions.[62] To attempt to resolve these issues, the U.S. Office of Personnel Management (OPM) has implemented a system of flexibility regarding compensation for certain cybersecurity positions, with the understanding that there may need to be additional incentives to retain qualified employees.[63] Despite OPM's efforts, these complications provide further proof that the government and the private sector need a strengthened, collaborative effort to ensure that the best minds are fulfilling the nation's need for comprehensive cybersecurity. While considerations for security clearance and the need-to-know status present potential issues related to information sharing, there is no appropriate solution without changing the clearance process and implementing it government-wide.

Another issue that inhibits progress to create stronger coordination between the government and the private sector is information sharing. The current process by which information is shared between separate government entities is subpar and worse between defense agencies or private contractors. This occurs when certain material is classified or designated as "need-to–know," which prevents the Intelligence Community (IC) from truly sharing best practices for

cybersecurity with the private sector.[61] The IC uses DHS to provide information-sharing with critical infrastructure stakeholders, to some success. As an example, the Food and Agriculture Sector integrated information regarding critical infrastructure with that of DHS to provide a more unified information-sharing environment with the other sectors of critical infrastructure.[64] However, this current framework is only advantageous for sharing information between critical infrastructure sectors, and not with all stakeholders in the private sector. This can potentially leave small business, hospitals, and other inherently governmental organizations (government contractors and universities) vulnerable. This vulnerability can create an opportunity for a new public-private partnerships to be used on a large scale for the other issues of employee retainment and information sharing.

Use of Government Contractors and Universities in Cybersecurity

While jurisdiction and reporting issues restrict the private sector regarding cyberattack response, the Federal Government does not have the legal right to use the armed forces as law enforcement within the U.S., as prohibited under the Posse Comitatus Act (further discussed in Chapter 3). The private sector can fill the void created by this restriction through the use of government contractors or universities. Both government contractors and universities use government grants or contracts to either provide a service to the government or use these funds to foster more innovation through research. Government contractors are vulnerable in that they have to abide by similar standards that government agencies have, without also having access to the same information as the government. Universities, on the other hand, are a great resource to foster new talent for the government to meet the needs of a growing cyber field by being at the forefront of new research and innovation.

Government contractors, as discussed previously, have often been a great resource for government outsourcing. Contractors are required by the U.S. government to develop and submit cybersecurity risk management plans for their companies to the government. This has allowed for better partnerships between the government and contractors.[65] Contractors are held to the same standards because the government considers protecting government information a main priority. As contractors often have possession of government information, they are responsible for protecting it.[66] If the government intends to outsource more of its security to

contractors, the government needs to be prepared to take responsibility if the contractors fail to protect government information. Government contractors, however, have the ability to retain more qualified employees than the government by having a competitive salary, and they often look to universities to recruit qualified employees.

Another potential partner to address cybersecurity issues is the higher education system. Much of the new innovation for competition starts in universities. According to a 2017 report released by the Institute for Information Security & Privacy at Georgia Tech, computer science programs at universities across the U.S. are experiencing a record number of applicants. This massive influx of potential computer science graduates will be needed to fill new cybersecurity jobs, the number of which increased by 91% between 2010 and 2014. As such, universities are attempting to utilize the most cutting-edge technologies to teach these students in order to create the most well-educated workforce.[67] Universities become an important stakeholder in U.S. cybersecurity by providing the educational training for students who will eventually be filling these high-demand positions. Community colleges have utilized certification and standard skills tests to assist potential employers in identifying the most qualified candidates.[68] If the government and universities work together, they can educate, train, and employ highly proficient and competent cybersecurity professionals.

Partnering with the government is advantageous for universities when considering the issue of intellectual property theft. Intellectual property is defined as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce."[69] The People's Liberation Army (PLA), China's armed forces, poses a significant threat to intellectual property. The PLA has created its own government agency, the Strategic Support Force (SSF), which is equivalent to U.S. Cyber Command. The goal of the SSF is to surpass the capabilities of the U.S. in all things cyber-related.[70] Through the SSF, China has become one of the largest threats to the intellectual property of U.S. companies. China has already targeted universities and defense contractors, including Duke University and Lockheed-Martin, to steal scientific research, defense secrets, and intellectual property.[71,72]

Protecting intellectual property is becoming a bigger issue for both the government and the private sector, as most threats to intellectual property can be attributed to competitors wanting to

use the information for new jobs or projects.[73] While the U.S. has established corporate espionage laws that prohibit competitors from stealing information, it is hard to implement the same concepts of enforcement and law internationally in regards to intellectual property and cybersecurity.[74] This leads to international implications of unfair competition from overseas competitors and nation-states stealing technology or trade secrets, which both have consequences on the ability of the U.S. to compete and maintain economic stability.

With intellectual property issues becoming more apparent, universities need to "lock-down" their research and skills-based information.[75] Recognizing the importance of the role of the private sector, and universities in particular, in intellectual property security is important for the government to implement a public-private partnership.[74] It is important to establish a public-private partnership that allows for protection of university intellectual property while also fostering new talent for government jobs.

Limitations

While this research indicates that the private sector can address some of the deficiencies of the government regarding cybersecurity and cyberattack response, there are limitations that influence the findings of this report. All of the information included in this chapter has been obtained through publicly-available sources. There may be more substantial information regarding existing public-private partnerships that the government utilizes or the full cybersecurity capabilities of the government or the private sector that have not been publicly disclosed. However, without access to this information it cannot be evaluated against the findings in this chapter.

There are also limitations as to what the private sector can and should currently be able to do in terms of cyberattack response. Government contractors are often restricted in that they must abide by the government standards for cybersecurity, particularly those of DoD, without also having access to the full breadth of information that DoD and the government has obtained regarding cyber threats.[76] Additionally, when the private sector takes cybersecurity into their own hands, as discussed above, there can be larger, political consequences.[57] The private sector

should not be able to respond to cyberattacks without proper information sharing with the government.

Additionally, there are limitations related to the ability of the private sector and the government to provide adequate cyberattack response. In the case of both the government and the private sector, the origin of the incident is critical when determining the appropriate jurisdiction for a response. In the case of the 2014 Sony attack, the U.S. government identified the North Korean government as the probable source of the attack and responded with financial sanctions against North Korea. This demonstrated that the Federal Government is willing to respond to an attack against the private sector the same way it would respond to any other "action under the law of armed conflict."[77,78,79] It does not appear that Sony took any action in this incident.

While there are many restrictions and vulnerabilities that the private sector must consider, there are ways in which the private sector can compensate for deficiencies in the government's capabilities and work with the government to secure U.S. corporate and government interests. Future research should be conducted to examine the length at which the private sector should be allowed to go to respond to cyberattacks. The government should directly support further research into private sector capabilities to facilitate better contracting mechanisms and improve the sharing of best practices. Additionally, the private sector can be used to foster more innovation for cybersecurity through universities, a public-private partnership, and large businesses. Innovation can help the U.S. in the future to compete with peers and near-peers at a more advanced level. While these are important considerations for the future of cybersecurity, it is outside of the scope of this paper to investigate and describe them in greater depth.

Recommendations and Conclusion

The research demonstrates that the private sector, through restrictions set by the government and lack of cybersecurity practices, is vulnerable to cyber incidents. However, the capabilities and flexibility of the private sector impart a greater ability to respond to cyberattacks and incidents than the government, as much of the critical infrastructure is privately-owned. This study provides two recommendations regarding cybersecurity capabilities for the private sector:

reinforcement mechanisms for small businesses, which are the most vulnerable to cyber threats; and a new public-private partnership for cybersecurity.

Small Business Reinforcement

The research shows there is a need for the government to adjust its current policies and regulations to better protect small businesses and incentivize large businesses to maintain robust cybersecurity systems. The disparity between the current levels of protection and the availability to recover from an incident provide an adequate rationale for government intervention.

One of the major disparities between small and large businesses is the use of cyber insurance. While cyber insurance is available to any business, only about 31% of all U.S. businesses currently own cyber insurance, and only 19% of small businesses.[21,80] Cyber insurance provides compensation for monetary losses incurred as a result of a cyberattack, as long as the company has met the basic cybersecurity standards imposed by cyber insurers.[81] Such a policy could help save small businesses from closing as a result of a cyberattack. For large companies, cyber insurance provides a disincentive to invest in the development and implementation of robust cyber defense systems, as their financial losses can be miniscule compared to total revenues and profits and can be recovered through insurance claims. This creates a potential moral hazard in that companies may act riskier because they know any losses due to a cyberattack will be minimized by the insurance. Additionally, the costs of cyber insurance continues to increase as more companies make claims against attacks, which can further disincentives businesses, especially small businesses with fewer financial resources, from purchasing it.[80] Government intervention in the provision of cyber insurance may be able to restore the market to encourage small businesses to purchase insurance and discourage large businesses from taking advantage of such a program.

In addition to adjustments in addressing current cyber insurance policies, the government needs to also determine the most appropriate course of action for providing cyber defense to both large and small businesses. The current FTC recommendations for cybersecurity implementation in the private sector are not legally enforceable, and therefore are not implemented by enough companies to fully protect the private sector.[10] Most companies are not accustomed to providing

their own internal crime defense systems, relying instead on local or Federal law enforcement. This reliance on outside sources may extend to a company's attitude toward cybersecurity. With cyber crime, however, there currently is no corresponding method of law enforcement protection and companies may be unsure how to appropriately address the situation.[41] Companies are also discouraged from investigating attacks on their own, especially given that an attack could arise from overseas, and there is fear among corporate executives that reporting a cyberattack to the government will become public and they will lose public support, negatively impacting them financially. Additionally, the current system for reporting cyber incidents is not clear with respect to proper reporting protocol, jurisdiction for response, and the likelihood of a response. In light of these concerns, as well as the lack of federal law requiring that breaches be reported, companies can continue to operate without reporting when a breach has occurred.[35,36] These issues coalesce to create a sense of insecurity within the private sector regarding cybersecurity and cyberattack response. This insecurity could be addressed through the development of new laws, regulation, and/or developments in cyber defense systems.

Public-Private Partnership

The research shows that there is a strong need for a public-private partnership for cybersecurity due to deficiencies in cybersecurity and cyberattack response in both the government and the private sector. The first aspect regarding cybersecurity in which the government is deficient is job fulfillment and retainment, as it must directly compete with the private sector for the most qualified candidates. The private sector provides higher potential salaries for employment in cybersecurity, forcing the government to fill cybersecurity jobs with individuals who are under-qualified or unqualified.[61] One way in which a public-private partnership can benefit the government is through a job training program in which the government works with the private sector to provide training and establish direct hiring paths to transition professionals from the private sector into government cybersecurity positions. To accommodate this transition, the government may need to provide a more competitive salary to complement the program.

However, due to budgetary constraints and considerations, the government may not be able to provide a salary level that allows them to directly compete with the private sector. As a result, the government could shift its focus from recruiting for cybersecurity positions to outsourcing

these capabilities, which could potentially be a more cost-effective method. One way in which cybersecurity could be effectively outsourced, that would be most beneficial to the government, would be to have the private sector develop and manage the cybersecurity systems for critical infrastructure, small businesses, and local government security, which represent the areas most in need for improved cyber defense systems.

Outsourcing cannot be efficiently achieved, however, if the government is not willing to fully share cyber threat information with the private sector. The foundation for an effective public-private partnership is contingent on the information flow from one sector the other. While the private sector may be more equipped at handling cybersecurity, an information-sharing mechanism should be utilized to share best practices between the sectors. Also, since government cyberattack response is known to be slow, establishing an information-sharing mechanism could potentially decrease the disparity between when a cyberattack occurs and the time it takes to respond.

A public-private information-sharing mechanism can best be implemented through Fusion Centers located across the country. Fusion Centers are defined as a "collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[82] If Fusion Centers were open to allowing input from the private sector, information sharing for cybersecurity would be more efficient and beneficial to all areas of U.S. technology. However, proper flow of information will continue to be one of the more difficult solutions to implement.

The establishment of a public-private partnership incorporating these recommendations will reinforce the cybersecurity capabilities of both the government and the private sector, while also potentially renewing the public's trust in the government's ability to respond to cyberattacks. The results of a *Gallup* poll conducted over a period of 10 years, from 2008 to 2018, ranged from a low of 14% and a high of only 28% in terms of the public's confidence in the Federal Government's ability to handle international and domestic issues.[83] Potential disadvantages of using a public-private partnership for cybersecurity include a decrease in overall government accountability, a slower information sharing mechanism, and a lack of change in "need-to-know"

status and security clearance process.[44] Despite this, there are ways to increase accountability from all parties by actively engaging both public and private partners as stakeholders in cybersecurity. Addressing these issues and utilizing the strengths of both the government and the private sector can help create a public-private partnership for cybersecurity that is beneficial for all U.S. institutions.

Although the private sector needs more reinforcement for small businesses, the private sector is still an under-utilized cybersecurity resource for the government. With government intervention into the provision of cyber insurance for small business and the establishment of a public-private partnership for cybersecurity, the private sector and the government can be better positioned to address the evolution of cyber threats. Where a lack of a formal reporting structure or comprehensive response framework may be nonexistent, or where the government might be restricted, the private sector can potentially fill in the gaps for cyberattack response to ensure the protection of U.S. national security.

References

1. Buxbaum, Jeffrey N, and Iris N. Ortiz. 2009. "Public Sector Decision Making for Public-Private Partnerships." *NCHRP Synthesis of Highway Practice 391*: 6-10 (6)
2. Cohen, Donald. 2016. "The History of Privatization." Talking Points Memo. https://talkingpointsmemo.com/features/privatization/one/.
3. Fernholz, Tim. 2014. "Barack Obama Says the Internet is a Public Good, and That's Why the US Needs Net Neutrality." Quartz. https://qz.com/293904/barack-obama-says-the-internet-is-a-public-good-and-thats-why-the-us-needs-net-neutrality/. (November 14, 2014).
4. O'Neil, Patrick H. 2015. "U.S. Military Plans to Outsource Cyberwar Support to Private Companies." The Daily Dot. https://www.dailydot.com/layer8/private-sector-cyber-warfare-dod-nsa/. (November 11, 2015).
5. Small Business Administration. 2018. 2018 Small Business Profile. https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf
6. Pence, H. E. (2015). Will Big Data Mean the End of Privacy? Journal of Educational Technology Systems, 44(2), 253–267. http://proxy.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1084389&site=eds-live
7. Federal Emergency Management Agency. 2011. *Strategic Foresight Initiative*. https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf
8. Federal Trade Commission Act. 15 U.S.C. §§ 41-58. (1914).
9. Woods, Jennifer. 2013. "Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5." American Bar Association. https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy/
10. Federal Trade Commission. 2016. *Data Breach Response: A Guide for Business*. https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf
11. Department of Health and Human Services. 2013. "HHS Breach Notification Rule." https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
12. Bagwell, Scott. (2015). "The Cure to Improve and Protect Health Care Records." *USA Today Magazine* 144 (2844): 26–27.
13. Uribe, L. P. M., & Schub, T. B. 2018. Health Insurance Portability and Accountability Act (HIPAA): Data Communication and Security. *CINAHL Nursing Guide*. http://proxy.library.tamu.edu.srv-

proxy1.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nup&AN=T904674&site=eds-live

14. Gramm-Leach-Bliley Act. Federal Register 83 40945 (1999).
15. White, Lawrence J. 2010. "The Gramm-Leach-Bliley Act of 1999: A bridge too far? Or not far enough?" *Suffolk University Law Review* Vol. 43 (4): 937-956.
16. National Conference of State Legislatures. 2019. "Data Security Laws | State Governments." http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx
17. Hinely, Mark. 2018. "GDPR Fundamentals: The Basics of the Law." KirkpatrickPrice. https://kirkpatrickprice.com/video/gdpr-fundamentals-the-basics-of-the-law/
18. Linden, Thomas, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2018. "The Privacy Policy Landscape After GDPR." Cornell University: arZXiv. https://arxiv.org/pdf/1809.08396.pdf
19. Sirur, Sean, Jason R.C. Nurse, and Helena Webb. 2018. "Are we there Yet? Understanding the Challenges Faced in Applying with the General Data Protection Regulation." Cornell University: arXiv https://arxiv.org/pdf/1808.07338.pdf
20. Defense Security Service. 2019. "Vision and Mission. https://www.dss.mil/
21. Beesley, Caron. 2016. "How and Why to Determine if Your Business is "Small"." U.S. Small Business Association. https://www.sba.gov/blogs/how-and-why-determine-if-your-business-small
22. Hephner, Lisa. 2015. "Why Security is More Important for Small Businesses then It is for Larger Companies." Pay Simple. https://paysimple.com/blog/why-security-is-more-important-to-small-businesses-than-it-is-to-mega-companies/
23. Dean, Benjamin. 2015. "Why Companies Have Little Incentive to Invest in Cybersecurity." The Conversation. https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570
24. Targeted Destructive Malware. 2014. U.S. CISA. https://www.us-cert.gov/ncas/alerts/TA14-353A
25. Statista. 2019. "Sony's total revenue from 2007 to 2017 (in 100 billion Japanese yen / billion U.S. dollars)*." https://www.statista.com/statistics/279269/total-revenue-of-sony-since-2008/.
26. Target Corporation. 2014. *Target 2013 Annual Report*. https://corporate.target.com/_media/TargetCorp/annualreports/content/download/pdf/Target-2013-Annual-Report.pdf?ext=.pdf

27. The Home Depot. 2014. "The Home Depot Announces Fourth Quarter & Fiscal 2013 Results; Increases Quarterly Dividend By 21 Percent And Provides Fiscal Year 2014 Guidance." http://ir.homedepot.com/news-releases/2014/02-25-2014-014521683

28. Kerbs, Brian. 2014. Target Hackers Broke in Via HVAC Company. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

29. Hawkins, Bret. 2015. Case Study: The Home Depot Data Breach. *SANS Institute.* https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

30. Morgan, Steve. 2018. 2018 Cybersecurity Market Report. https://cybersecurityventures.com/cybersecurity-market-report/

31. Bank of America. 2017. Bank of America Corporation 2017 Annual Report. http://media.corporate-ir.net/media_files/IROL/71/71595/BOAML_AR2017.pdf

32. Talton, Ellis and Tonar, Remington. 2018. A Lack Of Cybersecurity Funding And Expertise Threatens U.S. Infrastructure. *Forbes.* https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#5da03676264c

33. Microsoft. n.d "Microsoft's net income from 2002 to 2018 (in billions U.S. dollars)." In *Statista – The Statistics Portal.* https://www.statista.com/statistics/267808/net-income-of-microsoft-since-2002/.

34. Thomas, Ria. 2018. "Evolving Weapons of War: Cyberattacks on Companies." *Brunswick Group*. https://www.brunswickgroup.com/evolving-weapons-of-war-cyber-attacks-on-companies-i7638/. (April 18, 2018).

35. Newman, Craig. 2018. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times. https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. (March 5, 2018).

36. Amir, Eli, Shai Levi, and Tsafrir Livne. 2018. "Do Firms Under-Report Information on Cyber-Attacks?" The Columbia Law School Blue Sky Blog - Columbia Law School. http://clsbluesky.law.columbia.edu/2018/04/02/do-firms-under-report-information-on-cyber-attacks/. (April 02, 2018).

37. United States Computer Emergency Readiness Team. 2017. *US-CERT Federal Incident Notification Guidelines*. https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

38. United States Department of Homeland Security. 2019. "Information Sharing and Awareness." https://www.dhs.gov/cisa/information-sharing.

39. Van Impe, Koen. 2018. "How Can an ISAC Improve Cybersecurity and Resilience?" *SecurityIntelligence.* https://securityintelligence.com/how-can-an-isac-improve-cybersecurity-and-resilience/. (July 16, 2018).

40. Department of Homeland Security. n.d. *Cyber Incident Reporting A Unified Message for Reporting to the Federal Government.* https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf.

41. United States Department of Justice. 2018. *Best Practices for Victim Response and Reporting of Cyber Incidents*. https://www.justice.gov/criminal-ccips/file/1096971/download.

42. United States Federal Bureau of Investigation. 2018. "Small Business Information Sharing: Combating Foreign Cyber Threats." https://www.fbi.gov/news/testimony/small-business-information-sharing-combating-foreign-cyber-threats.

43. United States Securities and Exchange Commission. 2018. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.sec.gov/rules/interp/2018/33-10459.pdf.

44. Papier, Leesa. 2019. Authors Interview. The Bush School of Government and Public Service. (February 1, 2019).

45. Javers, Eamon. 2013. "Cyber attacks: Why Companies Keep Quiet." CNBC. https://www.cnbc.com/id/100491610. (February 25, 2013).

46. Wheeler, Tarah. 2018. "In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions." *Foreign Policy.* https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/.

47. Walters, Riley. 2018. Private Sector Cyber Incidents in 2017. *The Heritage Foundation*. https://www.heritage.org/cybersecurity/report/private-sector-cyber-incidents-2017. (January 3, 2018).

48. Truman Center. 2018. "The Private Sector's Role in Cyber Security." http://trumancenter.org/cybersecurity/the-private-sectors-role-in-cyber-security/.

49. Fredrick, Paul and David Inserra. 2018. "How Congress Can Help Protect U.S. Companies From Cyber Attack." The Heritage Foundation. https://www.heritage.org/technology/commentary/how-congress-can-help-protect-us-companies-cyber-attack. (January 30, 2018).

50. Department of Homeland Security. 2016. *National Response Framework.* https://www.fema.gov/media-library-data/20130726-1914-25045-8516/final_national_response_framework_20130501.pdf

51. Arizona Infragard. 2018. "Arizona Cyber Threat Response Alliance". http://azinfragard.org/?page_id=8 (November 20th, 2018).

52. Arizona Cyber Warfare Range. 2018. "About". https://www.azcwr.org/ (November 20, 2018). Atlantic Council. 2017. "Tallinn Manual 2.0 Clarifies How International Law Applies to Cyber Operations." http://www.atlanticcouncil.org/news/press-releases/tallinn-manual-2-0-clarifies-how-international-law-applies-to-cyber-operations

53. Friedman, Sara. 2018. "How States Respond to Cyber Threats." CGN Technology. https://gcn.com/Articles/2018/05/31/state-cybersecurity-approaches.aspx. (May 31, 2018).

54. Cohen, Natahsa & Brian Nussbaum. 2018. "Cybersecurity for the States: Lessons from Across America." New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_for_the_States_Lessons_from_Across_America_FINAL_3.pdf.

55. Cyberscoop. 2018. "Opportunities for Improving Cybersecurity Visibility at State & Local Government Agencies." Statescoop. https://s3.amazonaws.com/statescoop-media/uploads/Tenable-DisruptiveStudy-Final-1.pdf?mtime=20180419164427 (Pg. 16)

56. Robertson, Jordan and Michael Riley. 2014. "Corporations Warned Not to Hack Back." Insurance Journal. https://www.insurancejournal.com/news/national/2014/12/31/351326.htm.

57. McLaughlin, Kevin J. 2019. Authors Interview. The Bush School of Government and Public Service. (February 7, 2019).

58. Strom, David. 2018. "What Are the Legalities and Implications of "Hacking Back"? Security Intelligence. https://securityintelligence.com/what-are-the-legalities-and-implications-of-hacking-back/ (March 7th, 2019).

59. O'Neill, Patrick Howell. 2017. "'Hacking back' legislation is back in Congress." *Cyberscoop.* https://www.cyberscoop.com/hack-back-bill-tom-graves-kyrsten-sineman-cfaa/. (October 16, 2017).

60. Thomsen, Jaqueline. 2018. "Pentagon Cyber Official Warns U.S. Companies Against 'Hacking Back'." The Hill. https://thehill.com/policy/cybersecurity/416494-defense-cyber-official-warns-private-companies-against-hacking-back. (November 13, 2018).

61. United States Government Accountability Office. 2018. *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*. https://www.gao.gov/assets/700/694913.pdf

62. Chaillan, Nicolas. 2019. Authors Interview. The Bush School of Government and Public Service. (January 25, 2019).

63. United States Office of Personal Management. n.d. "Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals." https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf.

64. Director of National Intelligence. 2019. "Sharing with the Private Sector." https://www.dni.gov/index.php/who-we-are/organizations/ise/archive/additional-resources/2144-sharing-with-the-private-sector

65. Garrett, Gregory and Karen Schuler. 2017. "6 Cybersecurity Questions Government Contractors Should Address." BDO International. https://www.bdo.com/insights/industries/government-contracting/winter-2018/6-cybersecurity-questions-government-contractors-s.

66. Cassidy, Susan. 2016. "More Cybersecurity Changes Expected for Contractors in 2017." Inside Government Contracts. https://www.insidegovernmentcontracts.com/2016/12/cybersecurity-changes-expected-contractors-2017/. (December 29, 2016).

67. Georgia Tech: Institute for Information Security & Privacy. 2017. "Emerging Cyber Threats, Trends & Technologies Report. Georgia Tech, Institute for Information Security & Privacy". http://www.iisp.gatech.edu/sites/default/files/documents/2017_threats_report_finalblu-web.pdf.

68. National Science Foundation and the American Association of Community Colleges. 2002. "Protecting Information: The Role of Community Colleges in Cyber Education." https://www.nationalcyberwatch.org/ncw-content/uploads/2016/03/Workshop_Rpt-Role_of_CCs_in_Cyber_Ed-2002.pdf.

69. World Intellectual Property Organization. 2019. "What is Intellectual Property?" https://www.wipo.int/about-ip/en/.

70. Bing, Chris. 2017. How China's Cyber Command Is Being Built to Supersede Its U.S. Military Counterpart. *Cyberscoop.* https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod/. (June 22, 2017).

71. Bloomberg. 2012. "Intellectual-Property Threat Abound for U.S. Companies." https://www.bloomberg.com/news/photo-essays/2012-10-02/intellectual-property-threats-abound-for-u-dot-s-dot-companies.

72. McFadden, C., Nadi, A., and McGee, C. 2018. "Education or Espionage? A Chinese Student Takes His Homework Home to China." NBC News. https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881. (July 24, 2018).

73. Kohen, Issac. 2018. "Protecting Intellectual Property Against Cyberattack." CSO. https://www.csoonline.com/article/3245310/protecting-intellectual-property-against-cyberattack.html. (January 2, 2018).

74. Ruttenberg, Joan, Paige von Mehren, and Julie Yen. 2013. "The OPIA Insider's Guide to Intellectual Property And Cyberlaw." Bernard Koteen Office of Public Interest Advising Harvard Law School. http://www.hls.harvard.edu/content/uploads/2008/06/ip-cyberlaw-guide-final.pdf.

75. Tech Transfer Central. “Ensuring Cybersecurity to Protect University IP Assets.” https://techtransfercentral.com/marketplace/distance-learning/ensuring-cybersecurity-to-protect-university-ip-assets/.

76. Garrett, Gregory A. 2018. “Cybersecurity for Government Contractors: Next Steps.” BDO International. https://www.bdo.com/insights/business-financial-advisory/cybersecurity-for-government-contractors-next-ste. (February, 2018).

77. Theohary, Catherine A., and Anne I. Harrington. 2015. “*Cyber Operations in DOD Policy and Plans: Issues for Congress*.” The Congressional Research Service, https://fas.org/sgp/crs/natsec/R43848.pdf. (p.21-22).

78. Peterson, Andrea. 2014. “The Sony Pictures Hack, Explained.” *The Washington Post.* https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.0048bb417c6b

79. Nakashima, Ellen. 2015. “Why the Sony hack drew an unprecedented U.S. response against North Korea.” *The Washington Post*. https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html?noredirect=on&utm_term=.54d45fe9129f

80. Lynch, James, and Claire Wilkinson. 2017. “Small Business and Cyber Insurance.” Insurance Information Institute. https://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_103017.pdf

81. Hiscox. 2018. “Small Business Cyber Risk Report.” https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

82. Department of Homeland Security. 2008. “National Network of Fusion Centers Fact Sheet.” https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

83. Gallup. 2018. “Trust in Government.” https://news.gallup.com/poll/5392/trust-government.aspx.

Chapter 3

Cybersecurity and Individual Privacy

United States (U.S.) internet protocol (IP) space is dependent on critical infrastructure, and critical infrastructure is dependent on IP space. The all-encompassing realms, conflicting and overlapping jurisdictions, and competitive nature of cybersecurity create a contested space. Within this contested space exists adversaries with similar capabilities and advancements as the U.S. Throughout the 2017 National Security Strategy, the Trump Administration uses the term "competition" repeatedly in reference to other nations; this is the first time in the history of the National Security Strategy that the term has been used. This implies that the national leadership believes that any gaps in cybersecurity capabilities, whether in technology or knowledge, between the U.S. and its adversaries is closing and that the U.S. must compete for supremacy in the realm of cyberspace. Securing IP space is a matter of national security, which, depending on the target, severity, or perpetrator of the incident, could rise to the level of requiring the Federal Government to engage national defense capabilities. Given the nature of U.S. IP space, there arises the question as to whether or not DoD is restricted, or even over-restricted, from conducting national defense operations within U.S. IP space.

Answering this question requires first determining what, if any, restrictions exist regarding Department of Defense (DoD) operations within U.S. IP space and defining what constitutes an "over-restriction." The goal of this chapter is to evaluate the restrictions currently in place and provide an objective evaluation as to whether these restrictions are hindering DoD. For example, DoD is currently restricted in conducting law enforcement activities under Title 10 of the U.S. Code, the Posse Comitatus Act, and the Foreign Intelligence Surveillance Act (FISA), and therefore can only operate for means of national defense or in providing defense support of civil authorities (DSCA).[1] Conversely, DoD may be over-restricted in terms of being unable to access sensitive information and to complete investigations and operations against insider threats and those who are U.S. citizens or operating in the U.S. DoD is restricted in accessing U.S. persons information (USPI) as well due to constitutionally-guaranteed rights found in the First and Fourth Amendments, and these restrictions will be examined to determine if they over-restrict DoD from adequately fulfilling their mission of national defense.

Personal Information – The Fourth Amendment

A key consideration when discussing national security in the U.S. is the jurisdictional restrictions the government faces. One of the chief questions addressed here is whether the Federal Government, and specifically DoD, is currently restricted from effectively protecting the nation due to laws enacted with the intent to protect the privacy of U.S. citizens. While the efficacy of the restrictions in place will be discussed later in this chapter, the first objective is to identify and clarify what restrictions currently exist.

The origination of these restrictions is the constitutionally-guaranteed right against unreasonable search and seizures, found in the Fourth Amendment and commonly interpreted as a right to privacy.[2] The notion of a right to privacy has become deeply ingrained in the U.S. legal structure, ensuring that the property of an individual remains outside the jurisdiction of the government, unless the government has probable cause to investigate or seize that property. One issue that arises, which has not yet been decisively addressed, is the extent to which this provision can be applied in the ever-growing realm of IP space.

This issue raises questions as to whether the government can access things like email, phone records, and other personal digital information without a warning, in the interest of national security, or if those things are protected under the Fourth Amendment.[3] For privacy cases defended under Fourth Amendment protections, traditional jurisprudence has required that courts ask whether a reasonable expectation of privacy existed.[4] If an expectation of privacy did exist, the information would be protected under the Fourth Amendment and would therefore require a warrant. The questions that then arise regarding IP space is whether the traditional tests of privacy still apply, or if they are outdated when pertaining to digital information.

When the government needs to access information that is critical to national security, is it able to do so effectively under current restrictions, or are those restrictions hindering the government from protecting the American public? Although the overall legal structure for addressing this issues is considered to be "patching and in critical ways outdated,"[5] an effort can still be made to understand the most important laws currently in place and the areas of IP space in which they limit government access. Understanding what is currently in place will help construct a

theoretical framework for how the U.S. currently views privacy in the digital age, allowing firms to better understand how they can navigate that framework.

What Information is at Stake?

As cyberspace continues to advance and expand, so too does the amount of personal information that is available on digital platforms. Information that has historically been kept in purely physical form, such as written communication between individuals, is now conducted widely over the Internet. The storing of documentation on digital platforms, often containing sensitive information, has become commonplace. This paper will separate digital data into three categories: U.S. Person Information (USPI), Personally Identifiable Information (PII), and Digital Assets.

U.S. Person Information (USPI)

Information that is obtained through intelligence collection and analysis is governed by various regulations on how it can be gathered, depending on where it is obtained and to whom it belongs. If the information gathered is USPI, intelligence agencies will face additional prohibitions and restrictions on that information.[6] A U.S. person is defined under the U.S. Code (U.S.C.) and through Executive Order (EO) as being "a citizen of the United States; an alien lawfully admitted for permanent residence; an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence; or a corporation that is incorporated in the U.S."[6]

Department of Defense Manual (DoDM) 5240.01 broadly describes the kind of information that is included as USPI as "reasonably likely to identify one or more specific U.S. persons:"

> "USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional. USPI is not limited to any single category of information or technology. Depending on the

> context, examples of USPI may include: names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and Internet Protocol address information."[7]

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) does not differ greatly from USPI in substance, but its definition makes it more widely applicable. While restrictions on USPI are primarily in the realm of intelligence gathering, PII can exist wherever interactions between government entities and individuals interact. The Department of Homeland Security (DHS) defines PII as:

> "Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department."[8]

Additionally, PII can be classified as "sensitive" information. This includes data, such as credit card account information, that if obtained by a malicious actor could lead to harm such as fraud or identify theft.[9] DHS provide the following definition for such data:

> "Sensitive PII (SPII) is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."[8]

It is important to note that both sensitive and non-sensitive PII are commonly collected by both private and government entities.[10] This information is typically provided voluntarily by the individual when they sign a terms of agreement document or make a purchase from a website, or when they must provide it as a requirement for a new job.[9] From a practical standpoint, this means that PII is pervasive across the entire digital spectrum, interacting with citizens over the course of daily activities when the make an online purchase, create an online account, or accept employment with a firm that maintains digital employee records.

Digital Assets

Digital data can also fall under the definition of digital assets, in accordance with the legal structures and definitions established under the Uniform Digital Assets Law (UDAL). Under this law, digital assets encompass all "electronic record in which an individual has a right or interest."[11] Communications in electronic form, documents that are kept on cloud-based systems or on hard drives, cryptocurrency, and even social media accounts are all included in this definition.[11] The proliferation of digital assets has created hurdles in the ability of the government to protect individuals and their information without violating their right to privacy. Documents that might aid in a national security situation, even when they do not refer to any specific individual, might still fall within the definition of a digital asset. This type of information is further complicated by the emergence of cloud-based systems, which allows for large amounts of digital assets to be kept on Internet-based servers. The Federal Bureau of Investigation (FBI) identifies two unique issues regarding digital assets:

> "Executing law enforcement searches in a cloud-computing environment presents a twofold problem. First, little, if any, data pertaining to a computer user is found in a single geographic location. Second, and more important, even when the data is recovered, it may not be able to be converted to a format understandable by a human reader."[12]

The emergence, proliferation, and evolution of digital data technologies has forced privacy law to also evolve. To navigate the complexity this creates, the Federal Government has implemented laws and policies that have formed the current structure of privacy law. Although this structure is primarily built on congressional acts and Executive Branch policies, the court system has also developed extensive case law that has helped shape this system.

Digital Information's Impact on Policy

The emergence, proliferation, and evolution of digital data technologies has led to the creation of new privacy law.[13] The government has responded with laws and policies that have attempted to navigate these new digital complexities, ranging from legislation passed by Congress to rulings

handed down by the U.S. Supreme Court.[14] One of the primary goals of this report is to summarize and discuss a few key laws and policies.

How the U.S. Has Historically Handled Personal Information Data Collection

Historically, the U.S. has handled the collection of data containing USPI more loosely when compared to contemporary data protection protocols. Personal data has not always been legally protected, and intelligence agencies have not always been as restricted and under the same amount of oversight for conducting surveillance on U.S. citizens as they are currently. In the 1960s and 1970s, intelligence agencies such as the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Security Agency (NSA) surveilled domestic civil rights movements and anti-government protests and conducted covert action against foreign leaders and U.S. citizens, specifically through NSA wiretaps on Martin Luther King Jr.[15] and other political activists as revealed through the Church and Pike Congressional Committees.[16] In wake of the Watergate scandal, Congress investigated these intelligence agencies for evidence of potential intelligence abuse, finding that these agencies had conducted unlawful tactics for intelligence gathering, including illegal wiretaps, secret bugging, and harassment of U.S. citizens. These findings were used as the basis for establishing legislative oversight of the intelligence community (IC), to demand more accountability, through the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).[16] The findings were also instrumental in the creation of the Foreign Intelligence Surveillance Act (FISA) in 1978.[17]

There are specific policies currently in place that provide the government with specific and restricted authority to conduct intelligence operations on U.S. citizens and to collect data that includes USPI,[6] such as EO 12333 and FISA. These policies also apply to IP space, and it is the overwhelming presence of U.S. citizens activities within IP space that complicates federal defensive and intelligence-gathering activities, particularly for DoD and especially when USPI is involved. The rules under which DoD operates within IP space were originally established based on historical signal intelligence (SIGINT) collection and included the principles of Computer Network Operations (CNO), Computer Network Defense (CND), and Cyber Network Attacks (CNA), terms the U.S. military used to describe its activities in IP space.[18]

CNE is a broad military concept that allows the military to use computer networks to "gain strategic advantage" in the military paradigm.[19] This acknowledges that knowledge is power, and indicates that increasing the amount of information that can be collected regarding a potential adversary will better allow the military to make strategic decisions. CNE enables civilian and military organizations to protect, defend, and retaliate against malicious computer operations from enemy networks.[20]

CND is a set of processes and defense measures used to protect computer networks against infiltrations resulting in denial of service and server disruption. This term describes the actions taken within DoD to "protect, monitor analyze, detect and respond to an authorized activity within DoD information systems and computer networks."[21] A CND utilizes and allows for computer networks to execute offensive operations against enemy computers and networks.[22]

DoD defines a CNA as "the actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[23] These three terms (CNE, CND, and CNA) frame the discussion and form the terminology by which DoD operates within IP space, and define the activities in which they are authorized to engage. This baseline knowledge of DoD operations and the legality of operating within IP space is essential in determining if DoD is restricted in operating within U.S. IP space.

Policies by Which the Federal Government Must Abide

A full analysis of the means by which DoD is restricted in acting within U.S. IP space requires examining the following laws, policies, and acts:

- Fourth Amendment of the U.S. Constitution
- Department of Defense Manual 5240.01
- Executive Order 12333
- Title 10 of the U.S. Code
- Title 18 of the U.S. Code
- Title 32 of the U.S. Code
- Title 50 of the U.S. Code

- Foreign Intelligence Surveillance Act
- Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act (USA Freedom Act)
- Computer Fraud and Abuse Act
- Privacy Act of 1974

The U.S. Constitution establishes the fundamental rights and civil liberties of U.S. citizens, on which Congress has based legislated restrictions on the authority and ability of the Federal Government, in particularly DoD, to protect these rights and liberties. As discussed previously in this chapter, the Fourth Amendment establishes "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…"[2] This right has been interpreted by American citizens to apply to U.S. persons within IP space as well, protecting their digital persons and effects against unlawful search and seizure through interpretation that electronic surveillance is a form of search covered by the Fourth Amendment.[23] Through the interpretation of case law, such as *Katz v. United States* and *Smith v. Maryland*, discussed later in this chapter, there is a reasonable expectation to privacy regarding communication methods that is constantly challenged.

Department of Defense Manual 5240.01

Department of Defense Manual (DoDM) 5240.01, issued in 2016, "establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons."[24] The manual provides internal guidance and establishes internal procedures by which DoD Intelligence Components are to outline the collection, retention, and dissemination of USPI as well as the appropriate methods for electronic surveillance, concealed monitoring, physical searches, the searching of mail and use of mail covers, physical surveillance, and undisclosed participation in organizations. To intentionally collect USPI, a DoD Intelligence Component must first confirm that the information to be collected is reasonably believed to assist the mission given to them and that the information falls within one of the following 13 categories.[24]

1. Publicly available
2. Consent
3. Foreign intelligence
4. Counterintelligence
5. Threats to safety
6. Protection of intelligence sources, methods, and activities
7. Current, former, or potential sources of assistance to intelligence activities
8. Persons in contact with sources or potential sources
9. Personnel security
10. Physical security
11. Communications security investigation
12. Overhead and airborne reconnaissance
13. Administrative purposes

Retention of USPI in DoD networks depends on whether the information was intentionally or incidentally collected, if it was voluntarily provided, if there were any mitigating special circumstances, or if the information requires extended retention.[24] Further, dissemination of USPI collected or retained by a DoD Intelligence Component is allowed only if specific conditions are met. The authority to conduct electronic surveillance is dependent on the mission, the status and location of the U.S. person, the methods used to conduct the surveillance, and the specific type of communication sought, and must also comply with the Fourth Amendment.[24] A DoD Intelligence component may conduct surveillance targeting a person in the U.S. only for foreign intelligence or counterintelligence purposes.[24] The complexity of the procedures in place is apparent. These authorizations and limitations, established in DoDM 5240.01, form the basis for internal oversight of intelligence activities, which will be further discussed later in this chapter.

Executive Order 12333

Another source that helps define the authority of the U.S. government regarding data collection is EO 12333. Issued in 1981, EO 12333 is one of the primary documents that permits intelligence agencies to conduct surveillance activities, as well as collect, retain, and disseminate information

gathered under those activities. Specifically, the NSA uses EO 12333 to establish its legal authorization for un-encrypting information and collection of USPI.[25] In accordance with priorities set by the president, EO 12333 allows for the "…collection of information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction (WMD), intelligence activities directed against the U.S., international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents."[26]

United States Code

The appropriate framework for DoD by which DoD coordinates with other government entities to respond to acts of war will also depend on the different title classifications under which they fall. Title 10, Title 18, Title 32, and Title 50 all provide legal classifications for military or law enforcement agencies to fulfill specific duties and functions.

The U.S. Code (U.S.C.) provides the legal authority by which military and law enforcement agencies are governed during times of war and peace. The Title that authorizes a specific department's functions under will change depending on the functions that department will perform, so a single department could fall under any of a number of separate Titles depending on the specific situation.

Title 10 of the U.S. Code

Title 10 of the U.S.C. outlines the basic role of the armed forces. It provides the legal basis for their respective missions and organizations, the constitutional basis of which is derived from Articles 1 and 2. Title 10 governs active duty forces and is used to conduct military activities and articulate the basis for military operations where the primary mission is national defense. Oversight of Title 10 lies with the House and Senate Armed Services Committees. Active duty forces governed by Title 10 are paid with federal dollars and their orders originate from the President and are then executed through the Combatant Commands. Title 10, Section 111 states that it will "man, train and equip U.S. forces for military operations in cyberspace."[27] Therefore, military operations in cyberspace are an authorized activity for Title 10 forces.

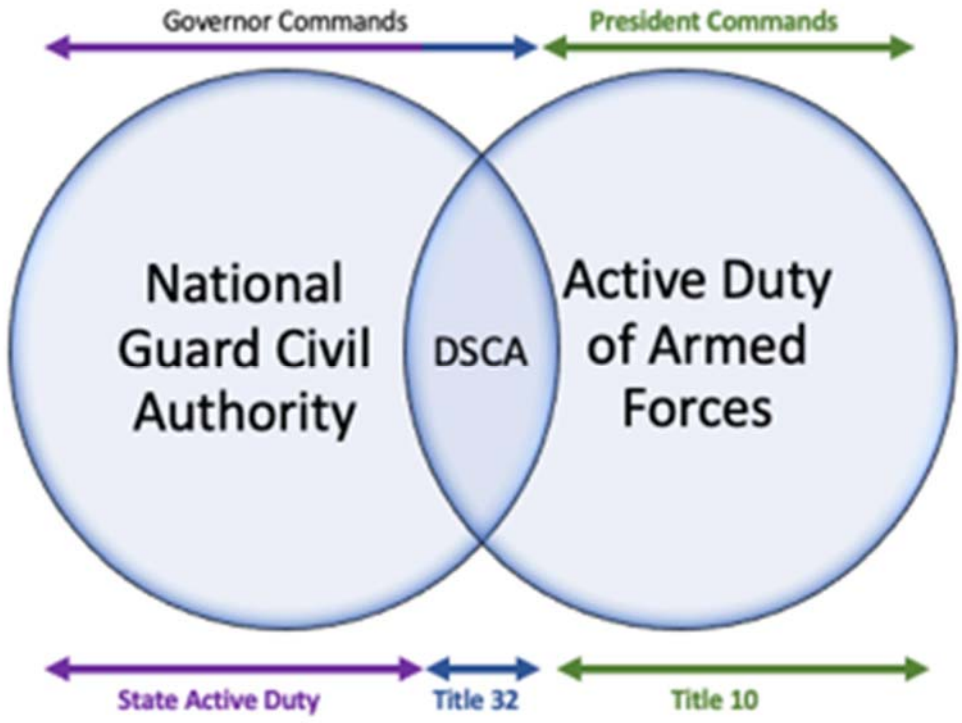
Title 32 of the U.S. Code

Title 32 of the U.S.C. and how it classifies the National Guard is a bit more complex when compared to other National Guard statuses: state active duty, active duty, or the mobilization/federalization. Under the command and control of the state governor, but paid by the Federal Government, forces authorized under Title 32 are utilized in response to natural disasters, large domestic attacks (e.g. 9/11 or the Oklahoma City bombing), training, and other Federally-authorized activities. If the National Guard operates under Title 32, they are not affected by the provisions of the Posse Comitatus Act, a Federal statute that prohibits the government's ability to use the military as a police force,[1] in any way, unless they operate under Title 10 authority. Operation Noble Eagle, the Federal Government's initial response to 9/11, is a primary example of a Title 32 action: It began with the mobilization of thousands of National Guardsmen to perform security detail for military installations, airports, and other potential targets. The mobilized units also provided defense and security around the White House, the Pentagon, the Capitol Building, and other government structures deemed as "high risk" for further attack.[28]

Figure 3-1 outlines the differences between Title 10 authorization for the active duty of the armed forces and Title 32 National Guard civil authority. When the National Guard for an individual state operates under state active duty status, the state governor commands their activities and the state pays for operations. National Guards can also operate under Title 32 authorization. In this case, the governor retains command of the National Guard but the Federal Government pays. For example, under Title 32 authorization, National Guard units can train for future overseas deployments and conduct disaster response operations. Again, these activities would be conducted under state authority but would be funded using Federal funds. Another example of National Guard operations under Title 32 authorization is their deployment along the U.S.-Mexico border in support of Customs and Border Control.

Title 10 controls Federal active duty forces, which can include the Reserves. The National Guard, when federalized, also falls under Title 10 authorization with the President serving as the Commander in Chief. The Federal Government would also financially support this activity.

Figure 3-1 Title 10 and Title 32 Authorizations



Title 50 of the U.S. Code

Title 50 of the U.S.C, entitled "War and National Defense in the United States," comprises the National Security Act of 1947 and outlines the U.S. national defense and security agencies and organizations as well as restructuring defense and intelligence agencies. When acting under Title 50 authorization, defense and intelligence agencies are only obligated to comply only with the U.S. Constitution and domestic statutes; they are not obligated to comply with international law.[29] The 2011 raid on Osama bin Laden's compound that resulted in his death is an example of a direct execution of Title 50: the Joint Operations Command planned and directed Seal Team 6 to operate under Title 50 authorities due to the classification and direct authority of the operation.[30] Most intelligence agencies operate under Title 50 authority, while the Defense Intelligence Agency (DIA) and NSA specifically operate under both Title 10 and Title 50 authorities. Under Title 50, the Secretary of Defense (SECDEF) possesses the overarching authority and directs U.S. government operations against unconventional threats, including cyber threats. Section 3093 of Title 50 also directly addresses U.S. IP space by authorizing agencies

and departments to “Secure U.S. interests by conducting military and foreign intelligence operations in cyberspace.”[27]

Title 18 of the U.S. Code

When examining military operations in U.S. IP space, including collecting USPI, it is important to also consider law enforcement authorizations and procedures. Title 18 of the U.S.C. contains the statues for domestic law enforcement agencies and defines the different crimes and corresponding criminal procedures. The statutes that are directly applicable to the scope of this research are Section 1385, which establishes authorization for the use of Army and Air Force personnel under Posse Comitatus, and Section 3052, which authorizes the FBI and their special agents and officials to make arrests, carry firearms, and serve warrants.

Table 3-1 outlines the various Titles of the U.S.C. discussed above and their corresponding authorization for military and law enforcement and intelligence agencies, their command and controller, oversight officials, their mission, funding sources, restrictions, and authorizations.

Table 3-1 Applicable Titles of the U.S. Code for Defense and Law Enforcement

	Title 10	Title 18
Name	Active Forces, Armed Forces, Department of Defense	Posse Comitatus, Law enforcement. Federal Government not state (DPS) describes criminal statutes/etc.
Command and Control	President	Depends on the department, secretary, or level of government the Title 18 force is under
Oversight	Senate Armed Services Committee, House Armed Services Committee	President and the Cabinet secretary have direct oversight, and the President has oversight over Cabinet secretaries. If it is an agency, it reports through the Executive Branch. Congress always has oversight over laws, but no operational control here
Mission Types	National defense	Wiretaps for law enforcement. Authorizes FBI. Ends use of Federal troops in law enforcement. Law enforcement war on drugs. Prohibits law enforcement by military. Emergency situation of WMD
Funding Source	Federal	Local law enforcement by state sale and income tax, funding authorized by Congress of major departments as well
Restrictions	Posse Comitatus, limited domestic law enforcement operations. Must abide by international law compliance	FISA restrictions
Authorizations	Article 1 and 2 of U.S. Constitution	-

Table 3-1 Applicable Titles of the U.S. Code for Defense and Law Enforcement

	Title 32	Title 50
Name	National Guard	War and National Defense, National Security Act of 1947
Command and Control	State Governors	SECDEF
Oversight	President, SECDEF, Senate Armed Services Committee, House Armed Services Committee	Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence
Mission Types	In service of the Federal Government: hazards, disasters, and emergencies	Covert action, Intelligence communities, bin Laden raid, doesn't acknowledge publicly and isn't traditional military activities
Funding Source	Federal	ODNI reviews the budgets of the IC and distributes from there
Restrictions	Federalization event of NSSE no problem with Posse Comitatus, International law compliance	Doesn't have to comply with international law, but civil rights of American citizens must be considered.
Authorizations	Article 1, Section 8 of U.S. Constitution	-

Foreign Intelligence Surveillance Act (1978)

FISA, enacted in 1978 by Congress, is another document that limits the extent to which U.S. intelligence agencies can monitor the communications, including digital, of U.S. citizens. The act establishes the Foreign Intelligence Surveillance Court which permits the use of wiretaps and monitoring of foreign agents and adversaries within the U.S. In 2008, Congress added the controversial Section 702 to the act, which allows warrantless monitoring of communications by foreigners in the U.S. and abroad,[31,32] which in turn picks up communications of Americans who are communicating with those foreign agents. This becomes controversial when U.S. citizens' information gets swept up with the intelligence collection.

FISA protects U.S. citizens against espionage, sabotage, and attacks by monitoring individuals suspected of such activities. Section 702 allows intelligence agencies to collect foreign intelligence from non-U.S. citizens located outside the U.S. Because of this provision, it is believed that large scale collection of communications of U.S. citizens has incidentally occurred.[33,32]

The USA Freedom Act (2015)

The USA Freedom Act imposes limits on the bulk collection of metadata of U.S citizens by intelligence agencies.[34,35] The act was passed in 2015 in response to the Edward Snowden information leak that exposed questionable programs run by the NSA to collect USPI.[36] This act ends bulk collection of all records authorized under Section 215 of the Patriot Act.[37] In response to the provisions of the USA Freedom Act, tech companies became more aware of their legal responsibility to protect user data they collect and their relationship with the government. When it comes to understanding the restrictions placed on the Federal Government, the inability to collect bulk data is an important aspect to be remembered.

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act of 1984 is used to address digital privacy and cybersecurity by identifying as a federal crime the unauthorized accessing or hacking a protected computer without acceptable warrants and permission.[38] After being amended in 1994 to more broadly

include protections of the private sector, private companies began citing this act to protect their trade secrets and economic information and sensitive/protected research.[39] The provisions of the act were originally designed to protect the information systems and databases of the U.S. government; following 9/11, the Patriot Act expanded the scope of the Computer Fraud and Abuse Act to better adapt to emerging threats by expanding the scope of computer crime.[38] The complexities of this act play an important role in cybersecurity, laying a foundation for jurisdiction between the Federal Government and private sector entities when it comes to hacks.

The Privacy Act

The Privacy Act of 1974 established a code of fair information practices by governing the collection and dissemination of U.S. citizens' information that is maintained by Federal agencies, including tax returns and PII.[34,40] The Privacy Act places restrictions on the accessing of U.S. citizens' information and requires that certain procedures be followed whenever this information is. This is important in the framework of government restrictions as it places severe yet important safeguards around individual's information. The purpose is to balance national security concerns with personal safeguards and privacy, and to maintain transparency regarding the information the Federal Government has on its citizens.

Case Law

To fully understand the current U.S. policies surrounding the security of personal information, the relevant case law must be evaluated. When discussing case law, it must be viewed from the perspective of: 1) What the court has said regarding previous, specific situations where Fourth Amendment protections were challenged; and 2) The impact these cases may have on future policy. Viewing case law through this lens can provide a picture of how policy must be formed to fit within the precedent set by those cases can begin to form. This report will examine case law in two sections to better form a basic understanding for potential future policy. The first section will briefly discuss some key aspects of privacy law from the judicial perspective and how some cases have shifted that law. The second section will break down four cases that the authors of this report have chosen as examples of how the court has previously responded to specific issues regarding Fourth Amendment protections. Again, each of these sections will be

viewed through the lens of the impact on potential future policy, particularly how the court might resolve constitutional challenges and ambiguities contained within future laws. While this summary of case law is not meant to be exhaustive, the examples discussed herein can help to understand the impact the court system has had on privacy law.

Brief History of Key Decisions

Many cases decided during the 20th century regarding privacy focused on physical items and provided the foundation for what is now referred to as colloquially as "privacy law," which has been more recently expanded to include digital aspects. Although the discussion of non-digital aspects of privacy law are not within the scope of this report, a brief summary of how the courts have historically interpreted privacy law is important.

Challenges to what falls within the purview of the Fourth Amendment have been pervasive, ranging from the famous *Weeks v. United States* case of 1914 to the more recent ruling in *Safford Unified School District v. Redding* in 2009,[41] and many more in between. One of the biggest debates that has arisen through these cases has been deciding what falls within the limits of requiring a warrant, based upon probable cause, before being searched or seized. As a response to this debate, the two-pronged test was created, as discussed further in the *Katz* case below. When an individual's privacy in a certain place, action, or item was questioned, that situation would be covered under Fourth Amendment protections if both the *individual* and *society* (emphasis added) believed that a reasonable expectation of privacy existed in that situation.[42,43]

This two-pronged approach was created in the ruling of *Katz v. United States* (1967), where the U.S. Supreme Court ruled that both individuals and society at large expect a reasonable amount of privacy when entering a phone booth.[42] An additional example of the discussion surrounding this test is *United States v. White* (1971), in which the Supreme Court ruled in that when a person invites someone else into their home, the homeowner gives up any reasonable expectation of privacy for what is said in the presence of the other person.[42] The *White* ruling has since formed the legal foundation for allowing an informant to wear a recording device to gather information that admissible in court. Lastly, two important cases, *United States v. Miller* (1939) and *Smith v. Maryland* (1979), were both used to establish the precedent that once an individual grants access

to someone else regarding their sensitive information, such as bank records, address, or phone number, that individual no longer has a reasonable expectation of privacy for that information.[42]

More recent cases dealing with emerging technologies have been forced to consider both new and old interpretations regarding privacy. Some of these cases are based on the precedents set above, while others have established new precedents. While there are many cases related to this issue that could be discussed, the following cases were specifically included in this discussion due to their strong importance and direct relevance to the development of digital privacy. The importance and relevance of the cases will be further discussed later in this report.

Carpenter v. United States (2018)

One of the most recent decisions that directly contributes to the discussion of digital privacy was handed down by the Supreme Court in *Carpenter v. United States*. In this case, the Court ruled that an individual's location data, collected by a cellular company, could not be obtained by the Federal Government without a warrant.[44] This case is crucial to the development of privacy laws in the digital age as it applied Fourth Amendment protections to digital information held by a third party, in this case, the cellular company.[44] This case established a precedent for restricting the government in gathering information from third-party cellular companies. The majority opinion of the Court prescribed that the location information of an individual belongs to the individual at all times, therefore falling directly within the limits of the Fourth Amendment.[45]

In the future, this could potentially extend to other third-party entities like Facebook, Twitter, online forums, and email servers. However, it is possible that the Court may rule differently in the future as Justices Kennedy, Thomas, Alito, and Gorsuch each individually dissented on this case. The essence of their various dissents was that the data was voluntarily given up by the individual to the cellular company, therefore making the company, not the individual, the owner of the data.[46] These two varying viewpoints will have a critical impact on how the government will be able to treat personal information and may be contentiously debated in the future.

United States v. Ackerman (2018)

Similar to the *Carpenter* case mentioned above, *United States v. Ackerman* also involved data from a third party, but this case took a slightly different direction. In the case of *Ackerman*, the email provider AOL discovered, through its internal filtering systems, that the plaintiff had sent incriminating evidence through the email system. AOL flagged this content and sent this information through an intermediary to law enforcement. The individual argued that his emails were protected under the Fourth Amendment and therefore the government should not have been able to access them without a search warrant, even though they were voluntarily given to the government. The government argued that the plaintiff violated AOL's terms of agreement by sending illegal content over their servers, and therefore had no expectation for privacy of his emails. The Supreme Court ruled against the plaintiff.[46]

Through this decision, a precedent was set that could allow for private companies to use their terms of agreement as protection against criminal activity and threats to national security. In the event that a private company discovers that their digital platform is being used for criminal activity, the ruling in *Ackerman* helped establish the possibility for them to begin providing that information to law enforcement, which will remain admissible in court.

Riley v. California (2014)

This case was critical for digital privacy as it confirmed a precedent set in a previous case, *United States v. Jones* (2012), which found that installing and using a global positioning system (GPS) to track a citizen constituted a search under the Fourth Amendment. In *Riley*, the Supreme Court found that law enforcement could not search an individual's phone without a warrant after an arrest.[43] Since this was the first case in which the Court specifically addressed electronic devices, the ruling helped establish that digital information on a phone is protected under the Fourth Amendment.[43] Since previous case law had established that items on a person could be searched after an arrest, this was a major step forward in defining the boundaries of digital privacy. The Riley case did this by clarifying that due to the large amount of information contained on a device, a warrant was needed to access that device.

United States v. Verdugo-Urquidez (1990)

This case is the oldest of those included in this report and does not directly deal with digital, but its importance on the overall discussion surrounding digital data and privacy cannot be understated. In the *Verdugo-Urquidez* ruling, the Supreme Court ruled that Fourth Amendment protections only apply to non-citizen individuals with strong voluntary connection to the U.S.[3] This means that searches and seizures of foreign individuals do not require a warrant. The precedent set by this ruling has massive potential implications for digital information. Since IP space is increasingly creating a "global" connection, with communications and more from foreign individuals intersecting with those of U.S. citizens, the issue can be raised as to whether Fourth Amendment protections apply to communication that occurs between a U.S. citizen and a non-U.S. citizen.[3] This case has established a precedent, which can potentially be used in cyber situations on a case-by-case basis, to determine whether the individual in question, usually a non-citizen, has a strong connection to the U.S. That answer can be used to decide whether Fourth Amendment protections apply.

Other Cases with Future Policy Implications

The cases described above provide good examples of why case law must be taken into consideration when discussing the issue of privacy and digital information. However, these are not the only cases that could be discussed. The following cases also each deal with the issue of privacy in some way, and form a good primer on case law for privacy and Fourth Amendment protections.

- *Safford Unified School District v. Redding*, 557 U.S. (2009)
- *Vernonia School District v. Acton*, 515 U.S. 646 (1995)
- *Skinner v. Railway Labor Executives Association*, 489 U.S. 602 (1989)
- *New Jersey v. T.L.O.*, 469 U.S. 325 (1985)
- *United States v. Robinson*, 414 U.S. 218 (1973)
- *Terry v. Ohio*, 392 U.S. 1 (1968)

Summary of Judicial Influence on Privacy Law

Generally speaking, many of the same Fourth Amendment protections that have existed for physical items have been transferred to the new digital world when it comes to personal property and the expectation of privacy. The two-pronged test for reasonable expectation of privacy is still used, although digital situations have yet to face this test. Many of these parameters are still being discovered and defined. The courts will likely have a busy few decades ahead of them, which means that close attention will need to be paid by anyone connected with the cyber world. Each new ruling that is handed down will shape the overall legal infrastructure, which could last for decades before seeing substantial change. The cases listed above are not exhaustive, but were included to illustrate the type of decisions that are being made. As it stands, there are few pieces of information in the digital realm that remain completely immune to possible search and seizure. Under the reasoning in the cases above, the Federal Government can access nearly all information available in the IP space, so long as the proper methods of obtaining a warrant are followed.

Findings - Is DoD Over Restricted?

The difficulty in the U.S. government's ability to operate in U.S. IP space for national defense is the prevalent activity and presence, as well as the vast amount of personal information, of U.S. citizens within IP space. This is not a flaw of the system, but rather an inherent characteristic. There are specific Federal Government policies in which DoD, DHS, DOJ, law enforcement, and state and local government laws must abide by. What exactly does this look like though, when it comes to real world actions by these Federal entities? How are the above policies, which delineate where and how intelligence agencies can operation, practically followed?

It should be noted that while there are many internal policies and manuals that direct the activity of each Federal agency, this report will only examine the major laws, policies, statutes, and case law discussed previously in this chapter and describe how each contributes to the restriction of DoD operations within IP space. This section will consider the complexity of the interworking nature of the major laws governing this industry and summarize the combined impact on DoD.

First, there are tangible ways in which DoD is restricted when operating within U.S. IP space while assisting DHS in protecting critical infrastructure. If DoD attempts to assist DHS while operating under Title 10 authority, it is restricted from collecting information on U.S. citizens and therefore is restricted from collecting any data, as it may inadvertently collect information on U.S. citizens in the process. In order to support civil authorities, including in law enforcement or in a defensive capacity, they must be authorized. Though potentially troublesome, this scenario provides the potential to institute a protocol for interagency cooperation to allow both agencies to access and use the information. The National Guard has some form of cybersecurity capabilities and expectations in all 50 states.

The issue then arises as to the restrictions specifically concerning U.S. Cyber Command operations in U.S. IP space, which will depend on what operations are being conducted and the location in which they are conducted. If U.S. Cyber Command is conducting operations under Title 10 authorization, and these operations extend beyond the "boundaries" of U.S. IP space, the operations would fall under the jurisdiction of international law, including the General Data Protection Regulation (GDPR), and would require compliance with other international legal obligations in cyberspace. If operations are conducted under Title 50 authority, however, there is no legal responsibility to comply with international law; they must only comply with the U.S. Constitution. Title 50 authorization is frequently for covert action, exemplified by the raid on Osama bin Laden's compound.

The restrictions on DoD operations in cyberspace are specific under Title 10 authorization but under Title 50 authorization there is a wider scope of authorizations and operational activities with different oversight. U.S. Cyber Command and NSA are each authorized under both Titles, so they have authorities and breadth of both. These restrictions can be avoided and passed around if components of the IC work hand in hand with the FBI or local law enforcement in fusion centers or intelligence sharing spaces, so the tradeoff of information and authorization would flow smoothly.

Policies cannot keep up with the current speed of technological innovations. Policies have bureaucratic red tape, requiring time to pass each one of them. The rules and regulations that establish restrictions on DoD regarding acquiring and collecting USPI will change depending on

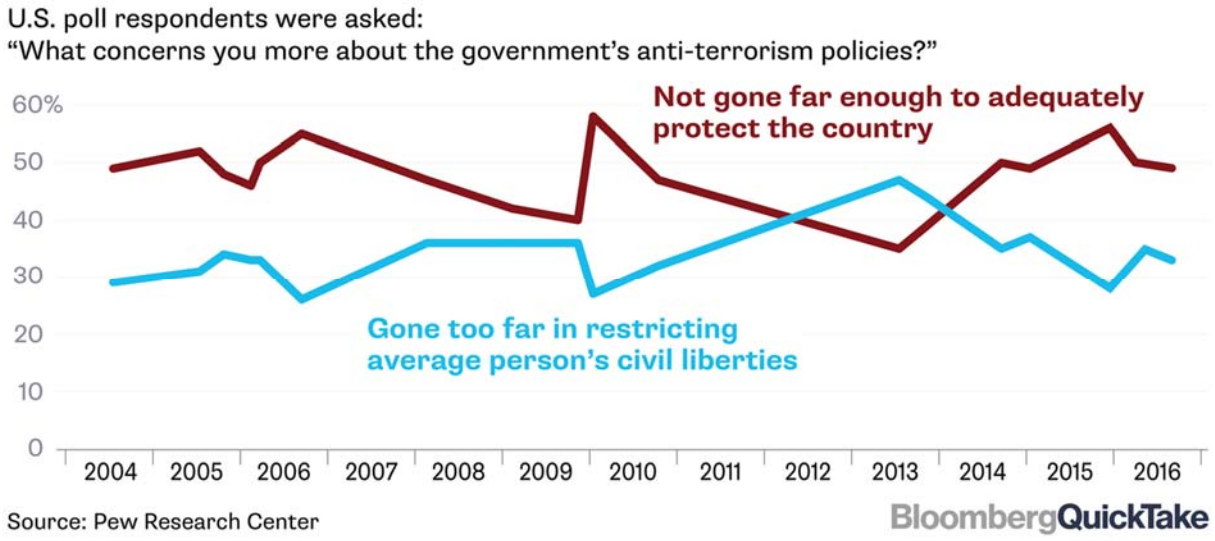
the citizenship classification of the person. For example, a foreign individual who has a U.S. physical address is classified as a U.S. person, and therefore the collection of that individual's USPI is not legal unless the DoD abides by the requisite rules and regulations. Within cyberspace, an individual located outside the U.S. can fake an IP address as being located within the U.S. DoD cannot analyze USPI without a specific mission that requires this analysis and a procedure or category which allows for the analysis to occur. This makes the current policy framework strict, but not over-restrictive. There are policies in place to protect the privacy and civil liberties of U.S. citizens but these policies are not over-restrictive. What could be considered potentially over-restrictive of DoD operations in cyberspace is the bureaucratic process of the Federal Government. However, this discussion is outside the scope of this research.

Understanding the Complexity of Future Action

The Security vs. Privacy Debate

Determining whether the Federal Government is over-restricted in U.S. IP space requires an understanding of the underlying debate that causes those restrictions and the complexities that debate creates. The core of the debate centers on differing opinions as to what is most important: privacy for individuals or the security of the nation. The difficulty in shaping relevant policy around this issue is that this opinion can and often does shift with time. Moreover, different groups of individuals often have competing goals. **Figure 3-2** presents two sets of polling data from the Pew Research Center.[47] The poll results show that U.S. citizens think the government has not gone far enough to protect the country from terrorist threats, while simultaneously believing that the government should not monitor communications of U.S. citizens. The electorate does not believe that the government has done enough to protect the country, but they also do not want to cede more power to the government to monitor individual communications, even when necessary to protect the government. This contradictory nature of the electorate can make it difficult to find a balance when creating policy on privacy.

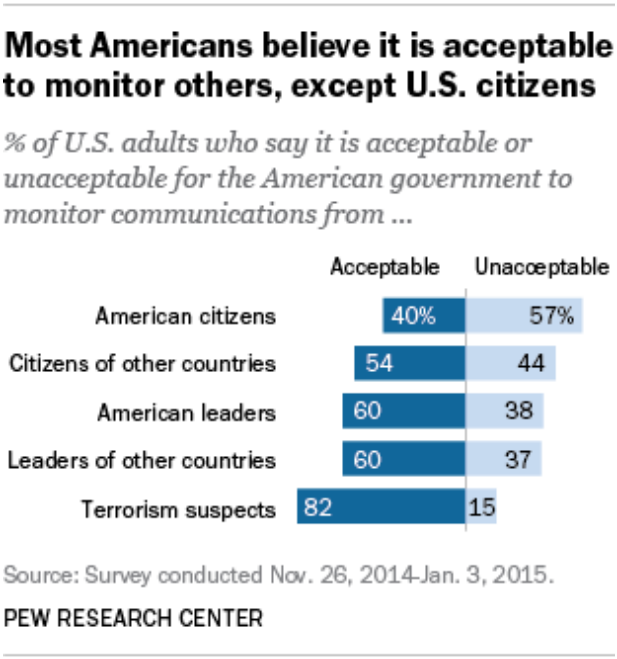
Figure 3-2 Weighing Security Against Privacy[47]



When framed in the perspective of anti-terrorism policies, data collected by the Pew Research Center between 2014 and 2015 revealed that a majority of the individuals polled believe that current U.S. policy has not adequately protected the country from terrorism, with a slight exception in 2013.[47] Other data sets collected have indicated that most Americans believe it is unacceptable to monitor communications from U.S. citizens.[48] These results are presented in **Figure 3-3**. It should be noted that these results show that public opinion on monitoring changes greatly depending on the target population group.

This privacy challenge does not only apply to concerns over active surveillance. Recent polling data has shown that users of mobile devices are hesitant to access government services on their mobile devices out of fear that the government will begin collecting their data.[49] This would imply that ease of access is not always worth the perceived cost to privacy for many people when the government is collecting the data.

Figure 3-3 How Americans have viewed government surveillance and privacy since Snowden leaks[48]



The desire for individual privacy must be balanced against the Federal Government's ability to fulfill its primary role and responsibility of ensuring the safety of the nation and its citizens. As IP space continues to advance and expand, so too does the complexity of ensuring that the government has the adequate tools necessary to combat emerging cyber threats. According to the Congressional Research Service,

> "Because modern-day criminals are constantly developing new tools and techniques to facilitate their illicit activities, law enforcement is challenged with leveraging its tools and authorities to keep pace. For instance, interconnectivity and technological innovation have not only fostered international business and communication, they have also helped criminals carry out their operations. At times, these same technological advances have presented unique hurdles for law enforcement and officials charged with combating malicious actors."[50]

Examples of these technological developments have been discussed previously. One of the more well-known examples was the subject of a recent controversy between the government and

Apple, when encrypted iPhones could not be accessed by officials investigating the terrorist attack in San Bernardino, California.[51] There are many ideas that have been proposed as a means to address these new challenges, some of which are far-reaching in their effect (proposals to ban outright any encryption of data that does not allow access to law enforcement being one far-reaching example).[50] Seeking a balance between maintaining privacy and security creates a difficult policy dilemma. Understanding that this dilemma exists, and the parameters that have so far been set, is the first step in evaluating possible recommendations.

Federal Actions to Accommodate this Debate

In the wake of the Edward Snowden leak in 2013, through which details of the NSA's collection of U.S. citizens' data was exposed, the issue of privacy has been frequently addressed in political discussions.[47] Although the evidence released by Snowden caused Americans to view government surveillance more disapprovingly,[48] the government has not remained silent on the topic. Strategies such as the 2018 DHS Cyber Security Strategy (DHS CS) have recognized that the issue of privacy is important:

> "DHS must uphold privacy, civil rights, and civil liberties in accordance with applicable law and policy. The Department empowers our cybersecurity programs to succeed by integrating privacy protections from the outset and employing a layered approach to privacy and civil liberties oversight."[52]

The creation and use of "Chief Privacy Officers," along with the implementation of standards tasked to those officers,[53] are examples of how the Federal Government is trying to uphold privacy, civil rights, and civil liberties in accordance with applicable law and policy. These Chief Privacy Officers, typically executive-level managers in the private sector or upper-level employees within the government, are responsible for creating policies that protect the private data of both employees and customers.[54] Although there is no single, comprehensive law governing data collection and privacy, many sector-specific pieces of legislation, such as HIPAA (see discussion in Chapter 2), have been passed into law.[55] Whenever DoD collects PII of a citizen, it currently publishes a "system of record" to the Federal Register.[56] Even the U.S. Office of Management and Budget (OMB) has entered the discussion of privacy and security, issuing a

directive that "…requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public."[57]

These situations illustrate that the Federal Government has taken direct action to address concerns over privacy while balancing the desires of the public regarding security. The question that then arises is whether Federal agencies, specifically DoD, have been over-restricted by these measures. As discussed previously in this chapter, the research indicates that the answer is no: Although there are restrictions in place, which are inherent to our constitutionally-guaranteed form of government, the research does not indicate that DoD is over-restricted. However, there are changes to the current system that can be implemented to better secure the digital world. Chief among these potential changes is an area that is in need of research, which is the involvement of the private sector in advanced methods of cybersecurity, often in ways in which the Federal Government cannot due to jurisdictional boundaries.

The Untouchable Void

Even if the final recommendations outlined at the end of this report are considered and implemented, the Federal Government is still faced with the problem of constraints on their jurisdiction that will never go away. This "untouchable void" is the jurisdictional boundary that the government cannot cross. It most often manifests itself as the private sector, i.e. as the private sector organizations and the customers with whom they interact, as well as private citizens' interactions within IP space. The jurisdiction of government does not extend into households for daily protection; similarly, neither does it extend into the realms of the private sector. Individuals and the private sector organizations are responsible for their own individual defense against cyber threats, just as they are responsible for their individual defense against physical threats. Further, if an attack occurs against a private sector organization, that organization is responsible for the mechanism with which to respond to that threat, as well as the mitigation of damage that occurs afterward.

There is potential for a cooperative partnership to exist between the public and private sectors, but that partnership can only expand the government's jurisdiction to a small degree. The individuals and firms will ultimately still be primarily responsible for a large part of the cyber

interaction that occurs today. When a malicious actor attempts to hack a private sector organization, it is the organization that will be responsible and have the best incentive to prevent the hack from occurring. If the hack is successful, it is the organization that will most significantly feel the effects and will be left to coordinate the response. Policy decisions must then consider how to fill this void what changes are required to permit the private sector to better manage cybersecurity on its own. Publicly available and open-source research in this area is lacking, but a quick conversation on the possible advantages of the improved system should be discussed.

Can Private Contractors Fill the Void?

Based on the research conducted, the recommended method for filling this void is by encouraging the private sector to perform actions that the government cannot, as exemplified in the *Carpenter* case discussed previously in which the Supreme Court ruled that the Federal Government must obtain a warrant to access an individual's cellular location data. The private sector can collect the same data without a warrant, if the individual agrees of their own volition to relinquish that data. This voluntary relinquishing of a constitutional right to privacy is a unique and powerful tool possessed by the private sector that the government does not possess.

While the government will always be responsible for national security, there are many situations in cybersecurity that do not amount to a national security concern. An attack against a private sector organization does not necessitate government involvement, but it does require a clear framework that allows private sector organizations to respond to these attacks.

Cybersecurity, from a historical perspective, has found increasing use of private sector organizations only recently. One high-profile example of which is the 2016 hack against the Democratic National Committee (DNC). In response, the DNC turned to a private company to identify and track the hackers, which the company accomplished in just a single day.[58] As one intelligence expert explained:

> "By stepping aside to let private firms expose nation-state hackers, the U.S. government preserves its intelligence capabilities and options to retaliate. It's an informal arrangement that has been good for business and government and bad for

> state-sponsored hackers… American government agencies are often loathe to speak publicly about the origin of cyber-attacks because they fear exposing their methods of monitoring nation-state hackers. Officials commenting publicly can also undercut efforts to pursue prosecution, apply diplomatic pressure, or retaliate in other ways. So the US government has been perfectly happy to let private companies take the lead while they formulate a response."[58]

Private sector organizations are in the unique position of being able to identify hackers and publicly release their identity, without risking political ramifications. This disincentive to hacking is a tool that public entities often cannot use, for risk of political retribution. An intelligence expert describes it this way:

> "Successful attribution makes hackers' jobs harder. As the risk of getting caught goes up, the likelihood of a country conducting an attack to obtain illicit information declines. When cybersecurity firms are able to call-out nation states for engaging in data theft, destruction, and espionage, hackers and the countries that employ them must consider real costs in the form of public embarrassment and potential retribution."[58]

ODNI designates attribution, or the "identification of the actor responsible for a [cyberattack]…" as "...a critical step in formulating a national response to such attacks."[59] Private sector organizations can respond quicker than government systems that can get caught up in procedural requirements. Further, computer forensics capabilities of the private sector are developing quickly and might even become more sophisticated than U.S. intelligence agencies.[61] However, this does not come without risks. Private firms do have large incentives to succeed in this area, as demand for their services will increase with more media attention and successful attribution of future cyberattacks.[60]

Another vital cybersecurity tool which the private sector has, but the government does not, is the ability to require individuals to voluntarily surrender their data and privacy through terms of agreement documentation, as discussed in the *Ackerman* and *Carpenter* cases. While the government cannot invade an individual's privacy without a warrant, individuals can relinquish

that privacy to a private sector organization through signing a terms and agreement document. This document can contain clauses that allows the private sector organization to collect and keep PII, and it can even contain clauses that require the individual to waive their right to sue the organization in court. The government cannot force an individual to relinquish a constitutional right, but it can be relinquished of the individual's own volition.

The discussion above illustrates that there are multiple methods by which the private sector can utilize the information that they gather through terms of agreement documents and other voluntary contracts. It should be noted that although the private sector possesses the tools described above, private sector organizations working for the government often face the same or similar restrictions as government entities, meaning they do not possess these tools. Regardless, if even a small portion of the private sector is able to become self-sufficient regarding cybersecurity, it will be to the benefit of the government. Government resources are limited, and the less it is required to assist or aide the private in minor cyber-related matters, the more it can focus these resources on issues of national security. Because of this, the authors of this report argue that increasing the self-sufficiency of the private sector regarding cybersecurity will require less strain on government resources.

There is a more important aspect to this discussion though, which is the mechanism for cooperation between private and public entities. As the *Ackerman* case shows, it is possible for these private contractors to serve as filtering agents for useful, national security or criminal related information. In the *Ackerman* case, a private sector organization (AOL) found incriminating evidence on their email servers belonging to an individual. They gave that evidence to a non-profit intermediary crime reporting agency, which in turn provided the evidence to law enforcement. This model is one that can be replicated and encouraged on a large scale across the private sector, allowing government resources to focus on other areas of national security concern. As publicly available and open-source literature is sparse in this area, the coming decades will be critical for developing the empowerment of the private sector to be more self-sufficient regarding cybersecurity. Theoretically, while government operations in U.S. IP space will always be restricted, the private sector is not subject to these restrictions. This means that private sector organizations can collect, analyze, and report actionable intelligence to law

enforcement that law enforcement may never have found on their own due to restrictions faced by the government when collecting intelligence.

Conclusion and Policy Recommendations

Despite its relatively new presence in the overall scope of warfare, security, and national defense efforts, cyberspace has already become incredibly complex and elaborate. As often occurs with new issues, the current framework of laws and policies governing cyberspace, particularly U.S. IP space, has been constructed on an "as needed" basis. This means that technology develops rapidly and new threats emerge that target a very specific sector of society, to which the U.S. responds with the creation of new procedures and policies that protect that specific sector or defend against that particular threat. Though this can be an effective method of response, this method ultimately results in a patchwork of sector-specific laws, resulting in "overlapping and contradictory protections,"[55] rather than comprehensive framework for both the Federal Government and the private sector. Despite this patchwork framework, DoD does not appear to be over-restricted in their ability to conduct national defense operations within cyberspace or U.S. IP space.

Keeping this in mind, the following recommendation can be implemented in an effort to further improve the current cybersecurity framework without significantly changing operational abilities of DoD within cyberspace. This recommendation was evaluated as a potential policy proposal under the following questions: 1) The constitutionality of the policy; 2) The potential improvement to DoD operations; and 3) The most effective use of resources, i.e. allowing the private sector to handle certain aspects of cybersecurity if doing so can be done effectively and safely while allowing for scarce federal resources to be allocated to matters of national significance.

1) ***Comprehensive policy changes that clarify the extent to which the private sector can defend themselves against hacking, through the use of active cyber defense measures.*** As defined under the Computer Fraud and Abuse Act, unauthorized access of a computer is an illegal act. On a practical level, this means that if a private company is hacked, they are not currently allowed to hack-back against

the intruder, even though such a tactic would help establish attribution and develop actionable evidence that can be provided to law enforcement. Since many law enforcement agencies do not have the resources to conduct such digital forensics,[47] allowing private sector organizations to utilize hacking-back has the potential to greatly reduce the prevalence of cyber incidents. It should be noted that there is potential for negative, unintended consequences from such a measure. This was briefly mentioned in Chapter 1, and it is a concern worth noting in this conversation. That being said, this paper argues that such consequences would be outweighed by the benefits, and thus the measures would be worth implementing. Such measures have been recently proposed, like those contained within the "Active Cyber Defense Certainty Act"[61] authored by Congressman Tom Graves of Georgia. In Congressman Graves' bill, private sector organizations would be able to hack back for the purposes of establishing the identity of the hacker, disrupting the incident, or monitoring the responsible party. Further, the provisions of the bill would implement specific procedures in reporting any hack back and the corresponding active defensive measures to law enforcement. This type of legislation, if implemented, has the potential to greatly improve the current cyber paradigm by creating a right to "self-defense" of digital property. Ultimately, if such a proposal were to be implemented, and as the private sector becomes more self-sufficient regarding cybersecurity, Federal resources could be saved purely for matters of national security. This would benefit both the private sector, which would gain increased response time to threats, and the Federal Government through the saving of funds.

References

1. Rand Corporation. "Appendix D: Overview of the Posse Comitatus Act." https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1251/MR1251.AppD.pdf (March 6th, 2019).
2. Legal Information Institute. 2019. "Fourth Amendment." Cornell Law School. https://www.law.cornell.edu/wex/fourth_amendment (April 1st, 2019).
3. Kerr, Orin. 2014. "The Fourth Amendment and the Global Internet." *Stanford Law Review* 67:285. https://poseidon01.ssrn.com/delivery.php?ID=604064031098125096069114071067075103018051001046052028106016013094007109078113018069062043121044102001042025095006115103083107024070038021022095075111026006068104037021071009125086005097015068102071068024083108102119108111099094086004084024007090022&EXT=pdf (January 31st, 2018).
4. Legal Information Institute. 2019. "Expectation of Privacy. "Cornell Law Scool. https://www.law.cornell.edu/wex/expectation_of_privacy (April 1st, 2019).
5. Cate, Fred H. & Beth E. Cate. 2012. "The Supreme Court and information privacy." *International Data Privacy Law* 2(4): 255-267.
6. Central Security Service. 2018. "*Frequently Asked Questions about Signals Intelligence (SIGINT).*" National Security Agency. https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4 (January 31st, 2019).
7. Department of Defense. 2016. *DoD Manual 5240.01.* https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887 (January 31st, 2019).
8. Department of Homeland Security. 2017. *Handbook for Safeguarding Sensitive PII*. https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf (February 1st).
9. Federal Trade Commission. 2016. "Protecting Personal Information: A Guide for Business." https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (April 1st, 2019).
10. National Conference of State Legislatures. 2019. "Data Security Laws | State Governments." http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx
11. Walker, Michael. 2017. "The New Uniform Digital Assets Law: Estate Planning and Administration in the Digital Age." *Real Property, Trust and Estate Law Journal* 52(1): 52-78 (53).

12. Cauthen, John. 2014. “Executing Search Warrants in the Cloud.” Federal Bureau of Investigation. https://leb.fbi.gov/articles/featured-articles/executing-search-warrants-in-the-cloud (April 2nd, 2019).

13. The Internet Society. 2012. “Data Privacy on a global scale: keeping pace with an evolving environment.” https://www.internetsociety.org/resources/doc/2012/data-privacy-global-scale-keeping-pace-evolving-environment/ (April 1st, 2019).

14. Solove, Daniel. 2017. “The U.S. Congress is Not the Leader is Privacy or Data Security Law.” TeachPrivacy. https://teachprivacy.com/us-congress-is-not-leader-privacy-security-law/ (April 1st, 2019).

15. Christensen, Jen. 2008. “FBI tracked King’s every move.” The Cable News Network. http://www.cnn.com/2008/US/03/31/mlk.fbi.conspiracy/ (March 6th, 2019).

16. Lee, Timothy. 2013. “In the 1970s, Congress investigated intelligence abuses. Time to do it again?” The Washington Post. https://www.washingtonpost.com/news/wonk/wp/2013/06/27/in-the-1970s-congress-investigated-intelligence-abuses-time-to-do-it-again/?utm_term=.896287d17f56_(March 6th, 2019).

17. Young, Thomas. 2015. “40 years ago, Church Committee investigated Americans spying on Americans.” The Brookings Institution. https://www.brookings.edu/blog/brookings-now/2015/05/06/40-years-ago-church-committee-investigated-americans-spying-on-americans/ (March 6th, 2019).

18. National Institute of Standards and Technology. 2019. “Glossary.” U.S. Department of Commerce. https://csrc.nist.gov/Glossary/?term=3537 (March 6th, 2019).

19. Cilluffo, Frank J. 2017. “A Borderless Battle: Defending Against Cyber Threats.” Center for Cyber & Homeland Security: Testimony before U.S. House Committee on Homeland Security.https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Cilluffo%20Testimony%20for%20HHSC%203-22-2017.pdf (March 6th, 2019). (Pg. 3).

20. Wilson, Clay. 2007. “*Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*.” Congressional Research Service. https://fas.org/sgp/crs/natsec/RL31787.pdf (March 6th, 2019). (Pg. 4).

21. Defense Information Systems Agency. 2019. “Computer Network Defense (CDN).” https://iase.disa.mil/cnd/Pages/index.aspx (March 6th, 2019).

22. Vega, Juan Carlos. 2004. “Computer Network Operations Methodology.” Naval Postgraduate School: Thesis. https://apps.dtic.mil/dtic/tr/fulltext/u2/a422320.pdf (March 6th, 2019). (Pg. 3).

23. Zwerdling, Daniel. 2013. “Your Digital Trail: Does the Fourth Amendment Protect Us?” https://www.npr.org/sections/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us (March 6th, 2019).

24. Department of Defense. 2016. *DoD Manual 5240.01.* https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887 (January 31st, 2019). (Pg. 1).

25. Richards, Rebecca J. 2014. "NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333. National Security Agency. https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_clpo_report_targeted_EO12333.pdf (March 6th, 2019). (Pg. 2).

26. Director of National Intelligence. 2008. "Reference Book - EO 12333." https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333 (March 7th, 2019). (Sec 1.4-B).

27. Theohary, Catherine. 2018. "*Defense Primer: Cybersecurity Operations."* Congressional Research Service. https://fas.org/sgp/crs/natsec/IF10537.pdf (March 6th, 2019). (Pg. 2).

28. Kreisher, Otto. 2007. "The Years of Noble Eagle." Air Force Association. https://www.norad.mil/Newsroom/Article/578175/the-years-of-noble-eagle/ (March 6th, 2019).

29. Chesney, Bobby. 2012. "The CIA, Executive Power, and International Law: Reflections on Yesterday's Speech." The Lawfare Institute. https://www.lawfareblog.com/cia-executive-power-and-international-law-reflections-yesterdays-speech (March 6th, 2019).

30. Wall, Andru E. 2011. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal* 3(1): 85-142 (86).

31. American Civil Liberties Union. 2019. "Warrantless Surveillance Under Section 702 of FISA." https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa (March 7th, 2019).

32. Foreign Intelligence Surveillance Act. 92 Stat. 1783-1798. (1978).

33. Brennan Center for Justice. 2017. "Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page." https://www.brennancenter.org/analysis/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333-and-section-215 (March 7th, 2019).

34. Department of Justice. 2015. "Privacy Act of 1974." https://www.justice.gov/opcl/privacy-act-1974 (March 6th, 2019).

35. USA Freedom Act H.R. 2048, Pub.L. 114–23. (2015).

36. Siddiqui, Sabrina. 2015. "Congress passes NSA surveillance reform in vindication for Snowden." The Guardian. https://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden (March 6th, 2019).

37. Human Rights Watch. 2015. “Strengthening the USA Freedom Act.” https://www.hrw.org/news/2015/05/19/strengthen-usa-freedom-act (March 6th, 2019).

38. Jarrett, Marshall H & Michael W. Bailie. 2010. *Prosecuting Computer Crimes*. Department of Justice. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (March 6th, 2019). (Pg. 2).

39. Curtiss, Tiffany. 2016. “Computer Fraud And Abuse Act Enforcement: Cruel, Unusual, And Due For Reform.” *Washington Law Review* Vol 91: 1813-1850. (1814-1815).

40. Privacy Act of 1974 (5 U.S.C. § 552a)

41. The Judicial Learning Center. 2015. “Your 4th Amendment Rights.” https://judiciallearningcenter.org/your-4th-amendment-rights/ (February 2, 2019).

42. Larkin, Paul. 2014. “The Fourth Amendment and New Technologies.” The Heritage Foundation. https://www.heritage.org/report/the-fourth-amendment-and-new-technologies (February 1st, 2019).

43. Fakhoury, Hanni. 2015. “Applying Fourth Amendment Protections to Electronic Devices and Data.” James Education Center. https://www.jameseducationcenter.com/applying-fourth-amendment-protections-to-electronic-devices-and-data/ (January 31st, 2019).

44. Litt, Robert. 2018. “Location Information Is Protected by the 4th Amendment, SCOTUS Rules.” JD Supra. https://www.jdsupra.com/legalnews/location-information-is-protected-by-78108/ (January 31st, 2019).

45. Totenberg, Nina. 2018. “In Major Privacy Win, Supreme Court Rules Police Need Warrant To Track Your Cellphone.” National Public Radio. https://www.npr.org/2018/06/22/605007387/supreme-court-rules-police-need-warrant-to-get-location-information-from-cell-to

46. Brennen Center for Justice. 2018. “U.S. v. Ackerman.” https://www.brennancenter.org/legal-work/us-v-ackerman (February 3rd, 2019).

47. Strohm, Chris. 2017. “Privacy vs. Security.” Bloomberg. https://www.bloomberg.com/quicktake/privacy-vs-security (February 3rd, 2019).

48. Geiger, Abigail. 2018. “How Americans have viewed government surveillance and privacy since Snowden leaks.” Pew Research Center. http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (February 3rd, 2019).

49. Wood, Colin. 2018. “Most people don't want to access government services with their mobile devices.” Statescoop. https://statescoop.com/most-people-dont-want-to-access-government-services-with-their-mobile-devices/ (February 3rd, 2019).

50. Finklea, Kristin. 2016. "*Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations.*" Congressional Research Service. https://fas.org/sgp/crs/misc/R44187.pdf (March 19th, 2019) (Summary).

51. Pressman, Aaron. 2018. "The Secret History of the FBI's Battle Against Apple Reveals the Bureau's Mistakes." Fortune Magazine. http://fortune.com/2018/03/27/fbi-apple-iphone-encryption-san-bernardino/ (March 19th, 2019.

52. Department of Homeland Security. 2018. *Department of Homeland Security Cybersecurity Strategy*. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (Pg. 5).

53. Teufel, Hugo. 2008. *Privacy Policy Guidance Memorandum*. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (February 3rd, 2019). (Pg. 1-4).

54. Rouse, Margaret. 2014. "Chief Privacy Officer (CPO)." TechTarget. https://whatis.techtarget.com/definition/chief-privacy-officer-CPO

55. O'Connor, Nuala. 2018. "Reforming the U.S. Approach to Data Protection and Privacy." Council on Foreign Relations. https://www.cfr.org/report/reforming-us-approach-data-protection (February 3rd, 2019).

56. Department of Defense. 2019. "Systems of Records Notices." https://dpcld.defense.gov/Privacy/SORNs/ (February 3rd, 2019).

57. Orszag, Peter. 2010. *Memorandum For The Heads Of Executive Departments And Agencies: Guidance for Agency Use of Third-Party Websites and Applications*. Office and Management and Budget. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf (January 31st, 2019).

58. Rich, William. 2018. "The US Leans on Private Firms to Expose Foreign Hackers." Wired. https://www.wired.com/story/private-firms-do-government-dirty-work/ (February 7th, 2019).

59. Director of National Intelligence. 2018. *A Guide to Cyber Attribution*. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf (Pg. 2).

60. Romanosky, Sasha. 2017. "Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?". LawFare. https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government

61. Graves, Tom. 2017. "Active Cyber Defense Certainty Act." 115th Congress. https://www.congress.gov/bill/115th-congress/house-bill/4036

Recommendations

The inherent dangers of cyberspace, to private individuals as well as institutions, systems, and networks owned by both government and private sector entities requires ample and coordinated protection. However, the research presented in this report shows that the current state of cybersecurity in the U.S. is far from coordinated. We have therefore developed the following recommendations for improving cybersecurity processes and systems and developing a comprehensive U.S. cyber framework.

- Chapter recommendations
    - Coordinated Federal cyber framework
    - Small business reinforcement
    - Public-private partnership for cybersecurity and cyberattack response
    - Private sector self-defense
- Additional recommendations
    - Reserve Cyber Guard
    - Coordinated terminology
    - Recommendation for further study

Chapter Recommendations

The following are the recommendations that were provided in the previous chapters of this report.

Coordinated Federal Framework (Chapter 1)

The lack of consistency between the various documents that regulate and guide U.S. cybersecurity efforts, particularly at the Federal level, can be addressed through the development and implementation of a single, comprehensive cybersecurity and cyber incident response strategy. The establishment of the new Cybersecurity Infrastructure and Security Agency (CISA) within DHS as the new, central authority for cybersecurity and critical infrastructure protection in 2018 affords the opportunity to place this development under the purview of one agency. The new cyber response document should include an incident handbook that aligns with the 2018 National Cyber Strategy and the 2017 National Security Strategy and should be continuously updated to include the most accurate data and information for effective cyberattack response.

CISA would coordinate with the individual sector-specific agencies to update and align their individual cyber incident response plans to reflect and expand upon what is included in the new Federal guidance document, putting each individual sector of critical infrastructure in concurrence with the direction of the central authority and streamlines the individual response mechanisms for each sector. Lastly, through incorporating the updates and changes issued by CISA, the cyber infrastructure sections in each of the existing guidance documents should be completely removed or updated to reflect what is included in the new document.

Small Business Reinforcement (Chapter 2)

The inseparable relationship between government and the private sector requires cooperation with and the inclusion of private entities when developing a comprehensive cyber incident response framework. Extending government considerations for cybersecurity to the private sector is important as the private sector is the major vehicle for U.S. economic strength, and because the majority of critical infrastructure is owned and/or operated by private sector entities. Though there are potential concerns of government overreach and intrusion into private sector operations, there are ways to alleviate these concerns.

Apart from the Federal Government regulating the cybersecurity systems of the private sector, there is a potential to establish cooperative support through cyber insurance. Cyber insurance provides compensation for damages and losses incurred as a result of a cyber incident. This type of policy could help save small businesses from closing as a result of a cyber incident. Because of the potential moral hazard that large companies will purchase such insurance as a replacement for increased investment into cybersecurity, and because the costs of such insurance are increasing due to the nature and proliferation of malicious cyber activity, intervention by the Federal Government may be required in order to encourage small businesses to purchase such insurance and to discourage large businesses from taking advantage of such a policy.

Public-Private Partnership for Cybersecurity and Cyberattack Response (Chapter 2)

Comprehensive and cooperative cyber incident response for both the government and the private sector can best be achieved through the implementation of a cybersecurity-specific public-private partnership. This type of partnership can benefit the government through a program in which the

government works with the private sector to provide training and establish direct hiring paths to transition professionals from the private sector into government cybersecurity positions. Bringing cybersecurity professionals from the private sector into the government not only will ensure that the best minds are working together toward a national cybersecurity framework, but it also provides transference of knowledge gained from private sector cyber concerns and solutions to the government. Additionally, this partnership can only be achieved successfully if the government provides more information regarding cyber threats with the private sector. The foundation for an effective public-private partnership is contingent on the information flow from one sector the other, and while the private sector may be more equipped at handling cybersecurity, an information-sharing mechanism should be utilized to share best practices between the sectors.

Private Sector Self-Defense (Chapter 2)

The Federal Government can also support the ability of the private sector to protect itself against malicious cyber activity. Legislation that has been proposed in Congress would allow private sector entities to utilize the hacking back method to disrupt the cyberattack and identify the responsible party. Placing more responsibility and capability for cyber response in the hands of the private sector would allow the government to focus its resources on matters of national security. This would also further strengthen the public-private partnership, as the government could leverage the strength of the private sector to accomplish the initial incident identification tasks, after which the government could investigate the necessary response mechanism.

Additional Recommendations

The following recommendations were developed in addition to those that described above, and are meant to be comprehensive of all findings, conclusions, and recommendations from our analyses.

NCCIC Cyber Guard

The NCCIC currently serves as the national hub for cyber and communications information, technical expertise, and operational integration.[1] The NCCIC is contained within CISA and

includes a variety of legacy programs. These programs include the National Communications System (NCS), National Coordinating Center (NCC), United States Computer Emergency Readiness Team (US-CERT), and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Each of these functions support the following overall guiding principles of the NCCIC:[1]

- Put Customers First;
- Lead the Global Mission;
- Be an Active Force for Good;
- Drive Innovation;
- Be Right, Be Fast;
- Earn Trust.

These principles are specifically intended to guide the critical mission activities. These mission activities include:[1]

- Information Exchange;
- Training and exercises;
- Risk and vulnerability assessments;
- Data synthesis and analysis;
- Operation planning and coordination;
- Watch operations;
- Incident response and recovery.

In 2017, the NCCIC began to merge incident response and operational programs specifically under US-CERT and ICS-CERT. Bringing these two entities together under the NCCIC broadens the capabilities and mission of the NCCIC and increases the effectiveness of the overall mission to defend the nation's critical infrastructure.[1] NCCIC also works with the private sector to report cyber incidents and facilitate information sharing between the sectors. However, there is still the potential to improve the NCCIC operations and equip it with the capabilities to best fulfill its mission. Our recommendation for this improvement is to give select groups within the NCCIC, specifically those that function to support readiness and preparation, the same title

authorities as that of the United States Coast Guard (USCG) and organize them in a single entity. This entity would be called NCCIC Cyber Guard.

Currently, the USCG operates as an entity with DHS, not DoD.[2] Although it is not housed under DoD, it is still considered a military service at all times under Title 14 of the U.S. Code.[3,4] In times of war or when otherwise called on by the President, the USCG can be transferred to the Navy and used as a DoD entity through this Title. However, the USCG also operates domestically as it has authorities that DoD-only entities do not have, such as pollution response (Title 14), customs and border enforcement (Title 19), and vessel boarding within U.S. jurisdiction or beyond (Title 14). Though it has these domestic authorities, it also shares authorities with the DoD as it is part of the IC through Title 50.[3] The importance and value of the USCG having multiple authorities allows them to operate in multiple arenas.

Positive perception is vital for public support of a government agency or entity. Though the USCG is given Title 50 authorizations, it is not necessarily subject to the same public scrutiny as other IC agencies.[5] Creating a non-DoD and autonomous cyber entity that is given multiple authorizations similar to that of the Coast Guard, rather than operating strictly as an intelligence agency, could instill public confidence and trust in the government's ability to provide cybersecurity and incident response.

The DHS Office of Intelligence and Analysis (DHS OIA) currently represents DHS interests within the IC.[6] Operating with DHS OIA with Title 50 authorization would legally allow NCCIC to participate in activities within the IC during high risk situations. This could potentially improve the efficiency of information sharing between DHS and the IC in the event of or in preparation for a cyber incident. Additionally, authorizing the NCCIC with Title 32 operational powers could allow them to work in direct coordination with state National Guard units to again, streamline and improve efficiency for information sharing as well as incident response and mitigation.

It is important to stress that the recommendation is not that the NCCIC is allowed to exercise all these authorities at any time; instead, they would be allowed to exercise the capabilities under each separate Title only when directed by the President in instances of high stress or

vulnerability. An example of this is during times of election. Allowing the NCCIC to have these authorities would enable it to better help prepare state and local governments through the National Guard (and Title 32) in the event of an election hack or breach. While National Guard units are beginning to build cyber capabilities, the resources and technically capabilities currently available within the NCCIC could be vital to creating a proactive posture in assisting the National Guard with SLTT response to a potential direct threat during the election.

Additionally, this recommendation is likely to be received well by the American public. In the wake of the Edward Snowden leaks, public perception of the NSA greatly decreased and the public remains wary of U.S. intelligence operations.[7] By allowing the NCCIC to assist in protecting American interests and infrastructure in this way, through having certain operational authorities at very explicit times, a viable option has been created for both functionality and public perception.

Coordinated Terminology

Another potential area in which the U.S. could improve regarding cybersecurity is adopting consistent terminology. In light of the potential risk that some cyber threats pose, especially when wielded by one government against another, the terms "cyberattack" and "cyberwar" have entered the lexicon. To regard a cyberattack as a potential act of war can be a reasonable assumption if the conventional (but not legal) definitions of these terms are applied. The Miriam-Webster Dictionary, which for the purposes of this paper provides conventional definitions, defines war as "a state of hostility, conflict, or antagonism."[8] An act of war could then be assumed to mean an action that instigates a state of antagonism. Cyberattack is likewise defined as "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm."[9] It is not hard to suggest that a correlation exists between "causing damage or harm" with "antagonism," and therefore a cyberattack against a computer or computer system that serves a strategic military, intelligence, or defense purpose could be presumed to initiate a state of conflict. Indeed, Russia utilized a cyber incursion prior to its invasion of Georgia in 2008.[10]

The assumptions presented above become less straightforward when the legal definitions of the terms, as specified in the U.S. Code (U.S.C), are considered. A cyber threat is defined as "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system."[11] This definition is similar to the Miriam-Webster definition above. An act of war, however, is defined as "armed conflict, whether or not war has been declared, between two or more nations."[12] This legal definition differs from the conventional definition by including the term "armed conflict." To regard a cyberattack as an act of war would therefore first require considering a cyberattack as a form of armed conflict. This correlation has yet to be legally established under the U.S.C. As such, it is difficult to conclude that the U.S. Congress currently has the legal authority to declare a war that is conducted solely in cyberspace.

The legal definition is further complicated in that cyberattacks cannot always be directly linked to deliberate actions undertaken on behalf of nation or state (i.e. the problem with cyber attribution). In the case of the 2016 U.S. presidential elections, the Russian government denied any involvement; any retaliatory hostile actions against Russia by the U.S. would therefore have been considered unprovoked and could have resulted in a far worse situation, potentially an actual armed conflict. The U.S. instead chose to respond with sanctions against Russia as a deterrence against future cyber activity.[13] This has led to further strain in U.S.-Russian relations.

Considering these complications, the U.S. could look to the Tallinn Manual as a potential basis for both policy and legal frameworks regarding cyberattacks as acts of war. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, as commissioned by the NATO Cooperative Cyber Defence Centre of Excellence, provides a "comprehensive analysis of how existing international law should apply in the cyber realm."[14] The "rules" included in the Tallinn Manual present "broad principles and specific norms that apply in cyberspace."[15] Each rule also includes commentary from the International Group of Experts, distinguished legal scholars and practitioners that developed the Tallinn Manual. These Experts were led by Dr. Michael Schmitt, an American global cyber security expert.[16] This commentary "indicates the… legal basis, applicability in international and non-international armed conflicts, and normative content."[15]

The Tallinn Manual itself does not establish any laws and does not have the force of law, and was developed to be policy- and politically-neutral.[16] The U.S., though instrumental in the development of the Manual, has been reluctant to adopt it in practice, with specific reservations about how the Manual defines state sovereignty regarding cyberspace and cyber activities. The particular concern is at what level a cyberattack can "legally" elicit a response.[17] However, implementing principles and rules similar to what is included in the Tallinn Manual into all future cybersecurity frameworks or legislation will provide the U.S. with a relatively established international definition and understanding of cyberattack and cyber war, as well as to allow coordination with the international community regarding cybersecurity.

Consistent and coordinated terminology would also require addressing USPI throughout Federal documents. This could be accomplished through the creation of a SIGINT annex to be included at the end of EO 12333, DoDM 5240.01, or Intelligence Community Directive 102. This annex would rectify the lack of consistency between the current laws, manuals or directives that do not necessarily address USPI and cyberspace uniformly, or even at all when discussing USPI specifically. This annex would outline, in detail, the lawful procedures of SIGINT collection, dissemination, and retention of USPI and the procedures that all federal agencies must follow when operating in U.S. IP space. The annex would be developed by interagency groups of lawyers and operators within the IC, as well as members of other stakeholder groups. This would be of benefit to the affected Federal agencies because it would lessen the potential for confusion of the current restrictions in place which prescribe Federal agency operations regarding USPI.

Recommendation for Further Study

The analyses presented in this report have identified deficiencies, inefficiencies, and even confusion in the current bureaucratic structure of cybersecurity and cyberattack response in both the public and private sectors. Based on the findings of these analyses, and particularly considering the overwhelming ubiquitous nature of cyberspace, we have concluded that further study into the possibility of a new, cabinet-level secretary of cybersecurity should be conducted. This recommendation exceeds the scope of this report, however our findings clearly indicate that such a study would be extremely beneficial to the continuing discussion of a comprehensive cyber framework.

Final Thoughts

Cybersecurity will continue to be an important but contentious issue, especially given the need to balance security with the right to privacy and the restrictions on government defense operations within U.S. IP space. The current method by which cybersecurity frameworks and strategies have been developed ad hoc as mandated by Executive Order or in response to growing cyber concerns will not be sufficient in the future, particularly as the cyber capabilities of adversarial nations like China, Russia, Iran, and North Korea become more sophisticated and prolific. The government cannot afford to wait until a "digital Pearl Harbor" has occurred to develop a comprehensive, national cyber framework. The recommendations presented above can serve as a basic foundation around which such a framework could be structured and fully developed.

References

1. About Us. 2019. Cybersecurity Infrastructure and Security Agency | Department of Homeland Security. https://www.us-cert.gov/about-us
2. Military.com. 2019. "The Unique Role of the U.S. Coast Guard." https://www.military.com/join-armed-forces/coast-guard-mission-values.html
3. United States Coast Guard. 2018. "Authorities." Department of Homeland Security. https://www.uscg.mil/readings/Article/1548177/authorities/
4. Dolbow, Jim, and Jim Howe. 2017. "Shift the Coast Guard to DoD." *Proceedings* 143(2). https://www.usni.org/magazines/proceedings/2017/february/shift-coast-guard-dod
5. Pew Research Center. 2015. "Ratings of federal agencies, Congress and the Supreme Court." http://www.people-press.org/2015/11/23/4-ratings-of-federal-agencies-congress-and-the-supreme-court/. (November 23, 2015).
6. Office of the Director of National Intelligence. 2018. "Dept. of Homeland Security Office of Intelligence and Analysis." https://www.intelligence.gov/index.php/how-the-ic-works/our-organizations/420-dhs-office-of-intelligence-and-analysis
7. Geiger, Abigail. 2018. "How Americans have viewed government surveillance and privacy since Snowden leaks." Pew Research Center. http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (February 3rd, 2019).
8. war. n.d. In *Miriam-Webster's online dictionary (11th edition).* https://www.merriam-webster.com/dictionary/war
9. cyberattack. n.d. In *Miriam-Webster's online dictionary (11th edition).* Retrieved from https://www.merriam-webster.com/dictionary/cyberattack
10. Flournoy, Michèle and Michael Sulmeyer. 2018. "Battlefield internet: A plan for securing cyberspace." *Foreign Affairs* 97(5) 40-46.
11. U.S. Code Title 6 § 1501
12. U.S. Code Title 18 § 2331
13. McDavid, Sandra. 2017. "When does a cyberattack become an act of war?" *InCyberDefense*. https://incyberdefense.com/news/cyber-attack-become-act-war/
14. Atlantic Council. 2017. "Tallinn Manual 2.0 Clarifies How International Law Applies to Cyber Operations." http://www.atlanticcouncil.org/news/press-releases/tallinn-manual-2-0-clarifies-how-international-law-applies-to-cyber-operations
15. Clark, Robert. 2015. "The Cybersecurity Canon: Tallinn Manual on the International Law Applicable to Cyber Warfare." Paloalto Network Research Center.

https://researchcenter.paloaltonetworks.com/2015/07/the-cybersecurity-canon-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

16. Jensen, Eric Talbot. 2016. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law 48*: 735-778.

17. Schmitt, Michael. 2018. "In Defense of Sovereignty in Cyberspace." Just Security. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/.

Annexes

Annex A: Hypothetical Cyberattack on Abilene, Texas (Taylor County)

The purpose of the following section is to illustrate the coordination, response, and recovery efforts between government and the private sector, utilizing the current governance and guidance documents presented in this report to respond to a cyberattack. *The following scenario is entirely hypothetical and was created by the authors of this report.*

Background

"The City of Abilene, Texas, is located approximately 180 miles due west of the Dallas/Fort Worth Metroplex. We're situated in west-central Texas near the geographic center of the state. Situated adjacent to Interstate 20, Abilene serves as the county seat for Taylor County, one of 254 counties in Texas. Taylor County has a current population of about 136,000, of which 120,373 live within the Abilene city limits.

Abilene's civic progressiveness and its logistic function as a regional center for distribution, commerce, industry, transportation, and education provide an assortment of lodging, dining, cultural, and shopping opportunities typically found only in much larger cities."[1]

Additionally, Abilene and Taylor County are home to Dyess Air Force Base (DAFB). DAFB is located 7 miles southwest of Abilene, Texas and covers 6,409 acres. DAFB employs more than 5,000 people and has an annual economic impact of around $310 million on the local community, making it the single largest employer for the area. The base contains nearly 200 facilities and 988 units of family housing. In total there are around 13,000 military personnel and civilians located on the base.[2]

DAFB is home to the 7th Bomb Wing and the 317 Airlift Wing of the United States (U.S.) Air Force. The 7th Bomb Wing consists of the largest B-1B operations group comprising 33 B-1B Lancers and 1,140 personnel assigned to three squadrons: The 9th and 28th Bomb Squadrons, and the 7th Operations Support Squadron. As of March 2019, DAFB is now home to the new B-21 Raider bomber mission and training center.[3]

Scenario

At approximately 1600 hours on Saturday, August 3, 2019, the City of Abilene Courthouse experiences a power outage. City officials first recognize that the outage has occurred when the

Dell PowerEdge Server[4] goes offline, quickly followed by the rest of the electrical power. Due to this power outage, all lines of communication are down. City officials then contact the local and regional electric power companies for assistance.

At 1800 hours, the Taylor County Judge and Sheriff make contact with DAFB, which has not lost power due to the renewable energy system that provides electrical power for the base.[5] Taylor County requests assistance from DAFB to help store food, route emergency communication, and provide other resources as necessary. At the same time, the Electric Reliability Council of Texas (ERCOT) reaches out to DHS, which connects them with the Department of Energy (DOE), the sector-specific agency (SSA) for power-related emergencies.[6] DOE then reports the problem to its internal Office of Cybersecurity, Energy Security, and Emergency Response.[7]

By 2100 hours, three-quarters of Taylor County residents, or nearly 100,000 people, have lost power. The three electric power companies that own and operate facilities within Taylor County meet regarding the outages of their own servers and to address the now county-wide situation. Additional entities that are highly impacted by the loss of electrical power include, but are not limited to, hospitals, nursing homes, childcare centers, grocery stores, water and wastewater management facilities, and gas companies.

At this point in time, Taylor County requests help from the Governor of Texas.[8] Additional assistance is requested from the Federal Bureau of Investigation (FBI).[9,10]

At 2200 hours, the National Security Agency (NSA)[10] along with the FBI determine that the power outage is due a cyberattack on the Taylor County electric systems achieved through a phishing email. The phishing email released a worm into the Supervisory Control and Data Acquisition (SCADA) systems within the electrical generation plants. The worm was intended to monitor the machine-controlling software, specifically targeting the smart meter to allow for remote access to shut down the power grid. Once the worm identified gaps in the system, it inserted itself into the smart meter to take control of the functions and shut down the power grid.

At 13 hours after the electrical power went out, 0500 on Day 2 of the power outage, state and local authorities have not determined attribution for the cyberattack. At this point, the Governor

of Texas calls on the President to make an Emergency Declaration through the Stafford Act.[11] The President then directs DHS to act through various cyber coordination and response plans such as the National Cyber Incident Response Plan (NCIRP)[10] and the National Response Framework (NRF).[12]

During this time, however, officials working the response discover that hackers of unknown identity and origin have been accessing the electric system for the past 6 to 8 months, remaining dormant but monitoring the systems during vulnerability testing until they could exploit a vulnerability that had not yet been patched by the electrical power companies. When this vulnerability was discovered, the hackers launched the attack on the city of Abilene using the phishing email.

The Department of Defense (DoD), specifically U.S. Northern Command (USNORTHCOM) and U.S. Cyber Command (USCYBERCOM), at this time are on standby for national response but are communicating and working with DAFB to ensure their safety and security against the attack. They are operating in support of DAFB, ready to support NSA activities if called upon.[10]

At around mid-day on Day 2 of the power outage, the NSA and FBI make the assessment, with moderate confidence, that the phishing email initiated a distributed denial of service (DDoS) attack to establish an advanced persistent threat (APT). At around mid-day on Day 3, the NSA and FBI attribute the attack to hacking groups located in Iran. This assessment is made based on intelligence reports that have recently discussed the growing capabilities of Iran to perform DDoS attacks on critical infrastructure, specifically electric grids. Additionally, this pattern resembles previous, similar Iranian DDoS attacks against the U.S. Financial Sector conducted between 2012 and 2013.[13]

It is unknown at this time what the effects of this attack have had on the entirety of the ERCOT power grid in the state of Texas.

Timeline Analysis

In applying our research to this scenario, we observed that the majority of the agencies involved, as stipulated through the relevant guidance documents, each assert themselves as being the entity

in charge. This observation was confirmed through speaking with DoD, FBI, and DHS officials who work in the cybersecurity realm, each of whom provided a different answer regarding which agency is “in charge” in the event of this attack.

The following commentary outlines the events and effects of the attack, as well as the response and recovery operations. The commentary has been structured to match the timeline included at the end of this Annex, and they should be viewed together. The first (bottom) tier of the four-tiered timeline documents the effects of the attack on and the response and recovery efforts of the government, private sector, and critical infrastructure stakeholders affected by the power outage. This tier corresponds with **Table A-1** below. The second tier, in gray, presents the response actors that are working to mitigate the issues of the sector problems. The third and fourth tiers, in green and blue, respectively, present the guidance and governance documents that specify the authorities and details for response and recovery efforts.

Sector Problems Timeline (Base Tier)

Table A-1 presents the time and description of the effects of the attack, and the response and recovery efforts. Each color in the Timeline Key corresponds to a specific sector affected by the attack.

Timeline Key:

Power Company (Co.) - Magenta
Fire and Police Responders - Red
Food/Agriculture - Orange
Water - Yellow
Health - Green
Fuel - Blue
Dyess Air Force Base (DAFB) - Purple
TC - Taylor County- Grey
Federal Action - No Fill

Table A-1a Sector Problems Timeline – Day 1

Event	Time	Sector	Description
START	1600	TC	SCADA Systems are Compromised - Power Goes Out.
1		Power Co.	Power companies try to restore power.
2		Fire/Police	Fire and Police are notified of the blackout.
3		Food/Ag	Ovens, fryers, fridges, lights begin to turn off in restaurants throughout Abilene.
4	1700	Fuel	Gas stations begin to cease pumping gas from the electric grid, those with generators continue pumping.
5		Power Co.	Power companies follow standard protocol and notify ERCOT of the outage.
6	1800	Fire/Police	Police Units are dispatched to control traffic due to street lights not being operational.
7		DAFB	TC calls DAFB about the outage - power assistance request.
8		Power Co.	Power companies determine it was a forced outage, not natural.
9	2000	Health	Hospitals cancel all nonessential appointments and elective surgeries.
10		Food/Ag	Refrigerated Food goes bad- FDA recommends that households, grocery stores, and restaurants throw refrigerated food out after 4 hours.
11		Fire/Police	Fire and EMS respond to multiple vehicular accidents, fires, and medical emergencies.
12		DAFB	TC requests DAFB to store food/essential resources under their energy source.
13	2100	TC	TC all residents have lost power.
14		Food/Ag	No safe refrigerated food is available in the town of Abilene, restaurants shut down.
	2200	TC	Phishing email discovered at the power generation plants.

15		Power Co.	Power companies request FBI assistance for digital forensics.
16		Health	Increased numbers of people heading to hospital/ other health providers due to accidents (“ambulance diversion”-- sending people to other places).
17	2300	Fire/Police	Police Units patrol the streets in order to minimize crime and assure citizens that order is being maintained.
18		DAFB	Police begin routing calls through DAFB - keep up information sharing for response overnight.

Table A-1b Sector Problems Timeline – Day 2

Event	Time	Sector	Description
19	0500	TC	**Governor calls President for Emergency Declaration**
20		Power Co.	Power companies continue to use backup generators to operate.
21		DAFB	DAFB begins working with local responders once resources are exhausted on response - Fire/Police, support role only. DAFB/DoD can begin mobilizing for emergency response independently of support function.
22		Fuel	Gas stations cease pumping via generators, using all of their on-hand supply of fuel.
23		Food/Ag	Other counties bring food through food trucks.
24		Fire/Police	Police are placed at gas stations who continue to pump gas in order to control fueling.
25	Mid-Day	Federal	USCYBERCOM and USNORTHCOM on standby for national response.
26		Health	Generators at the hospitals run out of initial rounds of power.
27		Food/Ag	Chain grocery stores get back up food from the chain store and chain restaurants but still cannot produce their own.
28		Federal	NSA and FBI have determined that there has been a DDoS and APT attack.

29		Power Co.	Power companies work with surrounding counties for power sourcing.
30	PM	Fire/Police	DAFB/TXNG provides units to assist in the security of Abilene due to an increase in looting and crime.

Table A-1c Sector Problems Timeline – Day 3

Event	Time	Sector	Description
31		Health	Vaccines at the hospital spoil (3 hours after refrigerators go down) and loss of access to medication, vaccines, water pressure, etc.
32	AM	Power Co.	Power company IT teams work with federal entities to help mitigate the potential attribution of Iran and protecting their systems henceforth.
33		Health	Start evacuating critical patients (start “triaging”).
34		Food/Ag	Guards stationed outside of grocery stores protecting food and supplies.
35		Fuel	Roads begin to clog as vehicles run out of gas and are abandoned or pushed to the side.
36	Mid-Day	Health	Elderly/chronically ill, critical patients, begin to pass due to prolonged exposure to the heat, lack of machines and access to medicine.
37		Federal	NSA and FBI make the assessment that this attack is linked to hacking groups located in Iran.
38		Fire/Police	Family resource centers are established to assist families of first responders.
39		Fuel	Fuel for cooking, such as propane, begins running out.
40		Water	Small wastewater plants begin to back up and generators have to be turned off. Water plant accidents occur as automatic controls allow for chemical leaks, or water is shut down completely.
41	PM	Fire/Police	Fire and Police “leave their post” and return to their families after three days of constant operations.

Response Actors (Second Tier)

When the Abilene City County courthouse experiences the power outage, they communicate with the local power companies to determine when power will be restored. The power companies are working through their operation plans to try to restore power. At this time, the power companies are working with ERCOT[14] which uses the National Institute of Standards and Technology (NIST) framework to identify and mitigate threats.[15] The power companies and ERCOT determine that it was a forced outage, and not due to natural events. Shortly afterwards, county officials call the Governor for aid, and the Texas National Guard is deployed to investigate the incident.[12] At 2200 hours, the FBI discovers the phishing email and works with the power companies to respond.[9] During this time, first responders begin deploying in the county in response to the needs of the citizens.

The next morning, the National Guard, operating under the authority of state officials, determines that response and recovery efforts exceed the capabilities and resources of the state and advise the Governor's office to call request assistance from the Federal Government. With this information, the Governor of Texas asks the President to make an Emergency Declaration through the Stafford Act.[16] Because the emergency directly affects the security of the electrical grid, the Secretary of Energy is authorized under Energy Department Rule 83 FR 1174 to order emergency measures to protect and restore the affected sections of the grid.[17] The NSA is brought in to help the FBI at this same time.[10] Shortly after the emergency declaration, the NSA and FBI determine that there has been a DDoS and APT attack on the Taylor County electric systems. With moderate confidence, the NSA and FBI eventually attribute the attack to hacking groups located in Iran. They advise the President of the new information. Throughout the day, the power companies are operating on backup generators to continue their work.

At the local level, the Taylor County Judge and Sheriff contact DAFB to request assistance to store food, help route emergency communication, and provide other resources as necessary. At the Federal level, DoD, specifically USNORTHCOM and USCYBERCOM, have been on stand-by for national response but are communicating and working with DAFB to ensure their safety and security against the attack.[10] They are operating in support of DAFB and in support of NSA if called upon. Finally, private parties have begun entering Taylor County, bringing supplies for

those in need. This includes power companies from outside the area, who are providing additional power support.

Guidance Documents (Third Tier)

The National Infrastructure Protection Plan (NIPP) is the primary guideline to ensuring risk management for the nation's critical infrastructure.[6] Specifically regarding cyber, the NIPP works directly with the five mission areas of the NRF: prevention, protection, mitigation, response, and recovery.[12] Taylor County should be implementing NIPP and the NRF throughout the year so that in the event of an incident like this cyberattack, they already have the appropriate measures in place to respond to the cascading effects of the loss of power, similar to the response mechanisms of a natural disaster.

NIST, part of the U.S. Department of Commerce (DOC), has set standards for cybersecurity protection for critical infrastructure.[15] These standards are a voluntary framework for private sector entities to implement as protective measures against cyberattacks. It is recommended that Taylor County abide by these standards year-round.

The NCIRP outlines three major response mechanisms that can be applied to this scenario and that are officially implemented after the emergency declaration for Federal response has been issued by the President. The first mechanism defines DHS authority for asset response.[10] Although DHS authority technically begins almost immediately through the DOE as the SSA[6], they are officially assigned, through NCIRP, with asset response at this time.[10] The second mechanism defines the responsibility of DOJ for threat response.[10] Similar to DHS, DOJ is involved, albeit remotely, through the initial assistance of the FBI. The more direct responsibilities of the DOJ are initiated through the authorization of NCIRP. The third mechanism identifies the Office of the Director of National Intelligence (ODNI) as the lead coordinator of intelligence support.[10] This creates an issue regarding authority for intelligence gather, specifically whether the FBI is the lead authority, or if ODNI is the lead authority, and coordinates with the FBI and NSA. Threat response and intelligence gathering go hand-in-hand, but until it is deemed an international threat, ODNI does not have quite the capabilities of the FBI with respect to domestic intelligence. Additionally, through the affected entity response, the

specific SSA, in this case DOE, will step in to coordinate information sharing and response. Federal response will be limited, however, in the event that an attack effects privately-owned critical infrastructure such as ERCOT. This is somewhat contradictory to the Federal response authorized in the above mechanisms.[10]

Governance Documents (Top Tier)

In the event of a cyberattack, the state of Texas implements the Texas Cybersecurity Strategic Plan (TCSSP), which outlines five goals that must be met in order to ensure security against cyberattacks.[17] These goals include cohesion between state and Federal agencies, proactive defenses, a well-trained workforce, improved response times, and outreach programs. The TCSSP provides both the government and the private sector a guideline for cyber situations as well as a plan to improve future response. Although this plan is currently officially in place, it provides little guidance on what to do in the event of an attack outside of utilizing information sharing methods.

The Texas Department of Information Resources (TDIR) has a response handbook that provides state and private entities with a specific approach to an emergency situation, including cyber incidents.[18] However, this handbook primarily covers only what to do in the event of a data breach. Despite this, the handbook can still be considered a good preliminary resource for state-level attack response. This handbook outlines contact the State Chief Information Security Officer and the State Cybersecurity Coordinator.[19]

When the Governor of Texas informs the President that the resources of Taylor County and Texas have been insufficient to address the attack and restore power, the Governor requests that the President declares the attack an emergency in order to mobilize Federal resources. After reviewing situational reports from the Governor, DOE and FBI, the President agrees and issues the emergency declaration. Federal resources are mobilized in accordance with the Stafford Act. The Secretary of Homeland Security is directed to assume coordination of the Federal response.

In accordance with PPD-41, the SSAs for the affected sectors of critical infrastructure, through NCIRP, are instructed to become directly involved in the response and recovery efforts.[20] The agencies to be involved in the efforts are:[6] DHS for the Commercial Facilities, Communications,

Dams, Emergency Services, Government Facilities (jointly with the General Services Administration), Information Technology, and Transportation Systems (jointly with the Department of Transportation) sectors; DoD for the Defense Industrial Base sector (specifically for DAFB); DOE for the Energy Sector; the Department of the Treasury for the Financial Services sector; the Department of Health and Human Services for the Healthcare and Public Health sector; the Department of Agriculture for the Food and Agriculture sector (jointly with the Department of Health and Human Services); and the Environmental Protection Agency for the Water and Wastewater Systems sector. In total, eight Federal departments and agencies are dispatched to assist in response and recovery efforts covering thirteen sectors of critical infrastructure.

Additionally, under PPD-21 and PEO 13800, DOJ and FBI are specifically instructed to begin investigating the attack to determine appropriate attribution.[21,22]

Applied Recommendation

The Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program, sponsored by the Defense Advanced Research Projects Agency (DARPA), is a program that tests the security of power grids within the Energy Sector. It enables a black-start recovery of power grids and provides educational and training opportunities for cybersecurity personnel, engineers, and other stakeholders within the Energy Sector. RADICS has partnered with DOE to conduct three different exercises.[23] It should be noted that this program expires in 2020.[24]

Jack Voltaic 2.0, a cyberattack exercise project sponsored by the Army Cyber Institute (ACI) and conducted in cooperation with the city of Houston, DHS and a variety private, state, and Federal entities, is an example of a simulation or exercise that can be used to demonstrate cyberattack response capabilities and authorities for critical infrastructure. This exercise, conducted in Houston in 2018, showed that state and local governments are not properly equipped to handle a large-scale cyberattack that affects multiple sectors of critical infrastructure.[25]

Based on the results and analyses presented in this study, and considering the results obtained from the RADICS program and the Jack Voltaic exercise, it is our recommendation that both of these programs continue beyond 2020. Additionally, it is recommended that RADICS and Jack

Voltaic should be conducted in coordination with each other. The exercises conducted under these programs should be expanded to include all 16 sectors of critical infrastructure and should be administered by CISA through the National Risk Management Center (NRMC). CISA should work with a variety of critical infrastructure stakeholders, including those in the private sector, to build upon the relationships that RADICS and Jack Voltaic have established. The benefit of continuing these programs and exercises is that they can help further prepare local, state, and Federal authorities and private sector entities in cyber response management and coordination, and help to identify. Using CISA to conduct these exercises allows for the combination of resources that were used in both Jack Voltaic and RADICS.

The results of our audit on the coordination of cyberattack response, through research in open-source literature, found that depending on the entity or agency in question, the approach to response and identification/delegation of the lead authority for cyberattack response differs, and can often be contradictory. Using simulations or exercises like RADICS and Jack Voltaic to further engage the response authorities will provide clarity for directing and conducting a response to a cyberattack against critical infrastructure, which can improve the safety and security of our nation.

Hypothetical Cyberattack Response Timeline

Day 1 | Day 2 | Day 3

Governance Documents

- Texas Cybersecurity Strategic Plan, TDIR Response Handbook
- Stafford Act
- PPD-41
- PPD-21
- PEO 13800

Guidance Documents

- NIPP
- NIST
- NRF
- NCIRP

Response Actors

- County Officials
- DHS, DOE
- ERCOT (NIST)
- Emergency Responders
- Governor
- National Guard
- FBI
- NSA
- DoD

- Power Comapnies
- Fire and Police
- Food and Agriculture
- Water
- Health
- Fuel
- Dyess Air Force Base
- Taylor County
- Federal Actions

SCADA System Compromised: 1600

Phishing Email Found: 2200

Emergency Declaration: 0500

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41

Dr. Danny W. Davis, 2019

References

1. City of Abilene. 2019. “About Abilene.” http://abilenetx.gov/living/about-abilene
2. Military Bases. 2012. Dyess AFB. Military Bases Information. http://www.militarybases.us/air-force/dyess-afb/.
3. Garner, Erica and Travis Ruiz. 2019. “Dyess Air Force Base selected as home of new B-21 bomber mission and training.” KTAB News. https://www.bigcountryhomepage.com/news/local-news/dyess-air-force-base-selected-as-only-home-of-new-b-21-bombers/1880793816.
4. Taylor County. 2019. “Functions: Information Technology.” https://www.taylorcountytexas.org/148/Information-Systems
5. U.S. Department of Energy. 2009. “Dyess Air Force Base: Water Conservation and Green Energy.” https://www.energy.gov/eere/femp/downloads/dyess-air-force-base-water-conservation-and-green-energy
6. Department of Homeland Security. 2013. *National Infrastructure Protection Plan.* https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
7. Office of Cybersecurity, Energy Security, and Emergency Response. 2019. “2018 Emergency Response Summary.” https://www.energy.gov/ceser/articles/2018-emergency-response-summary
8. Texas Division of Emergency Management. 2019. *Texas Emergency Management: Executive Guide*. https://www.dps.texas.gov/dem/GrantsResources/execGuide.pdf
9. Department of Homeland Security. N.d. *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*. https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf
10. Department of Homeland Security. 2016. *National Cyber Incident Response Plan*. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
11. Federal Emergency Management Agency. 2018. “The Disaster Declaration Process.” https://www.fema.gov/disaster-declaration-process
12. Department of Homeland Security. 2016. *National Response Framework.* https://www.fema.gov/media-library-data/20130726-1914-25045-8516/final_national_response_framework_20130501.pdf
13. Federal Bureau of Investigation. 2016. “International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector.” https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector

14. ERCOT. N.d. “Protecting ERCOT’s Electric System from Cyber Attacks.” http://www.ercot.com/content/wcm/lists/144927/Cybersecurity_One_Pager_FINAL.pdf

15. National Institute of Standards and Technology. 2018. Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

16. Federal Emergency Management Agency. 2018. “The Disaster Declaration Process.” https://www.fema.gov/disaster-declaration-process

17. Department of Energy. 2018. Grid Security and Emergency Orders: Procedures for Issuance. 83 FR 1174. January 10, 2018.

18. Texas Department of Information Resources. 2018. *Texas Cyber Security Strategic Plan: Fiscal Years 2018 - 2023.* https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Strategic%20Plan%202018.pdf

19. Texas Department of Information Resources. 2018. *Incident Response Team Redbook*. https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

20. Presidential Policy Directive No. 41. Weekly Comp. Pres. Doc. DCPD-201600495. (2016)

21. Presidential Policy Directive No. 21. Pub. Papers of the President, Book 1: 106 - 115. (2013)

22. Executive Order No. 13800. Federal Register, vol 82, no. 93, p. 22391-22397 (2017)

23. Marks, Joseph. 2018. “Pentagon Researchers Test 'Worst-Case Scenario' Attack on U.S. Power Grid.” *Nextgov.com*. https://www.nextgov.com/cybersecurity/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152803/

24. Weiss, Walter. n.d “Rapid Attack Detection, Isolation and Characterization Systems (RADICS). *Defense Advanced Research Projects Agency*. https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

25. Ackerman, Robert K. 2019. “Jack Voltaic 2.0 Gives a Glimpse of Future Infrastructure Protection.” AFCEA *SIGNAL Media*. https://www.afcea.org/content/jack-voltaic-20-gives-glimpse-future-infrastructure-protection

Annex B: List of Referenced Governance Documents

Intro

- The Stafford Act – authorizes the President to issue two types of declarations that could potentially provide federal assistance to states and localities in response to a major disaster or terrorist attack: a "major disaster declaration" or an "emergency declaration". This act provides a framework for disaster response and recovery.

Chapter 1

- National Infrastructure Protection Plan – the core document used for critical infrastructure preparedness and protections to ensure secure and resilient critical infrastructure. The plan does this through establishing a framework in which the private and public sector come together to share information, communicate, and prepare for attacks.

- Presidential Policy Directive 21 – states the Federal Government has a responsibility to strengthen the security and resilience of its own critical infrastructure against both physical and cyber threats. This directive established sixteen critical infrastructure sectors. The sixteen sectors are responsible for the financial, industrial, security, public health, communication, technological, and other critical infrastructure functions of our nation.

- Executive Order 13010 – established the President's Commission on Critical Infrastructure Protection.

- Executive Order 13636 – directs the Executive Branch to develop a technology-neutral voluntary cybersecurity framework; promote and incentivize the adoption of cybersecurity practices; increase the volume, timeliness and quality of cyber threat information sharing; incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure; and explore the use of existing regulation to promote cyber security.

- National Cyber Incident Response Plan – articulates the "roles and responsibilities, capabilities, and coordinating structures" for response and recovery from cyber incidents affecting critical infrastructure.

- Presidential Executive Order (PEO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure – implements "The Framework for Improving Critical Infrastructure Cybersecurity" produced by the National Institute of Standards and Technology (NIST). The PEO modernizes the cyber defense plans applied in PPD-21.

- National Response Framework – describes the roles, responsibilities, and structures for response "of a threat or hazard, in anticipation of a significant event, or in response to an incident"

- Framework for Improving Critical Infrastructure Cybersecurity – consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

- CISA Act – amends the Homeland Security Act of 2002 to re-designate the Department of Homeland Security's (DHS's) National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency. It transfers resources and responsibilities of the directorate to the agency.

- Presidential Policy Directive 41 – created principles that guide the Federal Government's response to any cyber incident, whether involving government or private sector entities.

- Department of Defense Cyber Strategy – represents the Department's vision for addressing cyber threats and implementing the priorities of the *National Security Strategy* and *National Defense Strategy* for cyberspace. It supersedes the *2015 DoD Cyber Strategy*.

Chapter 2

- Section 5 of the Federal Trade Commission Act of 1914 – prohibits "unfair and deceptive acts and practices in or affecting commerce."

- HHS Breach Notification Rule, 2013 – requires "HIPAA covered entities and their business associates to provide notification following a breach of unsecured, protected health information."

- Financial Modernization Act of 1999 or the Gramm-Leach-Bliley Act (GLBA) 1999 – requires financial institutions to disclose how they protect and share their customers' personal data.

- Posse Comitatus Act – prevents the use of military involvement in law enforcement, except in very explicit circumstances where the military can assist civilian law enforcement agencies.

- Texas - Business & Commerce Code § 521.052 – requires business and nonprofit sports associations that collect personal data to provide "reasonable procedures" to protect data.

- California - Civil Code § 1798.91.04 – requires manufacturers of connected devices to equip devices with reasonable security features to protect data they may collect, contain, or transmit from unauthorized access, destruction, use, modification, or disclosure.

- Colorado - H.B. 18-1128 – requires that entities that collect data develop written policies for the disposal of personal information when it is no longer needed.

- General Data Protection Regulation (GDPR) – passed into law in 2016 and made enforceable in 2018, GDPR is one of the toughest data protection laws in place. It gives the individual rights to their data that is held by companies, by implementing high standards for timely reporting.

Chapter 3

- The Patriot Act Section 215 – allowed the NSA to acquire "any tangible thing" from third parties (such as telephone companies) if it could persuade the FISA Court that the item was "relevant" to a foreign intelligence investigation.

- EO 12333 – established broad new surveillance authorities for the intelligence community, outside the scope of public law.

- Foreign Intelligence Surveillance Act Section 702 – removed the requirement that the government obtain a warrant from the FISA Court when seeking to wiretap communications between a foreign target and an American from inside the US.

- US Department of Homeland Security Cybersecurity Strategy – "This strategy provides the Department with a framework to execute our cybersecurity responsibilities during the next five years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient."

- Intelligence Community Directive 102 – created to improve the capability of IC elements to collect, retain, and disseminate information, in order to protect the US from terrorism and other threats to national security, while ensuring the IC activities are carried out in a manner that protects the legal rights, civil liberties, and privacy interests of US persons.

- Title 10 – outlines the role of armed forces in the United States Code. Federal authority over Service members falls under Title 10 of the U.S. Code. These laws apply to active duty, Reservists, and Guard members who are ordered to federal-level active duty for

federal-level missions. Funding comes from the federal government and the President of the United States has authority over these Service members. Title 10 also provides the basis for the roles, missions and organization of each of the branches of armed services as well as the United States Department of Defense.

- Title 50 – governs how the US declares and conducts its wars, and how it ensures national security

- Uniform Digital Assets Law – under this law, digital assets encompass all "electronic record in which an individual has a right or interest"

- Fourth Amendment – "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

Annex C: Guidance Document Analysis Scorecard

NCIRP	NIPP	DHS CS	NRF	CISA (Agency)	DoD CS	InfraGard	EO 13010	EO 13636	PPD 21	PPD 41	PEO 13800	DoD-DHS Agreement	NCS (WH)	NSS (WH)
DoD	DoD	DHS	NGOs	DHS	DoD	DoJ	DoD	DHS	DHS	SLTT	DHS	DHS	PEs	SSAs
DHS	DHS	SSAs	DoD	CD	OFAs	PEs	DoJ	DoD	SLTT	SSAs	OMB	DoD	SSAs	Fed Agency (Vague)
DoJ	SSAs	PEs	PEs	ECD	SSAs		NSA	SSAs	SSAs	NSC	DoC	NCCIC	Fed Agency (Vague)	
ODNI	SLTT	NIST	LGs	ISD	PEs		ACs	OMB	DoJ	PEs	DoJ	NRMC		
SLTT	DoS		STT+IAGs	NRMC			FBI	ODNI	DoD	DHS	DoD			
SSAs	DoJ		DHS	FPS			CIA	PEs	ODNI		ODNI			
	DoI		DoS				FEMA	ACs						
	DoC		ODNI				SSAs							
	ODNI						PEs							
	GSA						IPTF							
	NRC													
	FCC													
	FSRAs													
	ACs													

This Annex presents another version of the Guidance Document Analysis Scorecard included in Chapter 1. However, this version is separated by document only, with each of the agencies that have major duties identified in the columns underneath. The overlap is shown by the color coordination of each of the agencies and entities involved.

Annex D: Bibliography

Ackerman, Robert K. 2019. "Jack Voltaic 2.0 Gives a Glimpse of Future Infrastructure Protection." AFCEA *SIGNAL Media*. https://www.afcea.org/content/jack-voltaic-20-gives-glimpse-future-infrastructure-protection

Ahmed, Muhammad Ejaz, Saeed Ullah, and Hyoungshick Kim. 2019. "Statistical Application Fingerprinting for DdoS Attack Mitigation." *IEEE Transactions on Information Forensics and Security* 14(6): 1471-1484.

Ahrari, Ehsan. 2010. "Transformation of America's military and asymmetric war." *Comparative Strategy 29*(3): 223-244.

Alexander, Dean. 2012. "Cyber Threats in the 21st Century." *Security* 49(9): 70-76.

American Bar Association. 2017. "Digital Property Frequently Asked Questions." https://www.americanbar.org/groups/real_property_trust_estate/resources/estate_planning/digital_property/ (January 31st, 2019).

American Civil Liberties Union. 2019. "Warrantless Surveillance Under Section 702 of FISA." https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa (March 7th, 2019).

Amir, Eli, Shai Levi, and Tsafrir Livne. 2018. "Do Firms Under-Report Information on Cyber-Attacks?" The Columbia Law School Blue Sky Blog - Columbia Law School. http://clsbluesky.law.columbia.edu/2018/04/02/do-firms-under-report-information-on-cyber-attacks/. (April 02, 2018).

Ammori, Marvin, and Keira Poellet. 2010. "Security versus Freedom" on the Internet: Cybersecurity and Net Neutrality." *SAIS Review of International Affairs* 30(2): 51-65.

Arizona Cyber Warfare Range. 2018. "About". https://www.azcwr.org/ (November 20, 2018).

Atlantic Council. 2017. "Tallinn Manual 2.0 Clarifies How International Law Applies to Cyber Operations." http://www.atlanticcouncil.org/news/press-releases/tallinn-manual-2-0-clarifies-how-international-law-applies-to-cyber-operations

Arizona Infragard. 2018. "Arizona Cyber Threat Response Alliance". http://azinfragard.org/?page_id=8 (November 20th, 2018).

Bagwell, Scott. (2015). "The Cure to Improve and Protect Health Care Records." *USA Today Magazine* 144 (2844): 26–27.

Bajramovic, Eedita. 2015. "Cyber Security in Private Industry Critical Infrastructure." *International Journal of Economics and La, 5*(13): 9.

Banafa, Ahmed. 2015. "Internet of Things (IoT): More than Smart 'Things.'" Datafloq. https://datafloq.com/read/internet-of-things-more-than-smart-things/1060 (March 27, 2019)

Bank of America. 2017. “Bank of America Corporation 2017 Annual Report.” http://media.corporate-ir.net/media_files/IROL/71/71595/BOAML_AR2017.pdf

Beesley, Caron. 2016. “How and Why to Determine if Your Business is “Small”.” U.S. Small Business Association. https://www.sba.gov/blogs/how-and-why-determine-if-your-business-small

Bendix, William, and Paul J. Quirk. 2016. “Introduction: Governing the security state.” *Journal of Policy History* 28(3): 399-405.

Bing, Chris. 2017. How China’s Cyber Command Is Being Built to Supersede Its U.S. Military Counterpart. *Cyberscoop.* https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod/. (June 22, 2017).

Bishwas, Arit K., Mani, Ashish, and Palade, Vaslie. 2018. “An all-pair quantum SVM approach for big data multiclass classification.” *Quantum Information Processing 17*(10): 282.

Blinder, Alan, and Nicole Perloth. 2018. “A Cyberattack Hobbles Atlanta, and Security Experts Shudder.” The New York Times. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

Bloomberg. 2012. “Intellectual-Property Threat Abound for U.S. Companies.” https://www.bloomberg.com/news/photo-essays/2012-10-02/intellectual-property-threats-abound-for-u-dot-s-dot-companies.

Boo, Hyeong-wook. 2017. “An assessment of North Korean cyber threats.” *The Journal of East Asian Affairs 31*(1): 97-117.

Borgia, Eleonora. 2014. “The Internet of Things vision: Key features, applications and open issues.” *Computer Communications* 54: 1-31.

Botta, Alessio, De Donato, Walter, Persico, Valerio and Pescapé, Antonio. 2016. “Integration of cloud computing and internet of things: a survey.” *Future generation computer systems 56*: 684-700.

Brennan Center for Justice. 2017. “Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page.” https://www.brennancenter.org/analysis/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333-and-section-215 (March 7th, 2019).

Brennen Center for Justice. 2018. “U.S. v. Ackerman.” https://www.brennancenter.org/legal-work/us-v-ackerman (February 3rd, 2019).

Brown, Jared T, and Bruce R. Lindsay. 2018. “*Congressional Primer on Responding to Major Disasters and Emergencies.”* Congressional Research Service. https://fas.org/sgp/crs/homesec/R41981.pdf

Brzica, Nikola. 2018. “Understanding Contemporary Asymmetric Threats.” *Croatian International Relations Review 24*(83): 34-51.

Burns A.J., M. Eric Johnson, and Deanna D. Caputo. 2019. “Spear phishing in a barrel: Insights from a targeted phishing campaign.” *Journal of Organizational Computing and Electronic Commerce* 29(1): 24-39.

Buxbaum, Jeffrey N, and Iris N. Ortiz. 2009. “Public Sector Decision Making for Public-Private Partnerships.” *NCHRP Synthesis of Highway Practice 391*: 6-10.

Buyya, Rajkumar, Yeo, Chee Shin, Venugopal, Srikumar, Broberg, James and Brandic, Ivona. 2009. “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility.” *Future Generation computer systems 25*(6): 599-616.

Cassidy, Susan. 2016. “More Cybersecurity Changes Expected for Contractors in 2017.” Inside Government Contracts. https://www.insidegovernmentcontracts.com/2016/12/cybersecurity-changes-expected-contractors-2017/. (December 29, 2016).

Cate, Fred H. & Beth E. Cate. 2012. “The Supreme Court and information privacy.” *International Data Privacy Law* 2(4): 255-267.

Campbell-Kelly, Martin, and Daniel D. Garcia-Swartz. 2013. “The history of the internet: the missing narratives.” *Journal of Information Technology* 28(1): 18-33.

Carter, David L. 2009. “Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies.” Department of Justice: Office of Community Oriented Policing Services. https://fas.org/irp/agency/doj/lei.pdf (March 19th, 2019).

Carter, Donald P. 2016. “Clouds or clocks: The limitations of intelligence preparation of the battlefield in a complex world.” *Military Review 96*(2): 36-41.

Carlin, John P. 2016. “Assistant Attorney General John P. Carlin Delivers Remarks at Press Conference Announcing Seven Iranians Charged for Conducting Cyber Attacks against U.S. Financial Sector.” The United States Department of Justice. https://www.justice.gov/opa/speech/assistant-attorney-general-john-p-carlin-delivers-remarks-press-conference-announcing

Cauthen, John. 2014. “Executing Search Warrants in the Cloud.” Federal Bureau of Investigation. https://leb.fbi.gov/articles/featured-articles/executing-search-warrants-in-the-cloud (April 2nd, 2019).

Central Security Service. 2018. “*Frequently Asked Questions about Signals Intelligence (SIGINT).”* National Security Agency. https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4 (January 31st, 2019).

Chaillan, Nicolas. 2019. Authors Interview. The Bush School of Government and Public Service. (January 25, 2019).

Chansoria, Monika. 2012. “Defying borders in future conflict in East Asia: Chinese capabilities in the realm of information warfare and cyber space.” *The Journal of East Asian Affairs 26*(1): 105-127.

Chase, Eric C. 2009. “Intelligence preparation of the (asymmetric) battlefield.” *Marine Corps Gazette, 93*(2), 20-23.

Chertoff, Michael and Rasmussen, Anders F. 2019. “The unhackable election: What it takes to defend democracy.” *Foreign Affairs 98*: 156.

Chesney, Bobby. 2012. “The CIA, Executive Power, and International Law: Reflections on Yesterday’s Speech.” The Lawfare Institute. https://www.lawfareblog.com/cia-executive-power-and-international-law-reflections-yesterdays-speech (March 6th, 2019).

Chen, Thomas M. 2014. “Cyberterrorism after Stuxnet.” Strategic Studies Institute. https://ssi.armywarcollege.edu/pdffiles/PUB1211.pdf

Christensen, Jen. 2008. “FBI tracked King’s every move.” The Cable News Network. http://www.cnn.com/2008/US/03/31/mlk.fbi.conspiracy/ (March 6th, 2019).

Cilluffo, Frank J. 2017. “A Borderless Battle: Defending Against Cyber Threats.” Center for Cyber & Homeland Security: Testimony before U.S. House Committee on Homeland Security.https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Cilluffo%20Testimony%20for%20HHSC%203-22-2017.pdf (March 6th, 2019).

City of Abilene. 2019. “About Abilene.” http://abilenetx.gov/living/about-abilene

City of Arlington, Texas, et al. v. Federal Communications Commission et al. 2013. 569 U.S. 290.

Clark, Robert. 2015. “The Cybersecurity Canon: Tallinn Manual on the International Law Applicable to Cyber Warfare.” Paloalto Network Research Center. Cohen, Natahsa & Brian Nussbaum. 2018. “Cybersecurity for the States: Lessons from Across America.” New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_for_the_States_Lessons_from_Across_America_FINAL_3.pdf. (November 19, 2018).

Cohen, Donald. 2016. “The History of Privatization.” Talking Points Memo. https://talkingpointsmemo.com/features/privatization/one/.

Cohen, Natahsa & Brian Nussbaum. 2018. “Cybersecurity for the States: Lessons from Across America.” New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_for_the_States_Lessons_from_Across_America_FINAL_3.pdf (November 19, 2018).

Connor, Tracy, Tom Winter, and Stephanie Gosk. 2015. “Iranian Hackers Claim Cyber Attack on New York Dam.” NBCNews.com. https://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611

Cooper, Roy. 2014. “Mutual Aid Agreements Between Law Enforcement Agencies in North Carolina.” North Carolina Department of Justice. https://ncsheriffs.org/wp-content/uploads/2015/01/Mutual_Aid_Agreements-Oct2014.pdf (March 19th, 2019).

Curtiss, Tiffany. 2016. “Computer Fraud And Abuse Act Enforcement: Cruel, Unusual, And Due For Reform.” *Washington Law Review* Vol 91: 1813-1850.

Cybersecurity and Infrastructure Security Agency. 2018. *National Risk Management Fact Sheet.* https://www.dhs.gov/sites/default/files/publications/NRMC%20100%20Days%20Fact%20Sheet%2020181115_CISA%20v2.pdf

Cybersecurity and Infrastructure Security Agency. 2019. “About Us.” https://www.us-cert.gov/about-us

Cyberscoop. 2018. “Opportunities for Improving Cybersecurity Visibility at State & Local Government Agencies.” Statescoop. https://s3.amazonaws.com/statescoop-media/uploads/Tenable-DisruptiveStudy-Final-1.pdf?mtime=20180419164427 (November 20th, 2018).

cyberattack. n.d. In *Miriam-Webster’s online dictionary (11th edition).* Retrieved from https://www.merriam-webster.com/dictionary/cyberattack

Davis II, John S., Benhamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Olgetree, Geoffrey McGovern, Michael S. Chase. 2017. “Stateless Attribution: Toward International Accountability in Cyberspace.” Rand Corporation. https://www.rand.org/pubs/research_reports/RR2081.html

Dean, Benjamin. 2015. “Why Companies Have Little Incentive to Invest in Cybersecurity.” The Conversation. https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570

Defense Information Systems Agency. 2019. “Computer Network Defense (CDN).” https://iase.disa.mil/cnd/Pages/index.aspx (March 6th, 2019).

Department of Defense. 2016. *DoD Manual 5240.01*. https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887 (January 31st, 2019).

Department of Defense. 2019. “Systems of Records Notices.” https://dpcld.defense.gov/Privacy/SORNs/ (February 3rd, 2019).

Department of Defense. 2018. *Summary: Department of Defense Cyber Strategy*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Department of Energy. 2018. Grid Security and Emergency Orders: Procedures for Issuance. 83 FR 1174. January 10, 2018.

Department of Health and Human Services. 2013. “HHS Breach Notification Rule.” https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Department of Homeland Security. 2017. *Handbook for Safeguarding Sensitive PII*. https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf (February 1st).

Department of Homeland Security. 2016. *National Response Framework.* https://www.fema.gov/media-library-data/20130726-1914-25045-8516/final_national_response_framework_20130501.pdf

Department of Homeland Security. 2013. *National Infrastructure Protection Plan.* https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

Department of Homeland Security. 2016. *National Cyber Incident Response Plan.*. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Department of Homeland Security. 2015. *Presidential Policy Directive 21*. https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf

Department of Homeland Security. 2016. “Mission.” https://www.dhs.gov/mission.

Department of Homeland Security. 2018. “Cybersecurity and Infrastructure Security Agency: About CISA”. https://www.dhs.gov/cisa/about-cisa.

Department of Homeland Security. 2018. *Department of Homeland Security Cybersecurity Strategy*. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

Department of Homeland Security. 2017. *Handbook for Safeguarding Sensitive PII*. https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf (February 1st).

Department of Homeland Security. 2019. “Infrastructure Security”. https://www.dhs.gov/topic/critical-infrastructure-security

Department of Homeland Security. 2008. “National Network of Fusion Centers Fact Sheet.” https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

Department of Homeland Security. 2013. *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*. https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (March 19th, 2019).

Department of Homeland Security. 2019. “Cyber and Infrastructure Security Agency.” https://www.dhs.gov/CISA (March 19th, 2019).

Department of Homeland Security. N.d. *Cyber Incident Reporting A Unified Message for Reporting to the Federal Government.* https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf.

Department of Justice. 2015. “Privacy Act of 1974.” https://www.justice.gov/opcl/privacy-act-1974 (March 6th, 2019).

Department of Justice. 2018. *InfraGard: Connect to Protect.* https://www.infragard.org/Files/INFRAGARD_Factsheet_10-10-2018.pdf

Defense Security Service. 2019. “Vision and Mission. https://www.dss.mil/

Department of Veterans Affairs. 2012. *Management of Data Breaches Involving Sensitive Personal Information (SPI).* https://web.archive.org/web/20180710182048/http://web.archive.org/web/20150526030226/www.va.gov/vapubs/viewpublication.asp?pub_id=608 (January 31st, 2019).

DeVore, Marc R., and Sangho Lee. 2017. “APT(Advanced Persistent Threat)S and influence: cyber weapons and the changing calculus of conflict.” *The Journal of East Asian Affairs* 31(1): 39-64.

Dickman, Frank. 2013. “Hacking The Industrial SCADA Network II Latest Threats To Pipeline, Production And Process Management Systems.” https://www.automation.com/pdf_articles/SCADA_Threat_Assessment_Hacking_SCADA_Network_II.pdf

Director of National Intelligence. 2019. “Sharing with the Private Sector.” https://www.dni.gov/index.php/who-we-are/organizations/ise/archive/additional-resources/2144-sharing-with-the-private-sector

Director of National Intelligence. 2018. *A Guide to Cyber Attribution.* https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf

Director of National Intelligence. 2008. “Reference Book - EO 12333.” https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333 (March 7th, 2019).

Dolbow, Jim, and Jim Howe. 2017. “Shift the Coast Guard to DoD.” *Proceedings* 143(2). https://www.usni.org/magazines/proceedings/2017/february/shift-coast-guard-dod

Eilenberger, Dawn. 2016. *Intelligence Community Directive 102: Process for Developing Interpretive Principles and Proposing Amendments to Attorney General Guidelines Governing the Collection, Retention, and Dissemination of Information Regarding U.S. Persons.* Office of the Director of National Intelligence. https://www.dni.gov/files/documents/ICD/ICD%20102%20-

%20US%20Persons%20Principles%20%20%20(13%20June%202016).pdf (March 7th, 2019).

Electronic Privacy Information Center. 2018. "Jennings v. Broome: Concerning the Scope of Protections for Stored E-mail Under the Electronic Communications Privacy Act." https://epic.org/amicus/ecpa/jennings/ (January 31st, 2019).

ERCOT. N.d. "Protecting ERCOT's Electric System from Cyber Attacks." http://www.ercot.com/content/wcm/lists/144927/Cybersecurity_One_Pager_FINAL.pdf

Executive Order No. 13010. Federal Register, vol. 61, no. 138, p. 37347-37350 (1996).

Executive Order No. 13636. Federal Register, vol 78, no. 33, p. 11739-11744 (2013).

Executive Order No. 13800. Federal Register, vol 82, no. 93, p. 22391-22397 (2017).

Fakhoury, Hanni. 2015. "Applying Fourth Amendment Protections to Electronic Devices and Data." James Education Center. https://www.jameseducationcenter.com/applying-fourth-amendment-protections-to-electronic-devices-and-data/ (January 31st, 2019).

Featherly, Kevin. 2016. "ARPANET." Encyclopædia Britannica, https://www.britannica.com/topic/ARPANET (March 28, 2019).

Federal Bureau of Investigation. 2017. "2016 Crime Report." Federal Bureau of Investigation https://www.fbi.gov/news/stories/ic3-releases-2016-internet-crime-report (March 27, 2019).

Federal Bureau of Investigation. 2019. "About IC3." Federal Bureau of Investigation Internet Crime Complaint Center (IC3) https://www.ic3.gov/about/default.aspx (March 27, 2019).

Federal Bureau of Investigation. 2016. "International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector." https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector

Federal Emergency Management Agency. 2011. *Strategic Foresight Initiative*. https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf

Federal Emergency Management Agency. 2018. "The Disaster Declaration Process." https://www.fema.gov/disaster-declaration-process

Federal Trade Commission Act. 15 U.S.C. §§ 41-58. (1914).

Federal Trade Commission. 2016. "Protecting Personal Information: A Guide for Business." https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (April 1st, 2019).

Federal Trade Commission. 2016. *Data Breach: A Guide for Business*. https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf

Fernholz, Tim. 2014. “Barack Obama Says the Internet is a Public Good, and That’s Why the US Needs Net Neutrality.” Quartz. https://qz.com/293904/barack-obama-says-the-internet-is-a-public-good-and-thats-why-the-us-needs-net-neutrality/. (November 14, 2014).

Finklea, Kristin. 2016. “*Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations.”* Congressional Research Service. https://fas.org/sgp/crs/misc/R44187.pdf (March 19th, 2019)

Fire Eye. 2019. “Advanced Persistent Threat Groups.” Fire Eye https://www.fireeye.com/current-threats/apt-groups.html (March 28, 2019).

Fischer, Eric A., Edward C Liu, John W Rollins, and Catherine A Theohary. 2014. “*The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress.”* Congressional Research Service. https://fas.org/sgp/crs/misc/R42984.pdf (March 19th, 2019).

Flournoy, Michèle and Michael Sulmeyer. 2018. “Battlefield internet: A plan for securing cyberspace.” *Foreign Affairs* 97(5) 40-46.

Foreign Intelligence Surveillance Act. 92 Stat. 1783-1798 (1783).

Fredrick, Paul and David Inserra. 2018. “How Congress Can Help Protect U.S. Companies From Cyber Attack.” The Heritage Foundation. https://www.heritage.org/technology/commentary/how-congress-can-help-protect-us-companies-cyber-attack. (January 30, 2018).

Friedman, Sara. 2018. “How States Respond to Cyber Threats.” CGN Technology. https://gcn.com/Articles/2018/05/31/state-cybersecurity-approaches.aspx. (May 31, 2018).

Gallup. 2018. “Trust in Government.” https://news.gallup.com/poll/5392/trust-government.aspx.

Garner, Erica and Travis Ruiz. 2019. “Dyess Air Force Base selected as home of new B-21 bomber mission and training.” KTAB News. https://www.bigcountryhomepage.com/news/local-news/dyess-air-force-base-selected-as-only-home-of-new-b-21-bombers/1880793816.

Garrett, Gregory A. 2018. “Cybersecurity for Government Contractors: Next Steps.” BDO International. https://www.bdo.com/insights/business-financial-advisory/cybersecurity-for-government-contractors-next-ste. (February, 2018).

Garrett, Gregory and Karen Schuler. 2017. “6 Cybersecurity Questions Government Contractors Should Address.” BDO International. https://www.bdo.com/insights/industries/government-contracting/winter-2018/6-cybersecurity-questions-government-contractors-s.

Geiger, Abigail. 2018. “How Americans have viewed government surveillance and privacy since Snowden leaks.” Pew Research Center. http://www.pewresearch.org/fact-

tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (February 3rd, 2019).

Georgia Tech: Institute for Information Security & Privacy. 2017. "Emerging Cyber Threats, Trends & Technologies Report. Georgia Tech, Institute for Information Security & Privacy". http://www.iisp.gatech.edu/sites/default/files/documents/2017_threats_report_finalblu-web.pdf.

Giles, Martin. 2019. "Explainer: What is a quantum computer?" MIT Technology Review. https://www.technologyreview.com/s/612844/what-is-quantum-computing/ (March 27, 2019).

Goodman, Seymour E, Jessica C. Kirk, and Megan H. Kirk. 2007. "Cyberspace as a medium for terrorists." *Technological Forecasting and Social Change* 74(2): 193-210.

Government Accountability Office. 2005. *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities.* https://www.gao.gov/new.items/d05434.pdf

Government Accountability Office. 2018. *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption.* https://www.gao.gov/assets/700/690112.pdf.

Gramm-Leach-Bliley Act. Federal Register 83 40945 (1999).

Graves, Tom. 2017. "Active Cyber Defense Certainty Act." 115th Congress. https://www.congress.gov/bill/115th-congress/house-bill/4036

Grinberg, Emanuella. 2018. "The FBI is investigating a ransomware attack on the city of Atlanta." Cable News Network. https://www.cnn.com/2018/03/22/us/atlanta-ransomware-attack/index.html

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimutha Palaniswami. 2013. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* 29(7): 1645-1660.

Haines, Gerald K. 2008.. "The Pike Committee Investigations and the CIA." Central Intelligence Agency: Center for the Study of Intelligence https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter98_99/art07.html (March 6th, 2019).

Harper, Jim. 2018. "A Twenty-First Century Framework for Digital Privacy Balancing Privacy And Security In The Digital Age." The National Constitution Center. https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age#footnote-1 (January 31st, 2019).

Harrington, Ben. 2018. "*UPDATE: Supreme Court Takes Fourth Amendment Case about Cell Phone Location Data*." Congressional Research Office. https://fas.org/sgp/crs/misc/LSB10157.pdf (January 31st, 2018).

Hawkins, Bret. 2015. "Case Study: The Home Depot Data Breach." SANS Institute. https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Hephner, Lisa. 2015. "Why Security is More Important for Small Businesses then It is for Larger Companies." Pay Simple. https://paysimple.com/blog/why-security-is-more-important-to-small-businesses-than-it-is-to-mega-companies/

Hicks, Andrew, and Bryan S. Cline. 2014. "Managing Cybersecurity Risk in a HIPAA-Compliant World." Hit Trust Alliance. https://hitrustalliance.net/content/uploads/2016/01/Coalfire_HITRUST_Managing_Cybersecurity_Risk_in_HIPAA_Compliant_World.pdf

Hinely, Mark. 2018. "GDPR Fundamentals: The Basics of the Law." KirkpatrickPrice. https://kirkpatrickprice.com/video/gdpr-fundamentals-the-basics-of-the-law/

Hiscox. 2018. "Small Business Cyber Risk Report." https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

Hoffman, David E. 2011. "The New Virology." *Foreign Policy* 185: 77-80

Holloway, Michael. 2015. "Stuxnet Worm Attack On Iranian Nuclear Facilities". http://large.stanford.edu/courses/2015/ph241/holloway1/

Hughes, Rex. 2010. "A treaty for cyberspace." *International Affairs (London) 86*(2): 523-541.

Human Rights Watch. 2015. "Strengthening the USA Freedom Act." https://www.hrw.org/news/2015/05/19/strengthen-usa-freedom-act (March 6th, 2019).

Jabbour, Kamal, and Erich Devendorf. 2017. "Cyber Threat Characterization." *The Cyber Defense Review* 2(3): 79-94.

Jarrett, Marshall H & Michael W. Bailie. 2010. *Prosecuting Computer Crimes*. Department of Justice. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (March 6th, 2019).

Javers, Eamon. 2013. "Cyber attacks: Why Companies Keep Quiet." CNBC. https://www.cnbc.com/id/100491610. (February 25, 2013).

Jensen, Benjamin. 2018. "The Cyber Character of Political Warfare." *The Brown Journal of World Affairs* 24: 159-171.

Jensen, Eric Talbot. 2016. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law 48*: 735-778.

Johnson, James S. 2018. China's vision of the future network-centric battlefield: Cyber, space and electromagnetic asymmetric challenges to the United States. *Comparative Strategy, 37*(5), 373-390.

Johnson, Tim. 2016. "Government in Competition with Private Sector for Cybersecurity Experts." GovTech. http://www.govtech.com/security/Government-in-Competition-with-Private-Sector-for-Cybersecurity-Experts.html (February 7th, 2019).

Joint Chiefs of Staff. 2018. "Joint Publication 3-12: Cyberspace Operations." https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf ()

Ju, Jingrui, Luning Liu, and Yuqiang Feng. 2018. "Citizen-centered big data analysis-driven governance intelligence framework for smart cities." *Telecommunications Policy* 42(10): 881.

Kaur, Ratinder, and Maninder Singh. 2014. "A survey on zero-day polymorphic worm detection techniques." *IEEE Communications Surveys & Tutorials* 16(3): 1520-1549.

Kenney, Michael. 2015. "Cyber-terrorism in a post-Stuxnet world." *Orbis* 59(1): 111-128.

Kerbs, Brian. 2014. "Target Hackers Broke in Via HVAC Company." https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Kerr, Orin. 2014. "The Fourth Amendment and the Global Internet." *Stanford Law Review* 67:285.

Kleinrock, Leonard. 2008. "History of the Internet and its flexible future." *IEEE Wireless Communications* 15(1): 8-18.

Kohen, Issac. 2018. "Protecting Intellectual Property Against Cyberattack." CSO. https://www.csoonline.com/article/3245310/protecting-intellectual-property-against-cyberattack.html. (January 2, 2018).

Kornbluh, Karen. 2018. "The internet's lost promise: And how america can restore it." *Foreign Affairs 97*: 33-38.

Krcmaric, Daniel. 2018. "Varieties of civil war and mass killing." *Journal of Peace Research* 55(1): 18-31.

Kreisher, Otto. 2007. "The Years of Noble Eagle." Air Force Association. https://www.norad.mil/Newsroom/Article/578175/the-years-of-noble-eagle/ (March 6th, 2019).

Kremer, Jens. 2014. "Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace." *Information & Communications Technology Law 23*(3): 220-237.

Kriner, Douglas, and Schickler, Eric. 2018. "The Resilience of Separation of Powers? Congress and the Russia Investigation." *Presidential Studies Quarterly 48*(3): 436-455.

Lachow, Irving. 2011. “The Stuxnet Enigma: Implications for the Future of Cybersecurity.” *Georgetown Journal of International Affairs* 2011: 118-126.

Larkin, Paul. 2014. “The Fourth Amendment and New Technologies.” The Heritage Foundation. https://www.heritage.org/report/the-fourth-amendment-and-new-technologies (February 1st, 2019).

Lee, Robert M., Michael J. Assante, Tim Conway. 2016. “TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid.” SANS Industrial Control Systems | Electric Information Sharing and Analysis Center. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Lee, Timothy. 2013. “In the 1970s, Congress investigated intelligence abuses. Time to do it again?” The Washington Post. https://www.washingtonpost.com/news/wonk/wp/2013/06/27/in-the-1970s-congress-investigated-intelligence-abuses-time-to-do-it-again/?utm_term=.896287d17f56_(March 6th, 2019).

Legal Information Institute. 2019. “Expectation of Privacy. “Cornell Law Scool. https://www.law.cornell.edu/wex/expectation_of_privacy (April 1st, 2019).

Legal Information Institute. 2019. “Fourth Amendment.” Cornell Law School. https://www.law.cornell.edu/wex/fourth_amendment (April 1st, 2019).

Levinson-Waldman, Rachel. 2013. “What the Government Does with Americans’ Data.” Brennen Center for Justice. https://www.brennancenter.org/sites/default/files/publications/Data%20Retention%20-%20FINAL.pdf (February 7th, 2019).

Lewis, James A. 2014. *Cybersecurity and stability in the Gulf*. Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-and-stability-gulf

Li, Yuqing, Wenkuan Dai, Jie Bai, Xiaoying Gan, Jingchao Wang, & Xinbing Wang. 2019. “An Intelligence-Driven Security- Aware Defense Mechanism for Advanced Persistent Threats.” *IEEE Transactions on Information Forensics and Security* 14(3): 646-661.

Li, Zhen, and Qi Liao. 2018. “Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets.” *Government Information Quarterly* 35(1), 151-160.

Liang, Qilian, Xiuzhen Cheng, and Sherwood W Samn,. 2010. “NEW: network-enabled electronic warfare for target recognition.” *IEEE Transactions on Aerospace and Electronic Systems 46*(2): 558-568.

Libicki, Martin C. 2012. “Crisis and escalation in cyberspace.” The RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf

Lin, Herbert. 2012. “A virtual necessity: Some modest steps toward greater cybersecurity.” *Bulletin of the Atomic Scientists* 68(5): 75-87.

Lin, Herbert. 2012. “A virtual necessity: Some modest steps toward greater cybersecurity.” *Bulletin of the Atomic Scientists 68*(5): 75-87.

Linden, Thomas, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2018. “The Privacy Policy Landscape After GDPR.” Cornell University: arZXiv. https://arxiv.org/pdf/1809.08396.pdf

Lindsay, Bruce R. 2017. “*Stafford Act Assistance and Acts of Terrorism.*” Congressional Research Service. https://fas.org/sgp/crs/homesec/R44801.pdf

Lindsay, Jon R. 2015. “The impact of China on cybersecurity: Fiction and friction.” *International Security* 39(3): 7-47.

Litt, Robert. 2018. “Location Information Is Protected by the 4th Amendment, SCOTUS Rules.” JD Supra. https://www.jdsupra.com/legalnews/location-information-is-protected-by-78108/ (January 31st, 2019).

Liu, Yu-Li, Yuntsai Chou, and Chih-Liang Yeh. 2018. “Big data, the internet of things, and the interconnected society.” *Telecommunications Policy* 42(4): 277.

Long, David E. 2008. “Countering asymmetrical warfare in the 21st century: A grand strategic vision.” *Strategic Insights 7*(3).

Lord, Nate. 2018. “What is an Advanced Persistent Threat? APT Definition.” Digital Guardian, https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition (March 27, 2019).

Lynch, James, and Claire Wilkinson. 2017. “Small Business and Cyber Insurance.” Insurance Information Institute. https://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_103017.pdf

Maimon, David, and Eric R. Louderback. 2018. “Cyber-Dependent Crimes: An Interdisciplinary Review.” *Annual Review of Criminology* 2:191-216.

Marks, Joseph. 2018. “Pentagon Researchers Test 'Worst-Case Scenario' Attack on U.S. Power Grid.” *Nextgov.com*. https://www.nextgov.com/cybersecurity/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152803/

McDavid, Sandra. 2017. “When does a cyberattack become an act of war?” *InCyberDefense*. https://incyberdefense.com/news/cyber-attack-become-act-war/

McFadden, C., Nadi, A., and McGee, C. 2018. “Education or Espionage? A Chinese Student Takes His Homework Home to China.” NBC News. https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881

McLaughlin, JK. 2019. Authors Interview. The Bush School of Government and Public Service. (February 7, 2019).

Meese III, Edwin. 2011. “Who is responsible for America's security?” Heritage Foundation. https://www.heritage.org/the-constitution/report/who-responsible-americas-security

Microsoft. N.d. “Microsoft’s net income from 2002 to 2018 (in billions U.S. dollars.)” *In Statista – The Statistics Portal*. https://www.statista.com/statistics/267808/net-income-of-microsoft-since-2002/

Military.com. 2019. “The Unique Role of the U.S. Coast Guard.” https://www.military.com/join-armed-forces/coast-guard-mission-values.html

Military Bases. 2012. Dyess AFB. Military Bases Information. http://www.militarybases.us/air-force/dyess-afb/.

Mincu, Constantin. 2016. “Cyber Attacks, Major Threats and Vulnerabilities against States, Organizations and Citizens.” Annals: Series on Military Sciences 8(1): 3-15.

Miorandi, Daniele, Sabrina Sicari, Francsco De Pellegrini, and Imrich Chlamtac. 2012. “Internet of things: Vision, applications and research challenges.” *Ad Hoc Networks* 10(7): 1497-1516.

Morgan, Steve. 2018. “2018 Cybersecurity Market Report.” Cybersecurity Ventures. https://cybersecurityventures.com/cybersecurity-market-report/

Moteff, John. Claudia Copeland, and John Fischer. 2003. “*Critical Infrastructures: What Makes an Infrastructure Critical?”*. Congressional Research Service. https://fas.org/irp/crs/RL31556.pdf

Nakashima, Ellen. 2015. “Why the Sony hack drew an unprecedented U.S. response against North Korea.” *The Washington Post*. https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html?noredirect=on&utm_term=.54d45fe9129f

National Conference of State Legislatures. 2019. “Data Security Laws | Private Sector.” http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx (April 1st, 2019).

National Conference of State Legislatures. 2019. “Data Security Laws | State Governments.” http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx

National Institute of Standards and Technology. 2017. “*Framework for Improving Critical Infrastructure Cybersecurity.”* https://www.nist.gov/cyberframework

National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. 2019. “Glossary: attack.” NIST Computer Science Resource Center, https://csrc.nist.gov/glossary/term/attack (March 28, 2019)

National Institute of Standards and Technology. 2019. “Glossary: computer network attack.” NIST Computer Science Resource Center, https://csrc.nist.gov/glossary/term/attack (March 28, 2019)

National Institute of Standards and Technology. 2019. “Glossary: computer network exploitation.” NIST Computer Science Resource Center, https://csrc.nist.gov/glossary/term/attack (March 28, 2019)

National Institute of Standards and Technology. 2019. “Glossary.” U.S. Department of Commerce. https://csrc.nist.gov/Glossary/?term=3537 (March 6th, 2019).

National Protection and Programs Directorate. 2018. “Written testimony of NPPD for a House Homeland Security Subcommittee on Cybersecurity & Infrastructure Protection and House Armed Services Subcommittee on Emerging Threats & Capabilities hearing regarding Interagency Cyber Cooperation.” https://www.dhs.gov/news/2018/11/14/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity

National Public Radio. 2018. “Atlanta Paralyzed For More Than A Week By Cyber Attack.” https://www.npr.org/2018/03/30/598386485/atlanta-paralyzed-for-more-than-a-week-by-cyber-attack

National Science Foundation and the American Association of Community Colleges. 2002. “Protecting Information: The Role of Community Colleges in Cyber Education.” https://www.nationalcyberwatch.org/ncw-content/uploads/2016/03/Workshop_Rpt-Role_of_CCs_in_Cyber_Ed-2002.pdf.

Netolická, Veronika and Mares, Miroslav. 2018. “Arms race "in cyberspace" - A case study of Iran and Israel.” *Comparative Strategy 37*(5): 414-429.

Netscout. 2019. “What is DDos?” https://www.netscout.com/what-is-ddos (March 6th, 2019).

Newman, Craig. 2018. “When to Report a Cyberattack? For Companies, That’s Still a Dilemma.” The New York Times. https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. (March 5, 2018).

Newman, Lily. 2018. “The Ransomware that hobbled Atlanta will strike again” Wired.com. https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/

Nielsen, Suzanne. 2012. “Pursuing security in cyberspace: Strategic and organizational challenges.” *Orbis* 56(3): 336.

North Atlantic Treaty Organization. 2013. “The History of Cyber Attacks - a Timeline.”. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.html

O'Connor, Nuala. 2018. "Reforming the U.S. Approach to Data Protection and Privacy." Council on Foreign Relations. https://www.cfr.org/report/reforming-us-approach-data-protection (February 3rd, 2019).

Office of Cybersecurity, Energy Security, and Emergency Response. 2019. "2018 Emergency Response Summary." https://www.energy.gov/ceser/articles/2018-emergency-response-summary

Office of Information Security. 2019. "What is Sensitive Personal Identifying Information?" Northeastern University. https://www.northeastern.edu/securenu/sensitive-information-2/sensitive-information/ (February 1st, 2019).

Office of the Director of National Intelligence. 2018. "Dept. of Homeland Security Office of Intelligence and Analysis." https://www.intelligence.gov/index.php/how-the-ic-works/our-organizations/420-dhs-office-of-intelligence-and-analysis

O'Neill, Patrick Howell. 2017. "'Hacking back' legislation is back in Congress." *Cyberscoop.* https://www.cyberscoop.com/hack-back-bill-tom-graves-kyrsten-sineman-cfaa/. (October 16, 2017).

O'Neil, Patrick H. 2015. "U.S. Military Plans to Outsource Cyberwar Support to Private Companies." The Daily Dot. https://www.dailydot.com/layer8/private-sector-cyber-warfare-dod-nsa/. (November 11, 2015).

Orszag, Peter. 2010. *Memorandum For The Heads Of Executive Departments And Agencies: Guidance for Agency Use of Third-Party Websites and Applications*. Office and Management and Budget. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf (January 31st, 2019).

Ozment, Andy, Tom Atkin, Eric Goldstein and Scott Mann. 2015. *Critical Partnerships: DHS,DoD, and the National Response to Significant Cyber Incidents. Department of Defense*. Department of Defense. https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/DOD-DHS-Cyber_Article-2016-09-23-CLEAN.pdf

Osawa, Jun. 2017. "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?" *Asia-Pacific Review* 24(2): 113-131.

Papier, Leesa. 2019. Authors Interview. The Bush School of Government and Public Service. (February 1, 2019).

Park, Donghui., Julia Summers, and Michael Walstrom. 2017. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." University of Washington: The Henry M. Jackson School of International Studies. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Payne, Christian and Finlay, Lorraine. 2017. “Addressing obstacles to cyber-attribution: a model based on state response to cyber-attack.” *The George Washington International Law Review 49*(3): 535-568.

Peterson, Andrea. 2014. “The Sony Pictures Hack, Explained.” *The Washington Post.* https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.0048bb417c6b

Pence, H. E. (2015). Will Big Data Mean the End of Privacy? Journal of Educational Technology Systems, 44(2), 253–267.

Pew Research Center. 2015. “Ratings of federal agencies, Congress and the Supreme Court.” http://www.people-press.org/2015/11/23/4-ratings-of-federal-agencies-congress-and-the-supreme-court/. (November 23, 2015).

Porche III, Isaac R., Jerry M. Sollinger, and Shawn McKay. 2011. *A Cyberworm That Knows No Boundaries*. RAND Corporation: National Defense Research Institute. https://www.rand.org/pubs/occasional_papers/OP342.html

Presidential Policy Directive No. 41. Weekly Comp. Pres. Doc. DCPD-201600495. (2016).

Presidential Policy Directive No. 21. Pub. Papers of the President, Book 1: 106 - 115. (2013)

Pressman, Aaron. 2018. “The Secret History of the FBI’s Battle Against Apple Reveals the Bureau’s Mistakes.” Fortune Magazine. http://fortune.com/2018/03/27/fbi-apple-iphone-encryption-san-bernardino/ (March 19th, 2019.

Privacy Act of 1974 (5 U.S.C. § 552a)

Rand Corporation. “Appendix D: Overview of the Posse Comitatus Act.” https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1251/MR1251.AppD.pdf (March 6th, 2019).

Reimann, Jakob. 2019. *China is flooding the Middle East with cheap drones.* Washington: Inter-Hemispheric Resource Center Press.

Rich, William. 2018. “The US Leans on Private Firms to Expose Foreign Hackers.” Wired. https://www.wired.com/story/private-firms-do-government-dirty-work/ (February 7th, 2019).

Richards, Rebecca J. 2014. “NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333. National Security Agency. https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_clpo_report_targeted_EO12333.pdf (March 6th, 2019).

Rid, Thomas, and Ben Buchanan. 2018. “Hacking democracy.” *The SAIS Review of International Affairs* 38(1): 3.

Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988. Pub. L. No. 100-707; amending Pub. L. No. 93-288. Codified at 42 U.S.C. §§ 5121-5207.

Robertson, Jordan and Michael Riley. 2014. “Corporations Warned Not to Hack Back.” Insurance Journal. https://www.insurancejournal.com/news/national/2014/12/31/351326.htm.

Romanosky, Sasha. 2017. “Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?”. LawFare. https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government

Rouse, Margaret. 2014. “Chief Privacy Officer (CPO).” TechTarget. https://whatis.techtarget.com/definition/chief-privacy-officer-CPO

Rubin, David, Kim Lynch, Jason Escaravage, & Hillary Lerner. 2014. “Harnessing data for national security.” *The SAIS Review of International Affairs* 34(1): 121-128.

Rudner, Martin. 2013. “Cyber-threats to Critical National Infrastructure: An Intelligence Challenge.” *International Journal of Intelligence and CounterIntelligence* 26(3): 453-481.

Ruttenberg, Joan, Paige von Mehren, and Julie Yen. 2013. “The OPIA Insider’s Guide to Intellectual Property And Cyberlaw.” Bernard Koteen Office of Public Interest Advising Harvard Law School. http://www.hls.harvard.edu/content/uploads/2008/06/ip-cyberlaw-guide-final.pdf.

SBA. 2018. “2018 Small Business Profile.” https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

Schmitt, Michael. 2018. “In Defense of Sovereignty in Cyberspace.” Just Security. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/.

Schupak, Amanda. 2016. “Obama's cybersecurity plan: Why the government alone can't protect us.” CBS News. https://www.cbsnews.com/news/obamas-cybersecurity-plan-why-the-government-cant-protect-us/ (February 7th, 2019).

Sebenius, Alyza. 2018. “Iran-Based Hackers indicted in March Cyberattack on Atlanta.” Bloomberg. https://www.bloomberg.com/news/articles/2018-12-06/iran-based-hackers-indicted-in-march-cyberattack-on-atlanta

Shah, Shabaz H. and Verma, Sudheer S. 2018. “The US and Russia: Politics of spheres of influence in the 21st century.” *IUP Journal of International Relations 12*(4): 7-20.

Siddiqui, Sabrina. 2015. “Congress passes NSA surveillance reform in vindication for Snowden.” The Guardian. https://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden (March 6th, 2019).

Simon, David. 2017. “Raising the Consequences of Hacking American Companies.” The Center for Strategic & International Studies. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/171012_Simon_RaisingConsequencesOfHacking_Web.pdf (March 19th, 2019).

Sirur, Sean, Jason R.C. Nurse, and Helena Webb. 2018. “Are we there Yet? Understanding the Challenges Faced in Applying with the General Data Protection Regulation.” Cornell University: arXiv https://arxiv.org/pdf/1808.07338.pdf

Small Business Administration. 2012. “Frequently Asked Questions.” https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf

Softness, Nicole. 2017. “How should the U.S. respond to a Russian cyber attack?” *Yale Journal of International Affairs 12*(1): 99.

Solove, Daniel. 2017. “The U.S. Congress is Not the Leader is Privacy or Data Security Law.” TeachPrivacy. https://teachprivacy.com/us-congress-is-not-leader-privacy-security-law/ (April 1st, 2019).

Spezio, Anthony E. 2002. “Electronic warfare systems.” *IEEE Transactions on Microwave Theory and Techniques 50*(3): 633-644.

Srinivas, Jangirala., Ashok Kumar Das, and Neeraj Kumar. 2019. “Government regulations in cyber security: Framework, standards and recommendations.” *Future Generation Computer Systems* 92: 178-188

Statista. 2019. “Sony's total revenue from 2007 to 2017 (in 100 billion Japanese yen / billion U.S. dollars)*.” https://www.statista.com/statistics/279269/total-revenue-of-sony-since-2008/.

Stent, Dylan. 2018. “The great cyber game.” *New Zealand International Review 43*(5): 6.

Strohm, Chris. 2017. “Privacy vs. Security.” Bloomberg. https://www.bloomberg.com/quicktake/privacy-vs-security (February 3rd, 2019).

Strom, David. 2018. “What Are the Legalities and Implications of “Hacking Back”? Security Intelligence. https://securityintelligence.com/what-are-the-legalities-and-implications-of-hacking-back/ (March 7th, 2019).

Sullivan, Julia E., and Dmitriy Kamensky. 2017. “How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid.” *The Electricity Journal* 30(3): 30-35.

Symantec. 2019. “Internet Security Threat Report: Executive Summary.” https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf (March 27, 2019)

Tafoya, William L. 2011. “Cyber Terror.” Federal Bureau of Investigation Law Enforcement Bulletin https://leb.fbi.gov/articles/featured-articles/cyber-terror (March 27, 2019)

Talent, Jim. 2010. “A Constitutional Basis for Defense.” The Heritage Foundation. https://www.heritage.org/defense/report/constitutional-basis-defense

Talton, Ellis and Tonar, Remington. 2018. “A Lack Of Cybersecurity Funding And Expertise Threatens U.S. Infrastructure.” Forbes.

https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#3b60d590264c

Target Corporation. 2014. *Target 2013 Annual Report*. https://corporate.target.com/_media/TargetCorp/annualreports/content/download/pdf/Target-2013-Annual-Report.pdf?ext=.pdf

Targeted Destructive Malware. 2014. U.S. CISA. https://www.us-cert.gov/ncas/alerts/TA15-353A

Taylor County. 2019. "Functions: Information Technology." https://www.taylorcountytexas.org/148/Information-Systems

Tech Transfer Central. "Ensuring Cybersecurity to Protect University IP Assets." https://techtransfercentral.com/marketplace/distance-learning/ensuring-cybersecurity-to-protect-university-ip-assets/.

Techcrunch. 2018. "Atlanta Cyberattack." *https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/*

Tehrani, P Pardis Moslemzadeh, Nazura Abdul Manap, Hossein Taj. 2013. "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime." *Computer Law & Security Review* 29(3): 207-215.

Teufel, Hugo. 2008. *Privacy Policy Guidance Memorandum*. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (February 3rd, 2019).

Texas Department of Information Resources. 2018. *Texas Cyber Security Strategic Plan: Fiscal Years 2018 - 2023.* https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Strategic%20Plan%202018.pdf

Texas Department of Information Resources. 2018. *Incident Response Team Redbook*. https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Texas Division of Emergency Management. 2019. *Texas Emergency Management: Executive Guid*. https://www.dps.texas.gov/dem/GrantsResources/execGuide.pdf

The Home Depot. 2014. "The Home Depot Announces Fourth Quarter & Fiscal 2013 Results; Increases Quarterly Dividend By 21 Percent And Provides Fiscal Year 2014 Guidance." http://ir.homedepot.com/news-releases/2014/02-25-2014-014521683

The Internet Society. 2012. "Data Privacy on a global scale: keeping pace with an evolving environment." https://www.internetsociety.org/resources/doc/2012/data-privacy-global-scale-keeping-pace-evolving-environment/ (April 1st, 2019).

The Judicial Learning Center. 2015. "Your 4th Amendment Rights." https://judiciallearningcenter.org/your-4th-amendment-rights/ (February 2, 2019).

The Office of the Director of National Intelligence. "Sharing with the Private Sector." https://www.dni.gov/index.php/who-we-are/organizations/ise/archive/additional-resources/2144-sharing-with-the-private-sector.

Theohary, Catherine A., and Anne I. Harrington. 2015. "*Cyber Operations in DOD Policy and Plans: Issues for Congress*." The Congressional Research Service,. https://fas.org/sgp/crs/natsec/R43848.pdf. (p.21-22).

Theohary, Catherine. 2018. "*Defense Primer: Cybersecurity Operations.*" Congressional Research Service. https://fas.org/sgp/crs/natsec/IF10537.pdf (March 6th, 2019).

Thomas, Ria. 2018. "Evolving Weapons of War: Cyberattacks on Companies." *Brunswick Group*. https://www.brunswickgroup.com/evolving-weapons-of-war-cyber-attacks-on-companies-i7638/. (April 18, 2018).

Thomas, Timothy L. 2008. "China's electronic long-range reconnaissance." *Military Review 88*(6): 47-54.

Thomsen, Jaqueline. 2018. "Pentagon Cyber Official Warns U.S. Companies Against 'Hacking Back'." The Hill. https://thehill.com/policy/cybersecurity/416494-defense-cyber-official-warns-private-companies-against-hacking-back. (November 13, 2018).

Thompson, Mark. 2016. "Iranian Cyber Attack on New York Dam Shows Future of War." Time Magazine. http://time.com/4270728/iran-cyber-attack-dam-fbi/

Totenberg, Nina. 2018. "In Major Privacy Win, Supreme Court Rules Police Need Warrant To Track Your Cellphone." National Public Radio. https://www.npr.org/2018/06/22/605007387/supreme-court-rules-police-need-warrant-to-get-location-information-from-cell-to

Trautman, Lawrence J. and Peter C. Ormerod. 2018. "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things." *University of Miami Law Review* 72(3): 761–826.

Trautman, Lawrence. 2016. "Is Cyberattack the Next Pearl Harbor?" *North Carolina Journal of Law & Technology* 18(2): 233-289.

Truman Center. 2018. "The Private Sector's Role in Cyber Security." http://trumancenter.org/cybersecurity/the-private-sectors-role-in-cyber-security/.

United States Computer Emergency Readiness Team. 2017. *US-CERT Federal Incident Notification Guidelines*. https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

U.S. Code Title 18 § 2331

U.S. Code Title 6 § 1501

U.S. Department of Energy. 2009. “Dyess Air Force Base: Water Conservation and Green Energy.” https://www.energy.gov/eere/femp/downloads/dyess-air-force-base-water-conservation-and-green-energy

United States Coast Guard. 2018. “Authorities.” Department of Homeland Security. https://www.uscg.mil/readings/Article/1548177/authorities/

United States Department of Homeland Security. 2019. “Information Sharing and Awareness.” https://www.dhs.gov/cisa/information-sharing.

United States Department of Justice. 2018. *Best Practices for Victim Response and Reporting of Cyber Incidents*. https://www.justice.gov/criminal-ccips/file/1096971/download.

United States Federal Bureau of Investigation. 2018. “Small Business Information Sharing: Combating Foreign Cyber Threats.” https://www.fbi.gov/news/testimony/small-business-information-sharing-combating-foreign-cyber-threats.

United States Government Accountability Office. 2018. *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*. https://www.gao.gov/assets/700/694913.pdf.

United States Office of Personal Management. N.d. “Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals.” https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf.

United States Securities and Exchange Commission. 2018. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.sec.gov/rules/interp/2018/33-10459.pdf.

Uribe, L. P. M., & Schub, T. B. 2018. Health Insurance Portability and Accountability Act (HIPAA): Data Communication and Security. *CINAHL Nursing Guide*. http://proxy.library.tamu.edu.srv-proxy1.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nup&AN=T904674&site=eds-live

USA Freedom Act H.R. 2048, Pub.L. 114–23. (2015).

Ucko, David. H., and Thomas A. Marks. 2018. “Violence in context: Mapping the strategies and operational art of irregular warfare.” *Contemporary Security Policy* 39(2): 206-233.

Van Impe, Koen. 2018. “How Can an ISAC Improve Cybersecurity and Resilience?” *SecurityIntelligence.* https://securityintelligence.com/how-can-an-isac-improve-cybersecurity-and-resilience/. (July 16, 2018).

Vega, Juan Carlos. 2004. “Computer Network Operations Methodology.” Naval Postgraduate School: Thesis. https://apps.dtic.mil/dtic/tr/fulltext/u2/a422320.pdf (March 6th, 2019).

Volz, Dustin. 2016. “U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage.” Reuters. https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K

Young, Thomas. 2015. “40 years ago, Church Committee investigated Americans spying on Americans.” The Brookings Institution. https://www.brookings.edu/blog/brookings-now/2015/05/06/40-years-ago-church-committee-investigated-americans-spying-on-americans/ (March 6th, 2019).

Yun, Minwoo. 2010. “Insurgency warfare as an emerging new mode of warfare and the new enemy.” *The Korean Journal of Defense Analysi*, *22*(1): 111-125.

Walker, Michael. 2017. “The New Uniform Digital Assets Law: Estate Planning and Administration in the Digital Age.” *Real Property, Trust and Estate Law Journal* 52(1): 52-78.

Wall, Andru E. 2011. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action.” *Harvard National Security Journal* 3(1): 85-142.

Walters, Riley. 2018. Private Sector Cyber Incidents in 2017. *The Heritage Foundation.* https://www.heritage.org/cybersecurity/report/private-sector-cyber-incidents-2017. (January 3, 2018).

Wang, Lanjia., Zhichun Li, Zhi Fu, and Xing Lu. 2010. “Thwarting zero-day polymorphic worms with network-level length-based signature generation.” *IEEE/ACM Transactions on Networking (TON)* 18(1): 53-66.

Wang, Lingyu., Sushil Jajodia, Anoop Singhal, Pengsu Cheng, and Steven Noel. 2014. “k-Zero Day Safety: A Network Security Metric For Measuring The Risk Of Unknown Vulnerabilities.” *IEEE Transactions on Dependable and Secure Computing* 11(1): 30-44.

Wang, Zheng. 2019. “An elastic and resiliency defense against DDoS attacks on the critical DNS authoritative infrastructure.” *Journal of Computer and System Sciences* 99: 1-26.

War. n.d. In *Miriam-Webster’s online dictionary (11th edition).* https://www.merriam-webster.com/dictionary/war

Weed, Scott A. 2017. “U.S. Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure.” Air Force University Research Institute. *https://www.hsdl.org/?abstract&did=803892*

Weiss, Aaron. 2007. “Computing in the clouds.” *Networker 11*(4):16-25.

Weiss, Walter. n.d “Rapid Attack Detection, Isolation and Characterization Systems (RADICS). *Defense Advanced Research Projects Agency.* https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

Westby, Jody. 2015. “The Government Shouldn't Be Lecturing Private Sector On Cybersecurity.” Forbes. https://www.forbes.com/sites/jodywestby/2015/06/15/the-

government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity/#2df54282621b (February 7th, 2019).

Wheeler, Tarah. 2018. "In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions." *Foreign Policy*. https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/.

White, Lawrence J. 2010. "The Gramm-Leach-Bliley Act of 1999: A bridge too far? Or not far enough?" *Suffolk University Law Review* Vol. 43 (4): 937-956.

Williams, Peter 2019. "Does competency-based education with blockchain signal a new mission for universities?" *Journal of Higher Education Policy and Management* 41(1): 104-117.

Wilson, Clay. 2007. "*Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*." Congressional Research Service. https://fas.org/sgp/crs/natsec/RL31787.pdf (March 6th, 2019).

Wirtz, Bernd W., and Jan C. Weyerer. 2017. "Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats." *International Journal of Public Administration* 40(13): 1085-1100.

Wood, Colin. 2018. "Most people don't want to access government services with their mobile devices." Statescoop. https://statescoop.com/most-people-dont-want-to-access-government-services-with-their-mobile-devices/ (February 3rd, 2019).

Woods, Jennifer. 2013. "Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5." American Bar Association. https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy/

World Intellectual Property Organization. 2019. "What is Intellectual Property?" https://www.wipo.int/about-ip/en/.

Wortzel, Larry. 2003. "Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security." The Heritage Foundation. https://www.heritage.org/homeland-security/report/securing-americas-critical-infrastructures-top-priority-the-department (March 19th, 2019).

Zwerdling, Daniel. 2013. "Your Digital Trail: Does the Fourth Amendment Protect Us?" https://www.npr.org/sections/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us (March 6th, 2019)

Dr. Danny Davis: dannywdavis@tamu.edu
bush.tamu.edu/research/capstones/