Legal, Policy, and Organizational Impediments to the Protection of Critical Infrastructure from Cyber Threats

LT Miranda La Bash, USN
and
LT Christopher Landis, USN
02 August 2013

Carnegie Mellon University
Pittsburgh, PA 15213

Submitted in partial fulfillment of the requirements for the degree of Master of Information Technology Strategy.

Keywords: Critical Infrastructure Protection, Cybersecurity

For my beloved husband, Stephen, whose patience, understanding, support, and insight make everything I do possible.

-Miranda

For my loving wife, Amy: Thank you for your unfailing support in my career and extraordinary care in raising our son, David, when I am working toward earning this degree.

-Chris

Abstract

The evolution of defensive mechanisms to protect United States domestic critical infrastructure from cyber attack includes legal, organizational, and policy dimensions. Although recent focus on critical infrastructure protection has prompted the launch of a multitude of federal efforts to defend the nation from the very real threat of a cyber-launched attack, few people understand the breadth and scope of the complete work. However, armed with an understanding of the current landscape of the Department of Defense and Federal Government cybersecurity efforts, improvements are both possible and necessary to effectively protect critical infrastructure.

Acknowledgments

The information and findings in this report would not have been possible without the gracious assistance of many individuals, both active duty military and civilian. In each instance, these individuals were extremely generous in giving of their time and extensive expertise.

We would like to extend our extreme gratitude to the following individuals:

- Dr. Jose Latimer, Mr. Timothy Evans, and Mr. Dickie George, Johns Hopkins University (JHU), Applied Physics Laboratory (APL), for their time and help with understanding the relationship between APL as a University Affiliated Research Center (UARC), DoD, Department of Homeland Security (DHS), and private industry with respect to cybersecurity and Critical Infrastructure Protection (CIP) [64, 71, 87].
- Ms. Caitlin Durkovich, DHS, Assistant Secretary for Infrastructure Protection, National Protection and Programs Directorate (NPPD), for her insight into the division of responsibilities, working relationships, and critical work within DHS [62].
- COL Claire Cuccio, USA, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)), Deputy for Cyber and Technical Integration, for providing us with valuable input and understanding into the functional workings of the DoD with regard to CIP [40] and for reviewing and providing feedback on a draft of this paper.
- Mr. Matthew Butkovic, Carnegie Mellon University (CMU), Software Engineering Institute (SEI), Computer Emergency Response Team Coordination Center (CERT-CC), for his time and willingness to help us understand better CIP from the perspective of private industry and Computer Emergency Response Team (CERT) [29, 30].
- CDR Dave 'Rooter' Root, USN Ret., our CMU Faculty Advisor, for his academic guidance and mentorship throughout this process as we negotiated the development, research, and production of this practicum.
- Lt Col David R.E. Halla, USAF, for facilitating access to current work involving the National Guard and U.S. Cyber Command (USCYBERCOM) exercises.
- CDR Pablo Breuer, USN, for his professional mentorship, technical acumen, hard work, with an unfailing willingness to argue on behalf of the voice of reason [22].
- 1st Lt Logan Clark, USAF, USCYBERCOM Public Affairs, for her time and assistance in preparing and providing information pertaining to the DoD's role in CIP and USCYBERCOM's relationships with other USG entities [34].

- Mr. Eli Konikoff, Defense Information Systems Agency (DISA), our fellow Master of Information Technology Strategy (MITS) student, and LCDR Stephen La Bash, USN, for reviewing a draft of this paper and providing feedback for its improvement.

The MITS program at CMU is funded by the Deputy Chief of Naval Operations for Information Dominance (N2/N6) via the Naval Postgraduate School (NPS) Civilian Institutions Office.

Contents

Executive Summary

Cyberspace is a unique and evolving domain. The growing dependence of modern services upon its correct and continuous operation has fueled a need for effective security and resilience against failure. This is especially true for the industrial control systems and networks behind the operation of critical infrastructure. Many different types of cyber attacks have already been perpetrated against critical infrastructure and new vulnerabilities are exposed on a daily basis. The inherent interdependence of critical infrastructure combined with these vulnerabilities demonstrates a serious threat to public health and safety, the economy, and even national security. Leaders across government understand the need for collective action to secure and protect the nation's critical infrastructure, but effective legislation, policy, and governmental organization have been slower to evolve. Federal reorganization toward the task has made significant progress from 2008 to 2013; however, improvements are still both possible and necessary. At the Executive level, the Federal Acquisition Regulation must contain requirements for cybersecurity in contract language and the current Cybersecurity Coordinator requires directive and budgetary authority. Within the Department of Defense, a streamlined command and control structure and growth of the cyber force in size and skills, including offensive capabilities, are required to effectively operate as well as to provide some deterrent to attack. Meanwhile, legal code for cybersecurity has not kept pace with technological developments. Comprehensive cybersecurity legislation is required—beginning with mandatory participation of critical infrastructure owners and operators in federal information-sharing programs in a way that incorporates appropriate safeguards for industry liability and citizen privacy—in order to completely bridge the current public-private division of responsibilities for collective defense.

Chapter 1

Introduction

Discussing the need to launch his 60-day Cybersecurity Review just after taking office in 2009, President Obama succinctly described the double-edged sword of cyber: "The very technologies that empower us to create and to build also empower those who would disrupt and destroy... in short, America's economic prosperity in the 21st century will depend on cybersecurity" [106]. Cybersecurity has grown to be a key issue for the administration and indeed for the nation in the last several years even though concern for the integrity of Critical Infrastructure (CI) functions was evident in the 1990s. For CI, which includes a range of sensitive data and performs valuable functions that support the health, safety, and economic vitality of our modern nation, the growth of networked connections in cyberspace has meant the introduction of new threat vectors to systems that were not designed to securely connect to today's Internet. Because improving the cybersecurity of CI encompasses such a large body of work, widely distributed across government and private sector entities, unity of effort is difficult to achieve. President Obama admits that "when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should – with each other or with the private sector" [106].

In order to understand why such distribution of functions exists, one need understand the complexity and severity of the threat and examine the legal foundations and therefore how government has organized to counter those threats as they have emerged. Although there are many efforts underway, they must continue and they must improve, as "on a scale of one to ten, with ten being strongly defended, our CI's preparedness to withstand a destructive cyber attack is about a three" [3]. Indeed, the Defense Science Board (DSB) Task Force on Resilient Military Systems found that "the United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber

capabilities" in combination with conventional capabilities [45]. CI systems across sectors are also deeply interconnected, meaning that "...an attack against one or more of [America's CIs] may disrupt an entire system and cause significant damage to the nation" [124, p. 38]. With the ever increasing rate of cyber physical threats (actions taken in cyberspace that have physical consequences in another domain) and the extent of damage that they can cause, the need to protect CI has never been greater. Also, the age of cyber is just beginning:

> Cyber attacks are expected in every future conflict, and... the most significant vulnerability is in the U.S. critical infrastructure on which both the military capabilities and civilian populations depend. [45, p. 52]

This is not a future threat. Attacks and compromises are happening now. In testimony to the Senate Armed Services Committee (SASC) preceding the establishment of U.S. Cyber Command (USCYBERCOM) in 2010, then LTG Alexander alerted Congress to alarming increases of intrusions "both in infrastructure within the nation and within DoD" [11]. It is imperative that the Department of Defense (DoD) and the greater Federal Government be equipped to deter adversaries, mitigate vulnerabilities, develop resiliency to compromise, and defeat cyber attacks.

1.1 Defining Cyber

Cyberspace is a war-fighting domain but has only been recognized as such since about 2008 and so is still inadequately understood. It functions not only as a virtual space but also as a means and as a medium. Like freedom of the seas, modern society depends on the open commerce and safe transit of information across cyber systems. In our computerized and information-centric society, nearly everything touches this cyber grid. The public face of cyberspace is the Internet, but there are countless connected private and government networks.

While cyber is sometimes used as an ambiguous and all-encompassing term, in this paper it will be referred to synonymously with Computer Network Operations (CNO). CNO can be broken down by intent into three categories: Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA). Any CNO for intelligence purposes, typically referred to as CNE, intrinsically falls under Signals Intelligence (SIGINT). However, CND and CNA, although almost necessarily CNE/SIGINT-enabled, fall outside of the SIGINT umbrella. These definitions run deep through policy and authorities divisions, significantly affecting organizational responsibilities.

Modern CI relies on cyber infrastructure—its hardware, software, and protocols. Because CI component design has significant performance and reliability requirements, systems typically

cannot go offline for update or upgrade. Further complicating Critical Infrastructure Protection (CIP), many subsystems were designed to be stand-alone but then were later networked. Consequently, their Achilles' heel has become cybersecurity deficient interdependent infrastructures. Because of the deluge of demonstrable threats to this infrastructure and the very high cost of attacks from these threats succeeding, both in economic terms and in health and safety terms, much government and private work is underway to mitigate cyber vulnerabilities to the country's CI.

1.2 Open Questions

Because much recent work has been accomplished on many of the topics covered in this paper, finding new ground initially seemed difficult. However, in the DSB study, no policies and authorities concerning the use of cyber offensive capabilities, nor interagency coordination issues toward responsibilities for the protection of civilian infrastructure were addressed [45]. That is the subject of this paper. How has governance at the nexus of CI and cyberspace evolved over time? How has that framework organically resulted in the organizations that exist today? How are responsibilities divided between government agencies and between the Federal Government, the private sector, and the range of semi-private efforts in between? What are the realistic threats that exist and how are we and should we be equipped to respond to them?

Despite the many efforts underway, organizational, policy, and legal impediments remain in the United States' ability to properly defend its CI. This paper will describe the immediacy of these issues and attempt to decode the legal authorities, policies, and multitude of organizations' efforts to thwart and mitigate the debilitating effects of a cyber attack against the nation's CI. A thorough review of the evolution and direction of current efforts leads to recommendations for organizational and programmatic improvements.

Chapter 2

Threats to Critical Infrastructure

2.1 Prominent Critical Infrastructure Compromises

An untold number of cyber compromise and attack examples litter both the headlines and academic literature. There is also an increasing number of probes and successful attacks against Critical Infrastructure (CI). President Obama acknowledges in Executive Order (EO) 13636, Improving CI Cybersecurity, both the occurrence of "repeated cyber intrusions into critical infrastructure" and the dependence of national and economic interests on the security and "resilience of the Nation's critical infrastructure" [109]. A survey of vulnerability and threat vectors helps to convey the gravity of Critical Infrastructure Protection (CIP). The following examples provide a review of several CI-specific key cases, differing by actor, motive, target, and method. They highlight very real threats to U.S. CI and set the stage for a discussion of the cyber-related challenges facing the Department of Defense (DoD), Department of Homeland Security (DHS), and their interagency and private sector partners in defending the heartbeat of modern living, which begins with safe water and dependable power generation and distribution and extends beyond telecommunications, transportation, and finance.

2.1.1 Stuxnet

The most infamous cyber weapon may very well be Stuxnet. McAfee claims that Stuxnet was a game changer that alerted the CI industry to the reality that malware can be specifically designed to cause physical damage [18]. Unlike typical malware, Stuxnet is definitively classified as a cyber weapon because it damaged Iran's nuclear fuel processing plant via targeting the specific Supervisory Control and Data Acquisition (SCADA) systems in use at that plant in order to delay Iran's procurement of enriched nuclear material [2, 4, 12, 46, 77, 94].

2.1.2 Queensland Sewage

A less sophisticated attack, but perhaps one that had a greater affect on nearby civilians was an insider attack on the Queensland, Australia, sewer system. In 2000, Vitek Boden attacked the Maroochy Shire Council sewerage system as an act of vengeance toward his former employer, a Maroochy Shire Council Industrial Control System (ICS) contractor, and the Council, who did not hire him following his direct application for a position. Using stolen equipment and software, he was able to gain control of pumps and valves while disabling alarms resulting in 800,000 liters of spilled sewage into the environment, a hazard to both human and wildlife residents of the local area [1, 46].

2.1.3 Saudi Aramco

Saudi Aramco lost data on and the ability to use 30,000 computers in August 2012 after suffering an attack that used the Shamoon malware, which erased and overwrote hard drive data. Because of the target and the fact that the malware replaced critical system files with the image of a burning U.S. flag, the responsible actors likely desired to cause economic damage to the U.S. through the degradation of Saudi oil production [2, 3, 23, 113, 143]. Without the ability to export oil, Saudi Arabia loses one of its primary industries' incomes and consumer prices would increase throughout the U.S. following a constriction of supply.

2.1.4 Shushenskaya Dam

The impacts of SCADA malfunction, even outside of an attack scenario, can be drastic in financial and national security terms as well as in lives. An equipment malfunction at Shushenskaya dam in Russia in 2009 resulted in 75 lives lost and $1.3 billion in damages [89, p. 71]. Similar results could, theoretically, be achieved via a cyber attack.

2.1.5 Database Compromise

Other dams, specifically in the U.S., may be at risk of cyber attack. In January 2013, suspected Chinese hackers gained unauthorized access to the U.S. Army Corps of Engineers National Inventory of Dams database, which contains sensitive information on every one of the U.S.'s 8,100 domestic dams, many of which are used to generate hydroelectric power [73].

2.1.6 Shodan Exposure

Many ICSs are Internet-accessible, some without any authentication, creating vectors for attacks. An Industrial Control Systems-Computer Emergency Response Team (ICS-CERT) Control Systems Analysis Report originally published in 2010 and updated in 2013 with follow-on advisories examined the findings of Shodan, or Project SHodan INtelligence Extraction (SHINE), with regard to exposed Internet-facing ICS devices. Shodan scans the web, cataloging Internet devices by Internet Protocol (IP) addresses and ports. From one list of addresses, over 7,000 ICS-related devices in the U.S. alone were identified for remediation. The full report is only available via ICS-CERT's secure portal, which is not available to the public [56, 83].

2.2 Conflating Factors

The difficulty in developing appropriate mitigations for threats to CI is compounded by several factors inherent to the evolving technical and legal landscape of cyberspace. Together they create a need to establish widely accepted international norms in cyberspace, to develop offensive forces for deterrence effects, and to improve security culture and implementation in critical systems.

2.2.1 Anonymity and the Difficulty of Attribution

The Internet, as we know it today, is a partial mesh of public and private interests linked by major telecommunications providers. It was built for resiliency and assumed trust. Therefore, there are no robust authentication mechanisms built into the protocol upon which the vast majority of communications are carried: Internet Protocol (IP) . This creates a flexible underlying fabric that allows the Internet to evolve rapidly in many technological directions, but it also impedes reliable mechanisms to establish and authenticate trust relationships between people and machines interacting across its many interfaces. Although there are many identity markers that might enable activities-tracking, activity can typically only be tracked back to an originating IP address, which may not be the actual source. This makes cyber weapon positioning and other malware deliveries very difficult to definitively attribute to an actor. Luckily, this does not completely negate the inherent right of self-defense [8].

Since the Internet can provide anonymity, finding the source of an attack can be incredibly difficult. In the case of something like a Distributed Denial of Service (DDoS) attack, the probability of finding its source increases with the duration of the attack. However, even thorough analysis may not pinpoint the responsible entity. Ackerman illustrates the problem of accurate

attribution with a malware example, explaining that the Red October malware appears to be Chinese in origin at first glance, while further analysis yields Russian code. Even then, the authors may have had a Russian education but could be working for nearly anyone. As such, quick and decisive retaliation may strike a target other than the true source of the cyber attack [2].

2.2.2 Characterization of Intent

Another complicating factor is the inherent similarity between efforts taken in cyberspace toward espionage, corporate or otherwise, and pre-positioning (referred to in military terms as Operational Preparation of the Environment (OPE)), in preparation for a cyber attack. Cyber espionage requires the same basic access to a system through software (Trojan, backdoor, malware, and an unpatched vulnerability or zero-day exploit) or credential compromise , followed by privilege escalation. Cyber espionage's goal is to gain access to the sensitive areas of a system in order to harvest information therein. A cyber attack would leverage that very same access in order to leave behind malware or another payload designed to degrade or damage the system in some way. Both likely involve leaving some means for persistent access. Motivation for returning could range from continued data collection to triggering of the attack condition. Although various legal regimes have been tapped to rule on the matter of appropriate response, intent is sometimes impossible to derive and it may be the case that a prepared proactive defense, or even activation of the offensive team, in response to a potentially damaging cyber intrusion is required to ensure a catastrophic cyber attack is never allowed to occur on U.S. soil.

While so far there has been no cyber attack against the U.S of significant destructive physical effect, there are many examples of preparation. Just as it is in the case of a physical attack, the attacker must conduct espionage prior to an attack. In 2012, the frequently-consulted Information Security (InfoSec) company Mandiant Corporation published a report that all but conclusively links People's Republic of China (PRC) cyber espionage against a range of U.S. interests to a military organization under the People's Liberation Army (PLA) General Staff Department [90]. One must consider the delicate threshold at which espionage for one side translates as an act of war for the other side. Whereas espionage or Computer Network Exploitation (CNE) may or may not indicate a pending attack, it necessarily precedes one.

2.2.3 Legal Regimes

Questions about the legality of cyber action in the absence of clear code and case law complicates both the civilian protection mission and warfighter planning in cyberspace [61, pp. 26-27].

The jus ad bellum paradigm defined in Article 2(4) of the United Nations charter requires member states to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state." Under the argument of anticipatory self-defense, perhaps reasonable proof of intent to act in cyberspace, a nation state could legally deviate from the jus ad bellum paradigm under Article 51 of the United Nations Charter, individual or collective self-defense [39, p. 412]. These and other legal regimes, not to mention policy, are generally outpaced by technology. For example, the U.S. working definition of "cyber attack" only includes attacks that cause physical damage to property or injury to persons [77, p. 821]. However, attacks that degrade the operation of systems could result in equally deleterious effects. For example, the Russians demonstrated in conflict with Georgia that cyber attacks, like naval bombardment, can also be used to degrade or distract a target from the forthcoming kinetic military action [12, 77]. As such, in the case of cyber attack, a lack of internationally agreed upon definitions leads to ambiguity and could lead to an unnecessary escalation of force [29, 35, 46, 87, 114]. Legal ambiguity alongside the difficult characterization of intent and attribution together prompt the need to develop both widely accepted, legally defined terms and cyber forces to prepare for the eventuality of an attack and to deter attacks.

2.2.4 Code Reuse and Deterrence

One aspect of malware that is unlike kinetic munitions is that once it is released to attack its target, it can be used again and again by others who access it, even against its originator. This has contributed to the existence of a malware black market where those with malicious intentions can acquire exploits and those with good intentions can learn of the vulnerabilities so they can patch theirs and others' systems [2, 45]. The likelihood of code reuse largely negates potential deterrence effects for cyber weapons as they can be reused or retooled by the target and potentially third parties. Instead, reliance must be placed on prevention and system resiliency as well as organizational capability to respond, both to mitigate an attack in progress and to identify and debilitate the attacker. This response, especially to an attack against CI, must happen quickly and should not incur liability for a nation state acting in good faith in response to a cyber attack, even if attribution and characterization have not been adequately satisfied [39, pp. 415-416]. The establishment of such an international norm would raise the bar of cybersecurity worldwide as unprotected computers, which could be used as a staging area or midpoint for an attack, could expect to suffer the consequences for any malicious actions implicating their computer.

2.2.5 Permissive Culture and Poor Security Design

A permissive culture of security design and proper handling of InfoSec violations can also hinder the search for attribution and characterization of intent because it fosters a general attitude that involves a lack of attention to detail, which likely translates to a patchwork InfoSec program containing holes in its defenses. "Today's permissive cyber culture allows personnel to violate cyber policy in order to get the local job done. These local decisions frequently put the enterprise at risk and as a consequence, mission assurance at risk" [45, p 69]. Hard coded passwords are an example of manufacturers inadequately designing for security. Meanwhile, manufacturers are not held accountable for these obvious flaws [115]. Granger Morgan, Head of the Department of Engineering and Public Policy at Carnegie Mellon University (CMU), refers to several factors discouraging adequate security: the high additional cost of security measures, the externalities of these costs in the private model, the infrequent nature or low probability of a catastrophic event, and prioritization of other concerns under finite time and attention [92]. Even irresponsible researchers, through the discovery and publishing of ICS vulnerabilities, can allow malicious exploitation of these systems before they are patched. Researchers at DigitalBond, a SCADA security company, released a Metasploit exploit in January 2012 against multiple manufacturers' Programmable Logic Controllers (PLCs), a critical component of SCADA infrastructure, including exploits against "backdoors, lack of authentication and encryption, and weak password storage" that would allow attackers access to crash, stop, or change settings in systems [144]. There are several studies on the effects and externalities of disclosing vulnerability information to the public [9, 13, 14, 15]. A lack of attention to secure design combined with a lack of liability for software errors and lack of penalty for security violations has resulted in a vulnerability generating and sustaining computer culture.

2.2.6 Private Ownership with Public Responsibilities

Critical Infrastructure/Key Resources (CI/KR) in the U.S. is owned across public, private, and municipal interests, yet can have a regional or even national influence. At the root of DoD's very ability to function in its role to defend the nation from external threats is DoD's reliance on civilian owned and operated networks at some stage for 95% of its own communications. The very nature of cyberspace operations complicates distinction between civilian and military targets [77, pp. 852-853]. Meanwhile, the Federal Government has an obvious responsibility for the common defense. Although DHS has the preponderance of the homeland security portfolio, some functions are better accomplished with the Armed Forces. The DoD then needs to plan for

defense of CI/KR because of its reliance on CI and in preparation to effectively respond if called upon under Defense Support of Civil Authorities (DSCA) for Defend the Nation (DTN) [59, 80, 116]. At the same time, because of private ownership and operation of large sections of CI, the Federal Government, including the DoD, and industry owners and operators must cooperate to ensure the adequate protection and resiliency of CI functions.

Chapter 3

Evolving U.S. Policy

Shortly after the 1992 Oklahoma City bombing, 1993 first World Trade Center bombing, and a disruptive plot against the subways and bridges in New York, there was "...a growing concern about terrorist attacks, physical attacks, and focusing on soft targets and that meant critical infrastructure" [120]. This chapter provides an overview of the evolving policy that defines U.S. Government (USG)'s maturing role in Critical Infrastructure Protection (CIP), depicted in figure 3.1.

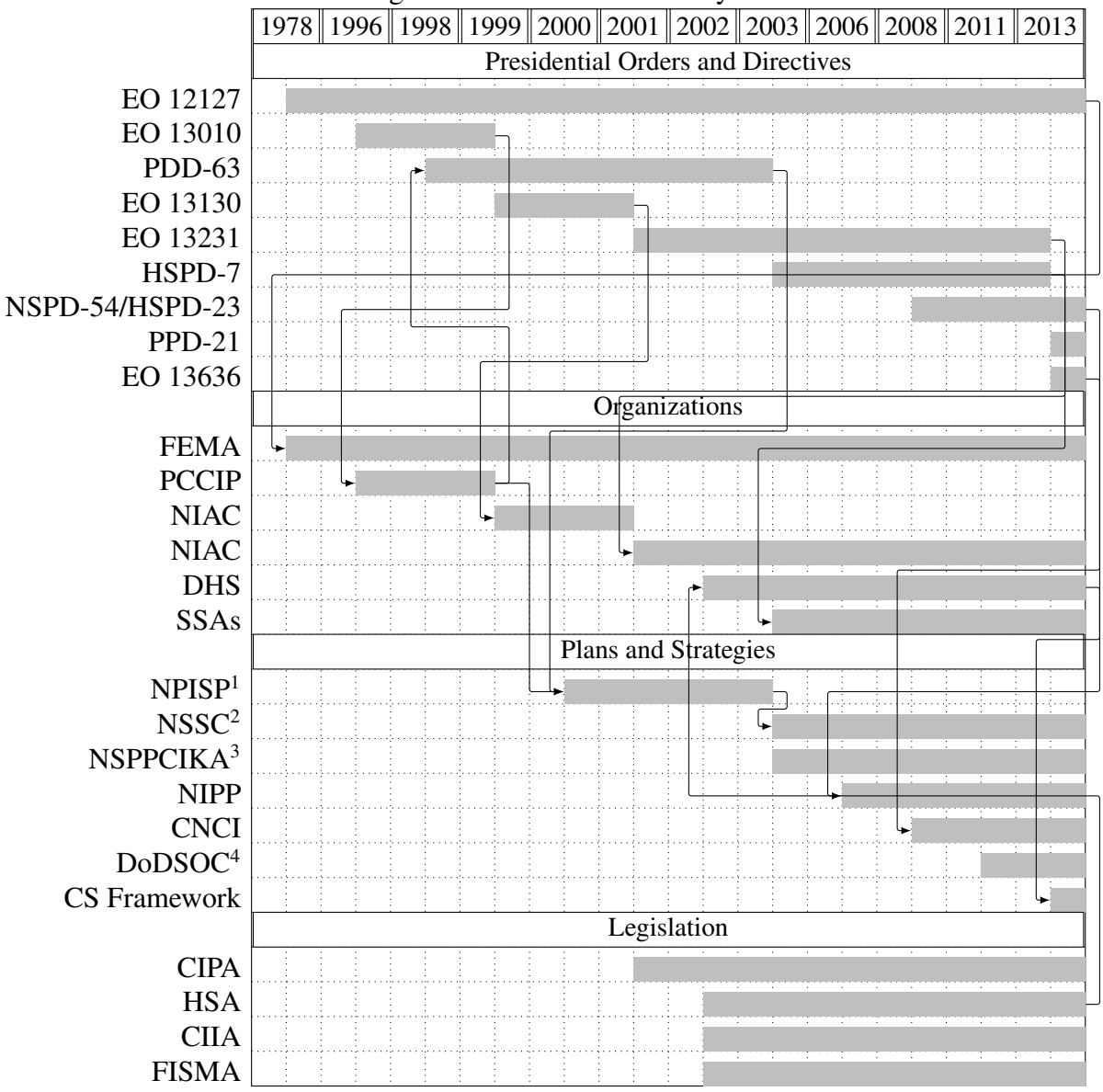
3.1 Creation of the Federal Emergency Management Agency

President Carter established and activated the Federal Emergency Management Agency (FEMA) with the Reorganization Plan No. 3 of 1978 and Executive Order (EO) 12127, respectively. Doing so consolidated the federal emergency management and response to improve the efficiency of the USG. Although not specific to Critical Infrastructure (CI) or cybersecurity, establishing FEMA was an early prerequisite for providing USG assistance to private entities in catastrophic circumstances [31, 76, 135]. FEMA is now organized under the Department of Homeland Security (DHS) [130, 136].

3.2 Executive Order 13010

President Clinton signed EO 13010, CIP, in July of 1996, establishing the President's Commission on Critical Infrastructure Protection (PCCIP) and acknowledging the potential of a cyber attack in addition to physical attacks. Although the PCCIP acknowledged the nation's ever-increasing dependence on cyber and the ever-increasing threat posed to cyber, it did not recommend any immediate action [36, 93, 102].

Figure 3.1: Evolution of Policy



[1]National Plan for Information Systems Protection [2]National Strategy to Secure Cyberspace
[3]National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
[4]Department of Defense Strategy for Operating in Cyberspace

3.3 Presidential Decision Directive-63

May 2013 marked the fifteenth anniversary since President Clinton signed Presidential Decision Directive (PDD)-63 on CIP, following the recommendations of the PCCIP. Richard Clarke, President Clinton's National Coordinator for Security, Infrastructure Protection, and Counterterrorism, led the committees on drafting both PDD-62 on Counterterrorism and Weapons of Mass

Destruction (WMDs) and PDD-63. Since PDD-63 is marked For Official Use Only (FOUO), it is available only in official channels. However, the Atlantic Council's Cyber Statecraft Initiative describes PDD-63 as all-encompassing on CIP and includes a section on protecting CI in the cyber realm. Furthermore, President Clinton later highlighted PDD-63 in his message in the National Plan for Information Systems (ISs) Protection (described in section 3.5), which PDD-63 called for, as one that focuses on vulnerability assessment of the nation's CI, including government-owned CI, and a Federal Government CIP plan. The USG acknowledged that approximately 85% (in 1998) of CI is owned and controlled by private industry and that the U.S. has an unprecedented and ever growing dependency on CI [38, 102, 120].

3.4 National Infrastructure Assurance/Advisory Councils

President Clinton signed EO 13130, National Infrastructure Assurance Council (NIAC), in July of 1999 to establish the NIAC. The NIAC's mission was to enhance the CIP public-private partnership, encourage risk assessments, and foster the development of Information Sharing and Analysis Centers (ISACs) [37]. Before the NIAC could meet, President Bush revoked EO 13130 by signing EO 13231, CIP in the Information Age, thus changing the council's name slightly to National Infrastructure Advisory Council (NIAC). Although the functions of NIAC fundamentally did not change, the EO also established the President's CIP Board to recommend CIP policies and programs [24, 93].

3.5 National Plan for Information Systems Protection

Called for by PDD-63, the White House released this plan in 2000 as an invitation for dialogue, hoping to stimulate the beginnings of a truly public-private partnership, instead of a mandated partnership, fostering domestic CIP. Going so far as to place "Version 1.0" on its title page, the plan's authors stressed the existence of ample room for improvement of this initial ISs protection plan, requesting that anyone with a constructive idea contribute to its revision [38, 93]. This led to ten town-hall meetings in which thousands of people and organizations provided input into the content and structure of the next version of this document: The National Strategy to Secure Cyberspace, described below in section 3.8.1 [26, 93].

3.6 Critical Infrastructure Protection Act of 2001

About a month and a half after the September 11th, 2001 terrorist attacks, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, which included the Critical Infrastructure Protection Act of 2001 (CIPA), was passed into public law. CIPA decreed that "a continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States" [129, §1016(b)(3)]. Continuing, it defines the policy of the U.S. toward CIP as one that focuses on proper risk management within a necessary public-private partnership. The focus on risk management instead of risk elimination is crucial because focus on risk elimination, which is nearly impossible in a computing environment, can lead to poor decision making and unnecessary expenses [120].

3.7 Homeland Security Act of 2002

The Homeland Security Act of 2002 establishes the DHS and contains several other acts including the Critical Infrastructure Information Act of 2002 (CIIA) and Federal Information Security Management Act of 2002 (FISMA). In addition to these acts, §223, Enhancement of Non-Federal Cybersecurity, allows DHS to provide cyber threat information on CI and technical assistance to improve CIP to private sector and other government entities upon their request [130].

3.7.1 Critical Infrastructure Information Act of 2002

The CIIA creates the CIP Program, which includes voluntary participation by private CI industry sharing their vulnerability information with the DHS. It also provides protection against liability and Freedom of Information Act (FOIA) disclosure for voluntarily shared Critical Infrastructure Information (CII).

3.7.2 Federal Information Security and Management Act of 2002

The FISMA is directed at improving the Information Security (InfoSec) of the USG's ISs. It distinguishes National Security Systems (NSSs) as a subset of ISs with more stringent requirements. It also amends National Institute of Standards and Technology (NIST)'s mission to include establishing standards and minimum requirements for ISs operated by the USG. Finally, FISMA

requires an annually updated inventory of all of the ISs throughout the USG, primarily for fiscal reasoning and secondarily for "monitoring, testing, and evaluation of information security controls..." [130, §1005(c)(2)-"(c)(3)(C)(iii)]. This inventory of ISs is only one of the beginning steps in a risk management or risk assessment process [86, 124]. An inventory of CI is not stipulated in the Homeland Security Act of 2002.

3.8 Two National Strategies

The White House released both of these two strategies in February of 2003, targeting two closely related fields: securing our nation's Critical Infrastructure/Key Resources (CI/KR) in cyberspace and securing them physically [93].

3.8.1 The National Strategy to Secure Cyberspace

In his opening address of the National Strategy to Secure Cyberspace, President Bush continued the public-private partnership mantra by describing it as the "cornerstone" of this cyberspace security strategy and appointing the DHS to lead the public side of the partnership. As such, this strategy calls for voluntary partnerships between government, industry, academia, and non-governmental groups to "secure and defend cyberspace" which functions as the "nervous system" of the country's CI/KR [26].

3.8.2 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

As its title suggests, this strategy focuses on the physical attack vector of CIP. The fundamental principle upon which this strategy exists is that the attacks of September 11th, 2001 exposed vulnerabilities and highlighted that the responsibility for the CIP subset of national security cannot be solely a government effort. Instead, it must be a shared responsibility, that is, through a public-private partnership [25].

3.9 Homeland Security Presidential Directive-7

In December of 2003, President Bush signed Homeland Security Presidential Directive (HSPD)-7, CI Identification, Prioritization, and Protection, thus superseding PDD-63. HSPD-7 primarily references and details how the executive branch will execute the Homeland Security Act of 2002.

Some of the highlights of HSPD-7 are that it clearly identifies terrorists as the primary threat to CI/KR and identifies CI sectors as including "information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping" and Key Resources as dams, government facilities, and commercial facilities [28, §15]. President Bush assigns the DHS Secretary as the national CIP coordinator and assigns various Sector-Specific Agencys (SSAs) as subordinates in the CIP efforts that are to provide assistance to the CI industry with vulnerability assessments and CI/KR risk management. In addition, HSPD-7 emphasizes the importance of information sharing within a public-private partnership and within the USG [28].

3.10 National Infrastructure Protection Plan

The National Infrastructure Protection Plan (NIPP) was first published by the DHS in 2006 through the coordination of various federal agencies and private sector entities. It aims to foster a national CI/KR protection through resiliency effort, involving both public and private sectors with lines of communication and coordination between them. The NIPP also emphasizes proper risk management including outlining a process for identifying CI entities and prioritizing them according to their level of risk based on the severity of impact if it was lost because of an attack. The DHS published an updated NIPP in 2009 to reflect the progress that has been made in the ever-changing and evolving CIP process. This document identifies eighteen CI/KR sectors [52, 76, 93].

3.11 Comprehensive National Cybersecurity Initiative

The Comprehensive National Cybersecurity Initiative (CNCI) was put into effect with President Bush signing National Security Presidential Directive (NSPD)-54/HSPD-23 in January 2008 and was expanded by President Obama in early 2009 based on the recommendations of his Cyberspace Policy Review. It consists of twelve initiatives – of which numbers 5, 11, and 12 directly concern CIP – to support three major goals: "establish a front line of defense against today's immediate threats, defend against the full spectrum of threats, and strengthen the future cybersecurity environment" [125]. CNCI-5 addresses the need for real-time cyber information and capability sharing within the USG to increase its efficiency in cyber operations. CNCI-11 acknowledges the potential for malicious actors to infiltrate the global supply chain of cyber products and aims to partner with industry to assist with developing acquisition risk management

and best practices. CNCI-12 aims to define the USG's role in implementing cybersecurity into CI/KR and emphasizes the importance of information sharing within a public-private partnership [125].

3.12 Department of Defense Strategy for Operating in Cyberspace

The Department of Defense (DoD) Strategy for Operating in Cyberspace, released in July 2011, only briefly touches on their role in CIP. It includes energy, banking and finance, transportation, communication, and the Defense Industrial Base (DIB) as types of CI and describes how our nation's CI is vulnerable to a debilitating attack from a myriad of different threats. To protect against attack, the strategy identifies a necessary and efficient cybersecurity relationship between the DoD and DHS and within the DHS's public-private partnership [47].

3.13 Presidential Policy Directive-21

Presidential Policy Directive (PPD)-21, CI Security and Resilience, signed by President Obama in February 2013, revokes HSPD-7, and necessarily repeats parts of HSPD-7, often with more detail on execution regarding facets like SSAs and other federal agency responsibilities. It also explicitly identifies sixteen CI sectors.[1] PPD-21 primarily focuses on the overarching vision of a national preparedness system with resilient CI and a shared responsibility of CIP and proclaims three strategic imperatives [110]:

1. "Refine and clarify functional..." CIP relationships within the USG to support the national effort. This imperative distinguishes between physical and cyber infrastructures as types of CI and directs a situational awareness center for each (National Infrastructure Coordinating Center (NICC) and National Cybersecurity and Communications Integration Center (NCCIC)), both operated by DHS, to be "inextricably linked."
2. "Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government." This strategic imperative identifies the foundation of effective CIP as efficient information exchange within a public-private partnership that provides adequate privacy and civil liberties safeguards on data.
3. "Implement an integration and analysis function to inform [CI] planning and operations decisions" through the NCCIC and NICC and be capable of collating, assessing, and inte-

[1] See table 4.1 for a comparison of sectors between the NIPP and PPD-21.

grating vulnerability and consequence information with threat information.

PPD-21 also sets deadlines of 12 July 2013 for DHS submitting an evaluation of the current public-private partnership, 10 October 2013 for updating the NIPP (section 3.10 above), and 12 February 2015 for submitting a CIP Research and Development (R&D) plan [110].

3.14 Executive Order 13636

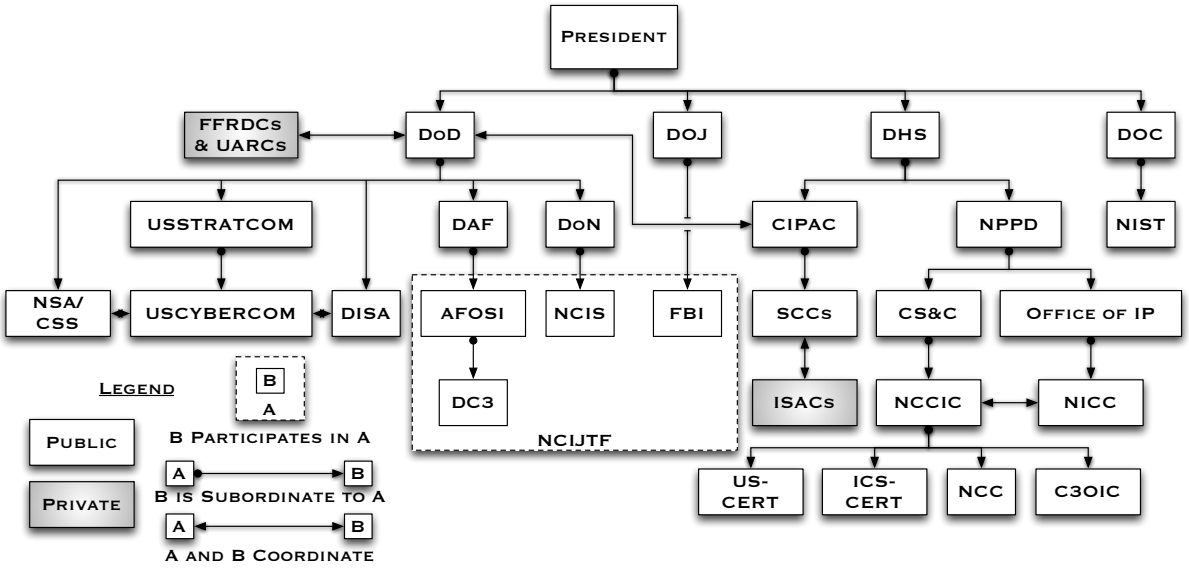
President Obama signed EO 13636, entitled "Improving CI Cybersecurity", on the same day he signed PPD-21 (see section 5.2, Collaboration by Executive Order). EO 13636 establishes several deadlines and provides amplifying instructions on existing legislation, namely the Homeland Security Act of 2002 (section 3.7 above). By 12 June 2013, the DHS and DoD were to work together to formulate a plan and deliver it to the President to expand the Enhanced Cybersecurity Services (introduced in §223, Enhancement of Non-Federal Cybersecurity, of the Homeland Security Act of 2002 (section 3.7 above) and codified in 6 United States Code (U.S.C.) 143 [130, 136]), including expediting the security clearance process for certain CI personnel and bringing private sector Subject Matter Experts (SMEs) into temporary government service. Privacy and civil liberties remain a priority with the requirement for the DHS Chief Privacy Officer and DHS Officer for Civil Rights and Civil Liberties to report on the level of compliance of safeguarding privacy within the DHS. President Obama directs NIST via the Department of Commerce (DOC) to develop the Cybersecurity Framework, incorporating input from industry. Since the information sharing program is voluntary, he directs the DHS Secretary to develop incentives to encourage owner and operator adoption of the Cybersecurity Framework and participation in the CII sharing program. Meanwhile, the Secretary of Defense (SECDEF) and General Services Administration (GSA) Administrator are to recommend to the President "...the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration...related to cybersecurity" [109, §8]. (An update to the Federal Acquisition Regulation (FAR) to include cybersecurity requirements is vital to the protection of CI.) By 12 July 2013, the DHS and SSAs were to have prioritized CI according to their risk related to catastrophic effects caused by a cybersecurity incident and confidentially notified corresponding industry entities of their level of risk. Then the SSAs are to report to the President via the DHS Secretary annually on the extent to which those private CIs considered high-risk adopt the Cybersecurity Framework. Finally, EO 13636 provides a requirement for the SSAs to report to the President within two years of NIST publishing the Cybersecurity Framework on whether they have appropriate authority to adequately meet their requirements specified therein [109].

Chapter 4

Force Structure by Organization

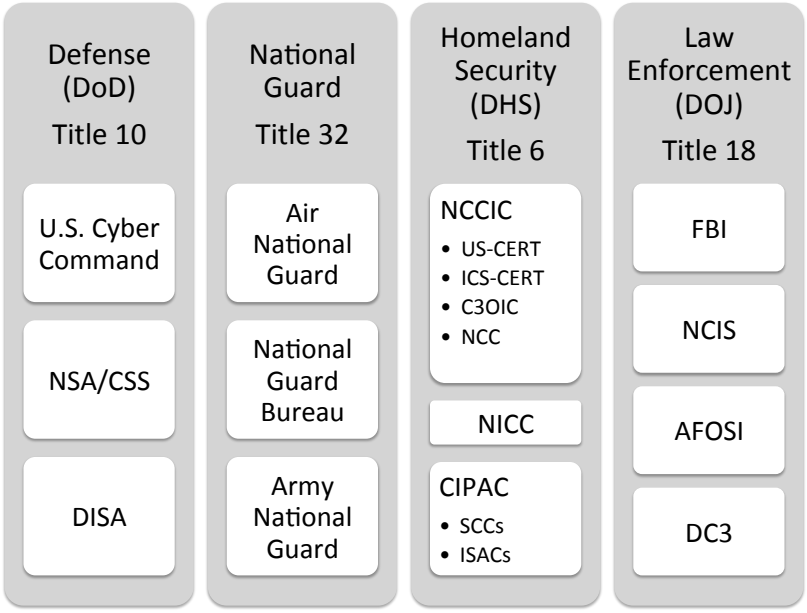
The ubiquity of the computing environment in our modern society, including through our Critical Infrastructure (CI), connects nearly every person, organization, and formerly isolated system. Because of this, they all have some need for computer security. However, this discussion is concerned with a level above system administration and network operation: verification, assurance, and response. The role of the government in Critical Infrastructure Protection (CIP) is to promote the welfare of the citizenry and provide for the common defense, which are most often achieved through regulation enacted by legislation and/or executive order. Figure 4.1 illustrates the relationships of the primary organizations discussed in this chapter. These organizations have evolved to both comply with existing and inform future policy and law.

Figure 4.1: U.S. Organizations with CIP Cybersecurity Roles



The Department of Defense (DoD) has a role in protecting the Defense Industrial Base (DIB) but no clear authority over infrastructure that is not owned by the DoD. Because of the way policy, regulation, and organizations have evolved over time, there exists a division of federal functions dividing the cyber domain into three areas: law enforcement functions which fall under the Federal Bureau of Investigation (FBI) through the Department of Justice (DOJ), foreign defense functions for which the DoD is responsible, and homeland defense functions over which the Department of Homeland Security (DHS) presides. The National Guard also plays a role in cybersecurity at the seams of Federal and State authorities. Figure 4.2 depicts these roles and organizations according to their United States Code (U.S.C.) Title authorities. Obviously, the division of responsibilities across federal government, between agencies and military commanders in the DoD, and across the multitude of ownership and operating arrangements of infrastructure across the country woven throughout the CI sectors makes identifying, thwarting, and mitigating the array of cyber attacks very difficult. This chapter identifies and describes the roles of various organizations that have cybersecurity functions for CI across the Federal Government.

Figure 4.2: U.S.C. Title Authorities Related to the Cybersecurity of CI



4.1 Department of Defense

[The DoD] is responsible for detection, prevention, and defense in foreign space, foreign cyber threat intelligence and attribution, security of national security and

> military systems; and, in extremis, defense of the homeland if the Nation comes under cyber attack from a full scope actor. [6]

While a convincing argument exists for the DoD alone to secure cyberspace and prevent foreign incursions into the systems controlling U.S. domestic CI, the Posse Comitatus Act of 1787 (18 U.S.C. 1385) limits the reach of DoD assets toward domestic purpose [7, p. 287]. Supervisory Control and Data Acquisition (SCADA) for most Critical Infrastructure/Key Resources (CI/KR) are operated as public, private, or semi-private commercial systems and thus fall under the purview of the DHS; DHS has the primary responsibility to defend domestic CI under both Title 6 U.S.C. and by Executive Order. However, the DoD has authority to protect systems owned, operated, and leased by the DoD under Title 10, as specified by policy. Also under Defense Support of Civil Authorities (DSCA), DHS can request support based on an extreme threat or overwhelming attack. DoD must also be prepared to aid in the defense of domestic CI. Per the Unified Command Plan (UCP), both U.S. Northern Command (USNORTHCOM) and U.S. Cyber Command (USCYBERCOM) must prepare for that task. DoD could provide technical support, attack prevention, or become actively involved to help defend the networks, depending on the nature of the request [80]. The specific circumstances or threat level that would prompt a request for assistance, the Command and Control (C2), coordinating relationships, and the flow of information for those events requires refinement and must be specified and relationships built in advance in order to ensure smooth transition and coordination under emergent conditions.

Specifically, per Secretary of Defense (SECDEF) guidance in the 2009 UCP, USCYBERCOM "is responsible for executing the specified cyberspace missions detailed in Section 18d(3) of the UCP as delegated by U.S. Strategic Command (USSTRATCOM), including working to...

> ...secure our freedom of action in cyberspace and mitigate the risks to our national security that come from our dependence on cyberspace... in coordination with mission partners, specific missions include: integrating cyberspace operations and synchronizing warfighting effects across the global security environment; providing support to civil authorities and international partners; directing global information grid operations and defense; executing full-spectrum military cyberspace operations; serving as the focal point for deconfliction of the DoD Offensive Cyberspace Operations (OCO); providing improved shared situational awareness of cyberspace operations, including indications and warning; and providing military representation to U.S. national agencies, U.S. commercial agencies, and international agencies for cyberspace matters. [80]

4.1.1 U.S. Cyber Command

Although "joint doctrine contains no guidance for cyber force presentation," [19] as Information System (IS) complexity and cyber threat sophistication and ubiquity grew, those responsible for defending the Global Information Grid (GIG)/Department of Defense Information Networks (DoDIN) across the services at all levels realized the need for unity of command in order to coordinate unity of effort for network defense. What started in the late 1990s as Joint Task Force-Computer Network Defense (JTF-CND) became Joint Task Force-Computer Network Operations (JTF-CNO) and later Joint Task Force-Global Network Operations (JTF-GNO), which merged with Joint Functional Component Commander for Network Warfare (JFCC-NW) to form the combined staff that instantiated USCYBERCOM as a subunified Combatant Command (COCOM) under USSTRATCOM [78, 88]. USCYBERCOM Initial Operational Capability (IOC) was originally scheduled for October 2009 but delayed until May 2010. Full Operational Capability (FOC) was declared in October 2010. The Office of the Secretary of Defense (OSD) decided to create USCYBERCOM as a subunified COCOM because of the immediacy of the threat compared to the relatively longer timeline required to establish a new COCOM [81]. Army General Keith Alexander was announced as the first commander of USCYBERCOM following Senate confirmation in May 2010, as an additional 'hat' for him to wear while continuing in his role as Director, National Security Agency (DIRNSA). At IOC, then SECDEF Robert M. Gates noted the change as an integration of an existing mission, one "in keeping with the Department's mission to protect and defend U.S. national security" [137]. USCYBERCOM's mission is to plan, coordinate, integrate, synchronize, and direct activities in order to "operate and defend the DoDIN and when directed, conduct full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries" [128]. USCYBERCOM provides support to the Geographic Combatant Commands (GCCs) by assigning Cyber Support Elements (CSEs) to them, through which they would coordinate any cyber-related planning in support of the GCCs' missions.

4.1.2 National Security Agency/Central Security Service

Executive Order (EO) 12333, issued in 1981 and amended in 2008, specifies that the SECDEF conducts Signals Intelligence (SIGINT) and Communications Security (COMSEC) activities as the Executive Agent of the U.S. Government (USG). It also charges DIRNSA/Chief, Central Security Service (CSS), to act on behalf of the SECDEF as the Executive Agent for COMSEC

of the USG. Furthermore, it defines National Security Agency (NSA) as one of the members of the Intelligence Community (IC) [27]. This results in a National Security Agency/Central Security Service (NSA/CSS) mission to "[lead the USG] in cryptology that encompasses both SIGINT and Information Assurance (IA) products and services, and [enable] Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances" [100]. The CNO portion of the mission statement was added in April of 2011 [84]. Meanwhile, NSA/CSS is also a Combat Support Agency (CSA), at least for the roles performed with respect to the DoD, responsible for acting as a supporting commander for the planning and conduct of military operations and countering threats to national security [60].

4.1.3 Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is a CSA that provides infrastructure to operate DoD networks globally. It performs acquisition and some network defense and mission assurance functions. A DISA Field Office as well as a support element were created to liaise with USCYBERCOM [80, pp. 211-213]. DISA was formerly the commander of JTF-GNO, responsible for operation and defense of the GIG. The decision to subsume JTF-GNO but not DISA into USCYBERCOM separated the organization and management functions (Defensive Cyber Operations (DCO) and DoD GIG Operations (DGO) at USCYBERCOM) from the acquisition, architecture, and some IA functions at DISA. While the segregation of these functions by organization is reasonable, complete separation is not possible. As a supported commander, USCYBERCOM must continually coordinate with and be able to exercise C2 of DISA.

4.1.4 Law Enforcement and Counterintelligence

During testimony in 2012, General Alexander described successful defense of the nation in cyberspaces as requiring "a coordinated response among several key players from throughout the government," namely the DHS, DoD, and FBI [6]. This coordination, without directive authority, is a common and necessary theme under separation of authorities within the current definitions in the federal legal code. The most active entities in the CI-cyber arena are the FBI, and two of the DoD service law enforcement arms, Air Force Office of Special Investigations (AFOSI) and Naval Criminal Investigative Service (NCIS). Each service law enforcement component has a responsibility to investigate cyber crimes and threats against service-specific assets.

4.1.5 Defense Cyber Crime Center

Subordinate to AFOSI, the Defense Cyber Crime Center (DC3) was established in 1988 and was designated as a national cyber center, as defined in National Security Presidential Directive (NSPD)-54/Homeland Security Presidential Directive (HSPD)-23, in 2008. Its mission is to "deliver superior digital forensics and multimedia lab services, cyber technical training, research, development, testing and evaluation, and cyber analysis capabilities supporting cyber counterintelligence and counterterrorism, criminal investigations, intrusion forensics, law enforcement, intelligence community, critical infrastructure partners, and information operations for the Department of Defense" [43]. DC3 is the operational focal point for the DoD's DIB Cybersecurity and Information Assurance (CS/IA) program, detailed in section 5.3.

4.2 Federal Bureau of Investigation

The FBI leads "the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud" [68]. They operate federally under Title 32 U.S.C. with responsibility for the detection, investigation, prevention, and response for malicious cyber activity detected in domestic space. The FBI leads the National Cyber Investigative Joint Task Force (NCIJTF) and, by Presidential Directive, is the coordinating organization for national cyber threat investigations [65]. Under the Comprehensive National Cybersecurity Initiative (CNCI), NCIJTF is a national cybersecurity center [66]. These responsibilities include all types of cyber threats; however the FBI also runs InfraGard, a program particularly focused on CI. The program began in 1996 as a response to Presidential Decision Directive (PDD)-63 and became a national "government and private sector alliance... to promote protection of critical information systems." InfraGard maintains representatives, one or more Special Agent InfraGard Coordinators, in each of the FBI's 56 field offices [67].

4.3 Department of Homeland Security

> DHS is responsible for securing unclassified networks for Federal Executive Branch civilian departments and agencies (the .gov domain). DHS works with owners and operators of CI/KR—private sector, state, and municipality-owned—to support cybersecurity preparedness through risk assessment, mitigation, and incident response capabilities. [55]

DHS is the "lead for coordinating the overall national effort to enhance the cybersecurity of U.S. CI and ensuring protection of the civilian Federal Government (.gov) networks and systems" [6]. Presidential Policy Directive (PPD)-21 assigns specific tasks to the DHS as the lead agency for CI cybersecurity. This role has evolved over time and coordination mechanisms are still evolving. For example, the DHS mentions in its 2011 Blueprint for a Secure Cyber Future, that the DoD will support the United States' execution of critical national defense mission responsibilities" through a DHS-DoD partnership, but there is no discussion of how the DHS and DoD will coordinate to elevate the security of cyberspace [54]. DHS is the 3rd largest department in Federal government and as the cyber threat has evolved, the cyber realm has been largest area of budget and personnel growth. Since the National Protection and Programs Directorate (NPPD), Secret Service, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and Customs and Border Protection (CBP), all part of the DHS, each have cybersecurity duties, even organizing to handle threats effectively is itself a challenge [98]. DHS coordinates with DoD representatives through the DHS-established Critical Infrastructure Partnership Advisory Council (CIPAC). The CIPAC's Sector Coordinating Councils (SCCs) create a means to engage all levels of public and private stakeholders in regular CIP-related discussions [51, 62].

4.3.1 National Cybersecurity and Communications Integration Center

> National Cybersecurity and Communications Integration Center (NCCIC) is staffed and structured to be an 'always on' multiagency incident response center with participation open to State, Local, Tribal, Territorial, and private sector partners. During steady-state operations, the NCCIC will utilize co-located partners and outreach mechanisms to coordinate steady-state cyber incident response activities and produce a common operational picture. Although each partner maintains its own operating mission, the execution of NCCIC's mission relies on coordinated operations, distributed execution, and common situational awareness. [53]

NCCIC has handled nearly a half million incident reports and issued over 26,000 alerts to private and public sector entities in the four years since it was instantiated into mid-2013. Government agencies such as the NSA and FBI are represented as well as the private sector [98]. NCCIC reports to the Office of Cybersecurity & Communications (CS&C) through the NPPD. NCCIC formally contains the Cyber & Communications Coordination & Operations Integration Center (C3OIC), U.S.-Computer Emergency Response Team (US-CERT), Industrial Con-

trol Systems-Computer Emergency Response Team (ICS-CERT), and the National Coordinating Center for Telecommunications (NCC). Other offices within the DHS also coordinate emergent issues through this operational entity [50, 63].

4.3.2 Office of Infrastructure Protection

Also within the NPPD is the Office of Infrastructure Protection which houses the National Infrastructure Coordinating Center (NICC), a 24/7 watch floor focused on physical CIP. Although NICC has had close working relationships with both NCC and US-CERT since shortly after DHS was created, after the signing of PPD-21, NICC made plans to move to physically co-locate with NCCIC by the end of 2013. Their parent offices also accomplish joint messaging and outreach regarding physical and cyber protection of CI. To accomplish the objectives outlined in EO 13636 and PPD-21, the Office of Infrastructure Protection and CS&C co-lead a DHS Integrated Task Force (ITF), which includes representatives from appropriate DHS components, Sector-Specific Agencys (SSAs) (such as DoD for the DIB), and other Federal agencies with roles in cybersecurity or CIP [62]. This cross-governmental collaboration is likely to forge professional ties that will endure beyond the life of the ITF. Meanwhile, within CS&C, both US-CERT and ICS-CERT have been busy discovering, reporting on, and providing technical assistance in the investigation of intrusions against CI. In 2012, US-CERT responded to 190,000 cyber incident responses while ICS-CERT handled 177 incidents with 89 site visits [98].

4.4 National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the Department of Commerce (DOC). As already described in section 3.14 above, EO 13636 tasks NIST with developing a security framework for CI. NIST is accomplishing this task through four working conferences across the country, open to government, industry, and academia in order to solicit those inputs (described in further detail in section 5.2).

4.5 Other Organizations

There are several other types of bodies involved in CI protection. There are regulatory bodies serving various functions involved in most of the CI sectors and membership organizations dedicated to information-sharing; most are just beginning to consider cybersecurity as a critical component of their operations. The financial services sector and DIB are probably the most

developed in terms of overall concern despite the lack of quality cybersecurity regulation.[1] In terms of utilities, the most developed regulatory model is in the electric sector in which the North American Electric Reliability Corporation (NERC). Within its mission to maintain electrical reliability, NERC has published nine CIP standards, eight of which directly relate to cybersecurity. These standards are required by legislation but developed collaboratively with and within industry. As they are subject to revision with approval[2] [103] and effectively require and carry assessment weight for the identification and protection of cyber assets related to the safety and reliability of the bulk electric system, they are a promising model for regulated private security of CI.

4.5.1 Research Centers

USCYBERCOM must develop the capability to model, war game, and eventually train for full-scale peer-on-peer cyber warfare, which is best facilitated through a Federally Funded Research and Development Center (FFRDC) or University Affiliated Research Center (UARC)—like a Center of Excellence [45, p. 51]. In the Fort Meade area, the headquarters of USCYBERCOM, NSA/CSS, and DISA, Johns Hopkins University (JHU) Applied Physics Laboratory (APL) is an obvious choice. The APL is largest of the UARCs and hosts such cutting-edge research as "Code DNA" [87]. UARCs have contractual relationships with DoD components and potentially other agencies that enable them to act as long-term agents toward developing future tool, technologies, and concepts [71]. Although commercial organizations sometimes have immense cyber laboratory resources, these government-funded research centers often have better value for the government because of their non-profit nature and long-term focus [87]. Other federal agencies, such as DHS, need to levy FFRDCs and UARCs similarly to develop the technologies they need to be effective in sensing, sharing, and mitigating cybersecurity threats to CI.

4.5.2 Information Sharing and Analysis Centers

There are fifteen Information Sharing and Analysis Center (ISAC) members of the ISAC National Council, which match imperfectly with the sixteen CI sectors (see table 4.1) [99]. The DHS Office of Infrastructure Protection meets with the ISACs through their monthly National Council meeting as a means to update members on DHS initiatives, programs, and exercise information.

[1] The Payment Card Industry Data Security Standard (PCI DSS) within the financial services sector probably comes the closest to quality cybersecurity regulation but still falls short in critical areas like personnel training [115].

[2] Version 5 of NERC's CIP standards is pending approval as of July of 2013.

The NICC and NCCIC also host ISAC and other industry representatives during incidents in order to promote "real-time private sector input into incident activities" [62].

Table 4.1: Critical Infrastructure Sectors versus Information Sharing and Analysis Centers

18 National Infrastructure Protection Plan (NIPP) Sectors [52]	**16 PPD-21 Sectors** [110]	**15 ISACs** [99]
Chemical	Chemical	—
Commercial Facilities	Commercial Facilities	Real Estate
Communications	Communications	Communications
Critical Manufacturing	Critical Manufacturing	Supply Chain
Dams	Dams	—
DIB	DIB	—
Emergency Services	Emergency Services	Emergency (EMR)
Energy	Energy	Electric Sector
Financial Services	Financial Services	Financial Services
Food and Agriculture	Food and Agriculture	—
Government Facilities	Government Facilities	—
National Monuments and Icons		—
Healthcare and Public Health	Healthcare and Public Health	National Health
Information Technology (IT)	IT	IT
—	—	Multi-State
Nuclear Reactors, Materials, and Waste	Nuclear Reactors, Materials, and Waste	Nuclear Energy Institute
—	—	Research & Education
Postal and Shipping	Transportation	—
Transportation		Maritime Security
		Public Transit
		Surface Transportation
Water and Wastewater Systems	Water and Wastewater Systems	Water

4.5.3 Owners and Operators

Because 90% of U.S. CI is privately owned (in 2013) [123] and governance has evolved over time, primarily outside of direct legislation, owners and operators have been asked to voluntarily cooperate with federal information-sharing programs. When it comes to designing and implementing security programs, John Sullivant, career security consultant and author of Strategies for Protecting National Critical Infrastructure Assets: A Focus on Problem-Solving, argues that industry needs to take the lead [124]. Increasing CI security is challenging for CI owners and operators, many of which operate as regulated monopolies that cannot arbitrarily raise rates to

pay for better security. Caitlin Durkovich, Assistant Secretary for Infrastructure Protection at DHS, explains that much CI is aging and overextended from its design. Meanwhile, ownership of infrastructure is stretched across the private sector as well as municipalities. DHS shares risk mitigation tools and works with owners and operators to assess risk and develop an understanding of the threats. DHS is now conducting quarterly cyber threat briefings for Chief Executive Officers (CEOs) of CI utilities [63]. Private interests want to be a part of the solution. "How to share at the speed of light" and how to appropriately, and quickly, handle classified information so that it can be of use where most needed are still challenges [63]. The ISACs remain the primary means for owners and operators to coordinate among themselves and the NCCIC for requests and reporting to the Federal Government.

Chapter 5

Current Efforts

> A determined and collaborated effort driven by regulators, security vendors, industry leaders, and politicians is required to protect our nation's critical infrastructure against disruptions and attacks. [72, p. 48]

5.1 Cybersecurity Coordinator

President Obama is serious about cybersecurity, as evidenced by his 2009 Cyberspace Policy Review, which resulted in his decision to reestablish[1] a White House Cybersecurity Coordinator. The Cybersecurity Coordinator is a member of both the National Economic Council and the National Security Counsel [69, 97]. He appointed Howard Schmidt who was followed by Michael Daniel upon Schmidt's resignation in June 2012 [97]. Daniel writes,

> ...cybersecurity is a cross-cutting problem, affecting not only all Federal agencies, but also state and local governments, the private sector, non-governmental organizations, academia, and other countries. It is a national security, homeland security, economic security, network defense, and law enforcement issue all rolled into one. As a result, it takes a truly cross-cutting response to address the problem, with the public and private sector working collaboratively. Within the government and the private sector, many organizations will need to work together in new and sometimes initially uncomfortable ways. We will also need a combination of technical, policy, and legislative tools to respond. [41]

[1] President Clinton appointed Richard A. Clarke as the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism [78]. Clarke continued to serve into the Bush administration before resigning in 2003, after which the White House Cybersecurity Coordinator position remained vacant until 2009 [35].

One Critical Infrastructure Protection (CIP) project undertaken by the Cybersecurity Coordinator beginning in January 2012 is the Electricity Sector Cybersecurity Capability Maturity Model initiative. It worked with executive level industry partners to institutionalize "processes within utilities and across the sector" and measure resilience against cyber threats [118]. Yet despite the recognized need for tools and other types of Executive branch action, the Cybersecurity Coordinator has no directive or budgetary authority, rendering him rather impotent as a cybersecurity advocate for Critical Infrastructure (CI) or anything else. One potential model for an empowered Cybersecurity Coordinator would be to establish the position as a Director of National Cybersecurity, modeled on the Director of National Intelligence (DNI), but provided budget and operational authority on cybersecurity across U.S. Government (USG) programs [102, p. 124]. Although this would add an additional layer of cybersecurity authority, it would centralize responsibility of the nation's cybersecurity efforts. This would necessitate Congressional appointment but would bring more capability to the position. Meanwhile, at least this Special Advisory to the President has the ear of the President and for the White House a moderately-sized staff (about ten people) [79]. The President continues to urge Congress to pass comprehensive cybersecurity legislation, specifically last year, the Cybersecurity Act of 2012 [108].

5.2 Collaboration by Executive Order

President Obama's 2009 60-day Cyber Policy Review highlighted a need to close the gap between governing laws and policies and growing technical capabilities [106]; the resolution of this mismatch was assigned to the Under Secretary of Defense for Policy and is ongoing. Meanwhile, several Executive initiatives, such as the President's National Strategy to Secure Cyberspace (section 3.8.1 above) and the Comprehensive National Cybersecurity Initiative (CNCI) (section 3.11 above) were set in motion to provide the framework for an "enduring national cyber policy" [80, p. 215]. These were extended for CIP through Presidential Policy Directive (PPD)-21 (section 3.13 above) and Executive Order (EO) 13636 (section 3.14 above), together requiring several specific actions that require annual review [109, 110]. The PPD also energized coordination of responsibilities for CIP across the Department of Defense (DoD), Department of Homeland Security (DHS), and Department of Justice (DOJ). Within the federal departments, the general divisions of authority by law are well understood, but the specific roles and coordination mechanisms for CIP have yet to be codified. However, there is high-level sharing, at least weekly, of threat information between them under CNCI-5 [40]. Meanwhile, top DoD and DHS officials entreat the private sector to contribute to solutions while supporting public-private initiatives and promoting

a strong culture of cybersecurity. Two such examples are DoD Chief Information Officer (CIO), Ms. Teri Takai speaking at a June 2013 Utilities Telecom Council-sponsored workshop supporting the development of the Public Safety Broadband Network (PSBN) [142] and GEN Alexander delivering a keynote address at the August 2013 Black Hat USA cybersecurity conference [20].

The National Institute of Standards and Technology (NIST) is working heavily with industry and academic participants in the development of the draft Cybersecurity Framework. After a preliminary workshop at the Department of Commerce (DOC) on April 3rd, 2013, Carnegie Mellon University (CMU) hosted the second Cybersecurity Framework workshop May 29-31. University of California at San Diego (UCSD) hosted the third July 10-12 and University of Texas at Dallas (UT Dallas) will host the fourth of four workshops in September of 2013 to help populate the initial body of standards, guidelines, best practices, tools, and procedures for the Framework. This open-conference method for inputs in the drafting of this framework represents an unprecedented public-private partnership effort to develop an actionable document that organizations can choose to adopt at various implementation levels, according to their needs and cost-benefit analyses. Most of the framers intend for this Framework to be an internal tool to help CI organizations buttress their cybersecurity and not as a cybersecurity grading tool for external entities.

Despite the great progress that has been made, some are, nevertheless, skeptical that once the Framework is in place, it will become mandated, at least to some extent (e.g., mandating the Framework for CI identified in the process directed in §9, Identification of CI at Greatest Risk, of EO 13636). A few have doubts of the Framework's success fueled by Secretary Napolitano's apparent lack of confidence in its future success, describing it as "an experiment" and stating "I don't think we have yet come to closure as to whether this is an appropriate thing to have as a shared responsibility" [98]. A few even considered the possibility that when (not if) the Framework fails, the DHS would be able to claim that involving the private industry in this "experiment" was a failure, necessitating legislative intervention. Refuting these sentiments, Mr. Robert Kolasky, Director of the DHS Integrated Task Force, led the closing remarks for the San Diego conference and represented the DHS's perspective of individual organizations' Framework implementation as merely laissez-faire. The DHS would like as many organizations to adopt the Framework but it cannot legally interfere in its adoption beyond an incentives approach [85]. NIST must publish a full draft of the Framework by 10 October 2013 to comply with the EO [109].

The DHS, as the lead department for coordinating the protection of most of domestic CI, has already produced several important products, including an analysis, with the DOC and Treasury,

on viable government incentives to encourage owner and operator participation in information-sharing and CI security initiatives. Yet despite significant progress facilitated by Executive fiat, including dramatic increases in funding to build the civilian workforce, legislation is still required to enable real-time sharing and create "additional law enforcement tools and hiring authorities similar to DoD to enable competitive hiring and pay scales" [98].

5.3 Defense Industrial Base Cybersecurity and Information Assurance Program

In May 2012, the DoD published an interim final rule to expand what was known as the Defense Industrial Base (DIB) Cyber Pilot, creating the DoD-DIB Voluntary Cybersecurity and Information Assurance (CS/IA) Activities. The DIB Cyber Pilot was a test program for Commercial Service Providers (CSPs) to "manage security services enhanced by government threat information to DIB companies" [6]. According to the Office of the Assistant Secretary of Defense for Public Affairs [138] and the Federal Register [107], the DIB CS/IA program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified Information Systems (ISs). The program includes bilateral "voluntary information sharing component under which DIB companies and the government agree to share cyber security information out of a mutual concern for the protection of Sensitive But Unclassified (SBU) information related to DoD programs on DIB company networks" [48]. The companies sign an agreement with the DoD and have an option to additionally participate in DIB Enhanced Cybersecurity Services (DECS), which involves the USG furnishing classified threat information to CSPs and select others as part of a joint activity with the DHS under its Joint Cybersecurity Services Program. This program is open to all DIB companies in order to reduce the threat aperture to DoD systems and information [48]. Measurements of success for this organization are required to see what types of interactions are most effective and the type of sharing formats that meet time requirements necessary to thwart threats. Yet this would seem to be a viable mechanism that bridges the need to provide threat warning information to DIB partners, most of which are already vetted for clearances and facilities to receive such information.

If proven successful, creating or expanding this effort in analogous relationships within other CI sectors should be a top priority for DHS in order to provide CI owners and operators with predictive threat warnings. Doing so would help achieve the EO 13636 requirement of expanding the DHS Enhanced Cybersecurity Services program. However, unlike the DIB, most CI sectors are not littered with cleared personnel and facilities, making expansion more difficult. Also, in

the current DIB CS/IA program, one impediment is that each company signs a separate "Framework Agreement" for voluntary information sharing with the DoD, which identifies particular executive level and other company representatives as points of contact for coordination [107]. This one-on-one means of administration may complicate matters. Additionally, as a voluntary organization, even though its membership has significantly expanded since beginning as the DIB Pilot, the DIB Voluntary CS/IA Activities program has little contractual ability to enforce adherence to a cybersecurity standard. The Enhanced Cybersecurity Services program also lacks serious enforcement mechanisms.

5.4 Preparedness through Exercises

Several recent annual exercises have put federal department leadership, legal staffs, and operations personnel into the same room to develop real-world coordination mechanisms, response frameworks, and sometimes simulated tactical responses to realistic attack and disaster scenarios. These include the DHS-led National Level Exercise 2012 (NLE 2012), and U.S. Cyber Command (USCYBERCOM)'s CYBER FLAG and CYBER GUARD exercises. Other tabletop discussions have been conducted either separately or in parallel to these exercises to further flesh-out legal and policy issues among staffs, both for Command and Control (C2) and for 'communication and coordination' in cases where directive authority does not exist.

For example, the DHS-led NLE 2012 examined national response plans and procedures in May of 2012 as part of a congressionally-mandated national exercise program. With a scenario including a cyber attack resulting in national ramifications, it served to exercise the National Response Framework (NRF), NRF Cyber Incident Annex, and the Interim National Cyber Incident Response Plan (NCIRP) [55]. In June 2012, President Obama convened an emergency cabinet meeting with department and agency officials as part of the simulation of a serious attack to the nation's CI [108].

USCYBERCOM conducted Cyber Wargame '13 (CW13) in June 2013 in order to "characterize the joint cyber resource and operational requirements for the 2018 epoch," in part toward a legal and policy framework that enables cyber operations required for that environment [139]. Fully one-third of the CW13 conference was devoted to policy discussion [140]. USCYBERCOM is exploring impacts across "grey-space" (industry, government, and social arenas) and red (adversary) and blue (military) operations with thought to offensive and defensive operations as well as exploitation. One key question is how to devise and establish policies and authorizations that match the cross-domain disciplines required for cyberspace operations. The sub-unified

Combatant Command (COCOM), USCYBERCOM, also seeks to identify shortfalls in enablers of cyber mission forces, such as organizational hurdles [141].

USCYBERCOM preceded CYBER GUARD 2013 with a legal and policy conference to synchronize an understanding among participants, including DHS, the National Guard Bureau, and multiple states' Guard forces of the potential use for the defense of CI of the various military authorities assigned by legal title. This could include Active and Reserve Duty Military under Title 10, Armed Forces [134] and State Guard or federalized Army or Air National Guard forces under Title 32, National Guard [132]. Not only are matters of legal authorities complicated but so are those of funding lines [104], chain of command, and communications channels. While forces operating at the direction of a state would be limited to defensive options, there is already resident in our Armed Forces an array of skilled cyber professionals who can fill a critical gap in state and federal emergency response mechanisms. Much of the legal and policy development involved in CYBER GUARD revolved around applying current force capabilities to the cyber realm while participating Guard units practice network defense and remediation in realistic CI outage and compromise scenarios at the tactical level. Although Title 10 forces are restricted domestically to several specific roles, state governors and/or DHS could use the Stafford Act or Economy Act to trigger support under Defense Support of Civil Authorities (DSCA) via a Request for Assistance, thereby prompting U.S. Northern Command (USNORTHCOM) to provide support on behalf of the DoD [59]. USCYBERCOM would then act as a supporting commander to USNORTHCOM for cyber actions. States can also work together under assistance agreements to remediate cyber incidents at a national level. Many aspects of the exercise prompted continued work in this area beyond the exercise. Included in the contributions was one state's draft Emergency Management Plan Domestic Cyberspace Response Annex, which might involve a request for state-to-state mutual assistance for cyber operations as established by a Cyber Emergency Management Assistance Compact (EMAC). Despite needing continued refinement, CYBER GUARD 2013 demonstrates progressive plans between the DoD, DHS, and state forces for the cooperative employment of mixed authorities in realistic cyber attack scenarios.

Chapter 6

Legislative Necessity and Obstacles

Private sector participation in executing the National Infrastructure Protection Plan (NIPP) is voluntary because the Executive branch of the government cannot mandate participation and Congressional action has encountered resistance. Meanwhile, many of the laws governing cyberspace are outdated and inadequate in providing the security governance necessary to ensure public safety. Much of the Executive effort toward cybersecurity improvement in private Critical Infrastructure (CI) has taken place under the form of recommendations, standards, and guidelines. Although documents such as Department of Homeland Security (DHS)'s 2011 System Security Recommendations for Standards Developers [57] are a good start, the government must reach beyond recommendations to requirements. CI owners and operators, understandably, are reluctant to embrace a mandatory standard on account of increasing their own already onerous compliance requirements. A standard that is flexible and developed in collaboration with industry, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, directed by Executive Order (EO) 13636, has the best chance of ensuring security without creating additional ineffective structures. Nevertheless, even the Framework is slated to remain entirely voluntary and there are doubts regarding the success of the overarching public-private shared Critical Infrastructure Protection (CIP) responsibility: DHS Secretary Napolitano laments, "Frankly I know that some in the private sector are suspicious about the Department of Homeland Security or any government agency's ability to fulfill its function under [Presidential Policy Directive (PPD)-21]. I have some question as to whether the private sector is willing to fulfill its function under the PPD" [98]. (See section 5.2 above for further discussion.)

Secretary Napolitano is not alone in the Executive departments with a desire for legislation to enable CIP. General Alexander, Commander, U.S. Cyber Command (COMUSCYBERCOM) and Director, National Security Agency (DIRNSA)/Chief, Central Security Service (CSS), re-

quests legislation that "...facilitates cybersecurity information sharing [within a public-private partnership], incentivizes [CIP] best practices and standards, [streamlines prosecution of cyber criminals], updates federal agency network security laws [including codifying DHS's role in cybersecurity], and [establishes] national data breach reporting requirements" [3]. There should also be a good security assessment program for CI owners to carry out to affect proper contingency planning [124]. To effectively involve government in a cooperation with industry to defend the nation's CI, there must exist a level of trust and quality communications for information sharing. There are several fundamental tenants described in the following sections that must be in place for this to work.

6.1 Presidential Powers in Defense of the Nation

> While the president has substantial inherent authority under the Constitution to take actions in defense of the nation, Congress should clarify the authority of the president to allow, or even require, the private sector to undertake measures necessary to protect the nation from a cyber emergency. [82, p. 13]

Any legislation must be careful in defining the authoritative boundaries of the President. If they are too constrictive, the President will not be able to issue the necessary orders to defend the nation. If they are too broad, the President may have too much authority, upsetting the separation of powers. With regard to execution, U.S. Cyber Command (USCYBERCOM) exists to ensure that the President can rely on the Information Systems (ISs) of the Department of Defense (DoD) and has military options available for his consideration when and if he needs to defend the nation in cyberspace [6].

6.2 The Cost of Adoption

Since private industry is in business because they are able to yield a profit, private entities will only participate in a voluntary program if they can still make profits as determined by a cost-benefit analysis. In other words, the cost of participating must be relatively low or it is likely to be prohibitively expensive. Private industry adamantly lobbies against mandatory participation because it degrades their ability to control security costs, thus having to pass increased costs onto their customers whether through direct rate increase or, in the case of regulated rates, lobbying for rate increases or government subsidies, which customers incur through taxes [29, 105]. There is likely a tipping point, which undoubtedly varies per industry, at which the outcome of a risk

assessment and Business-Impact Analysis (BIA) indicates that the cost of suffering an event of national significance has been reduced below the cost of further safeguarding against it. Such a risk-based approach must be used in an incentives model. This is why EO 13636 calls for incentives for participation in a CI cybersecurity program that should involve the NIST's Cybersecurity Framework and a public-private information sharing program [109]. However, unless the incentives can successfully garner the voluntary participation of the 'herd immunity' percentage of the sector, voluntary participation is inadequate. Furthermore, the unmitigated failure against an attack of a select few CI industries and components would be entirely unacceptable. This makes government ultimately responsible to act in the collective interest through legislative mandate in order to secure some guarantee. Even Secretary Napolitano explains that the voluntary private co-provision for the cybersecurity of CI "will not succeed unless there is total buy-in from the nation's owners and operators of critical infrastructure" [98].

6.3 Information Sharing Timeliness

As already described above, cyber incidents develop very quickly; therefore, an automated response is necessary to provide cyber threat signatures as close to real time as possible [82, 96]. As one company experiences a cyber attack, it needs to be able to share that threat signature with the government immediately. The government can facilitate dissemination of the signature across sectors quickly so that others can more readily defend against the attack. Meanwhile, the various agencies within government can investigate, analyze, and react according to the threat. Without cyber threat information sharing existing as an automated process, it is too slow to be reasonably effective in defending against a coordinated cyber attack.

6.4 Information Ownership

CI companies likely fear loss of revenue and a decline in their stock price in response to them being the target of a cyber attack. Their customers may lose trust and have a reason to, for example, use a different bank, go to a different hospital, etc. From many companies' perspectives, disclosing information to the government may as well be the same thing as disclosing the same information to the public because of the Freedom of Information Act (FOIA) [82]. Under FOIA, the U.S. Government (USG) must disclose certain information to the public upon request [135]. However, FOIA already provides exemptions for proprietary information and trade secrets; additional exemption under the Critical Infrastructure Information Act of 2002 (CIIA) may encourage

companies' negligence to properly safeguarding their cyber-physical systems because they can submit that information with the government and then not be able to be held liable for their negligence [122] (discussed further in section 6.5). Consequently, companies need to have a certain level of trust and confidence in the government before sharing cyber threat and attack information as well as an understanding that they will be held accountable for their own gross negligence. "Successful information sharing will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged" [93, p. 30]. "Currently, DHS signs Cooperative Research and Development Agreements (CRADAs) with companies that are willing to share information with the government, thereby invoking the protections of the CIIA" [82, p. 9]. This mechanism, however, is only adequate if the government requires a certain standard of cybersecurity practice as part of the CRADA. There must be the right balance of anonymity, privacy, and data protection versus openness in Critical Infrastructure Information (CII) sharing.

From the perspective of the government, sharing cyber threat information with industry has its risks as well, specifically with regard to classified threat information, which requires its own assurances. In other words, government needs to trust companies, or at least designated individuals at these companies, with classified cyber threat information. In addition, DoD components, while likely to depend on CI providers, are unlikely to have any direct authority over them. The only formal relationship that they have may be that of their service contract. Additionally, in the case of military mission classification or Operational Security (OPSEC) concerns, "private companies and utilities may not understand the scope of or specific dependencies between their businesses and the base's missions" [116, p. 10]. The USG uses security clearances as an indicator of the level of trust it has or needs to have in its employees and affiliates. Along with security clearances, however, comes necessary education and training in the proper handling, safeguarding, and destruction of classified information. Furthermore, these companies need to have trusted Intrusion Detection System (IDS) and/or Intrusion Protection System (IPS) equipment authorized to process, transmit, and receive classified information. This means that the equipment has been certified through the DoD Information Assurance Certification and Accreditation Process (DIACAP), which includes mechanisms for accountability for security violations [126].

As permitted by the Electronic Communications Privacy Act (ECPA), some states have laws requiring that parties at both ends of a communications stream consent to monitoring. This means that in these states, a company is not authorized to monitor, collect, or analyze its Internet traffic unless the other party in the communication consents of the monitoring, etc. However, cyber does not respect geographic or jurisdictional borders. While it may be relatively easy to get consent

from their customers and affiliates, it will be impossible to get consent from a cyber attacker; therefore, federal legislation needs to overrule these state laws to permit adequate participation of the CI industry partners in those affected states [82].

6.5 Liability

> While enhanced, and legally protected, cyber threat information sharing is necessary to meet the increasing threats to our critical infrastructure, it need not, and must not, come at the expense of Americans' privacy and civil liberties, particularly given the current availability of cost-effective technology to protect such information.
> [82, p. 7]

David Owens, Executive Vice President of Business Operations, Edison Electric Institute, a trade organization that represents 70% of electric power producers in the United States, explains that limited liability issues are the most significant impediment to private industry sharing information regarding cyber attacks. He agrees that enabling legislation is required. Besides the potential of public-private partnerships, there also exists a largely untapped the potential for collective action between interdependent industries [112]. A minimum national cybersecurity standard is required to protect CI, but in order to ensure incidents are reported and vulnerabilities mitigated, companies cannot be held liable when reporting compromise information to the government. Limitation of liability is one protection industry requires to bridge the gap and create "synergy between government and private industry as it [relates] to the security of Industrial Control Systems (ICSs)" [12, p. 14]. Currently, the ECPA and the Wiretap Act dissuade Internet Service Providers (ISPs) from monitoring traffic for threats because of the Personally Identifiable Information (PII) that data streams may contain. But technologies exist to monitor traffic without collecting, analyzing, or tracking PII in data streams and are inexpensive enough to be wide-spread throughout the ISP industry. Nevertheless, this is one of the areas where legislative attempts have particularly encountered resistance is with respect to information sharing [98].[1] With regard to private information about their customers like payment information or Social Security Numbers (SSNs), companies have an obligation to properly safeguard that information so that it cannot be used for unauthorized or malicious purposes. A failure to do so could lead to legal action by the Federal Trade Commission (FTC) [82].

[1] For an excellent review of cybersecurity-implicated governance and legislative proposals, see the Congressional Research Service report "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions" [69].

6.6 Privacy

One of the foremost aspects of an information sharing agreement between government and industry is public acceptance and the public is concerned about privacy protections. The inalienable rights granted by the Constitution breeds in Americans a certain disdain for anything resembling the notion of Orwell's "Big Brother," which some would regard as imminent if private industries were to provide extensive information about customers to the government, especially information containing PII [95, 96, 111]. As such, all of the cyber threat information that companies share with the government, and visa-versa, needs to be anonymous. Although there are some mechanisms that could allow the identification of individuals through their unique behavior signatures, this technology is not specifically covered under current law. Most states have data breach notification laws that require companies, in the case of a loss of their customers' PII, to notify these individuals. The requirements placed on companies by these laws vary widely from state to state, causing them unnecessarily high administrative overhead cost. One standardized federal law is in the best interest of companies, which they can pass-on to their customers, the American people, through lower administrative costs [82].

6.7 Legislative Mandate

Both CI industries and the public have valid concerns that need to be appropriately addressed, but nothing negates the collective security need for timely information sharing and the cooperative participation of industry in security controls for Supervisory Control and Data Acquisition (SCADA) and other critical systems. Participatory self-regulation of an adequate percentage of CI owners and operators is optimistic and a model unlikely to survive a major cyber attack. McAfee argues that, "...the nature of the new threats [that the CI] industry faces requires government involvement" [18, p. 24]. In the U.S., this translates to legislation. Although regulatory regimes are necessary, they are ineffective alone. Direct coordination is required. Information sharing programs must be jointly developed by shareholders, institutionalized, regulated, and assessed for effectiveness. The Congressional mandate to establish the North American Electric Reliability Corporation (NERC) is a good example of a legislated requirement effectively owned, developed, and managed by a consortium of those it effects. A similar legislative approach to information-sharing and cybersecurity requirements is imperative for all CI sectors.

Chapter 7

Recommendations

7.1 Organization and Missions

Kori Schake, a Hoover Institution research fellow and former Department of State (DoS) Deputy Director for Policy Planning, observed that "democracy is messy," [117] but does it have to be this messy? Unfortunately, there is no omniscient entity in the U.S. that understands all of the Critical Infrastructure Protection (CIP) efforts being executed and could perfectly reorganize our federal structures to best accomplish their missions. Reorganizations and changing requirements by executive mandate have attempted to better align federal department missions to mitigate current and potential cyber threats against Critical Infrastructure (CI). The missions and needs continue to evolve with changing technology and security trends. This is necessarily very "messy." But cross-organizational collaboration, despite extant legal and policy divisions, is possible through practice. Current social science research studies "us" verses "them" or in-group/out-group behavior. When it comes to cyber, the Department of Defense (DoD), at all levels, cannot act in an us-verses-them manner with the rest of the Federal Government, nor with industry. Within appropriate legal boundaries, we have to act as a team and teams may be held together by leaders, such as prompted under the executive mandate provided by Presidential Policy Directive (PPD)-21 and Executive Order (EO) 13636, but they are often effective because of trust woven over time into mid-level working relationships [33].

Within DoD, the force structure for cyberspace is still evolving with U.S. Cyber Command (USCYBERCOM) at its epicenter. The current dividing line for generating cyber capabilities within organizations lies with acquisition and infrastructure on one side and the operation and defense of the network on the other [40]. In this paradigm, Offensive Cyberspace Operations (OCO) and its supporting Computer Network Exploitation (CNE) are properly a specialty within

and well-connected to daily network operation and defense. One author argues that "by virtue of its advertised mission alone, USCYBERCOM must become the de facto network architect and chief advocate, for it cannot direct defensive action on a network incapable of executing its commands" [10]. USCYBERCOM certainly must act as an architect and advocate in order to get the capabilities it needs, but ultimate responsibility for that mission does not mean that USCYBERCOM as an organization has to accomplish all of those functions internally. The mission of designing, acquiring, operating, acquiring intelligence, and defending a network for the entire DoD as well as bringing deterrence through preparedness to attack is too wide of a function set to accomplish within one organization, especially at current manning of under 1,000 personnel. Besides, there already exist organizations whose primary mission is one or more of those functions. For acquisition and infrastructure support, Defense Information Systems Agency (DISA) has primacy for DoD networks (see section 4.1.3) and National Security Agency/Central Security Service (NSA/CSS) handles intelligence (see section 4.1.2), so instead what is required is a clear mandate as a headquarters and a stable civilian workforce in order to develop as an organization that can effectively manage problems and delegate tasking instead of tackling every aspect of analysis internally.

One recommendation from the Defense Science Board (DSB)'s 2010 Enhancing Adaptability of the U.S. Military Forces study was to implement red and blue teaming for cyber systems within each of the Combatant Commands (COCOMs) and services [44, p. 90]. While this sounds appealing, such distributed forces would neither train to the same standard nor have adequate surge capabilities. Placing this capability under USCYBERCOM instead of spreading it across the DoD enables identification, prioritization, and coordinated mitigation of cross-cutting vulnerabilities based on their level of risk to the global enterprise [44, p. 91]. Meanwhile, a hybrid of centralized training and prioritization paired with customer-focused tasking is possible through the design of the Cyber National Mission Forces (CNMFs). Each Geographic Combatant Command (GCC) will be able to prioritize concerns specific to its Area of Responsibility (AOR) through the Cyber Combat Mission Teams (CCMTs), which will focus on target development in support of COCOM missions. These CCMTs, the Cyber National Mission Teams (CNMTs) and the Cyber Protection Teams (CPTs) comprise the operational-level CNMFs under USCYBERCOM. The CNMTs have an offensive role in defense of the nation and the CPTs focus on hardening, operating and maintaining the Department of Defense Information Networks (DoDIN). There will be 13 CNMTs, 27 CCMTs, and 68 CPTs [34].

In testimony before Congress in 2013, General Alexander testified to an assigned active-duty military and civilian end-strength at USCYBERCOM of 834 with "strong" but "evolving"

service components for a combined "force mix" of 11,000 between the headquarters and service components: Fleet Cyber Command/Tenth Fleet, Army Cyber Command/Second Army, Air Force Cyber Command/24th Air Force, and Marine Forces Cyber Command [119]. However, it is unclear how many of the non-headquarters level service forces are actually operationally available to be directed toward USCYBERCOM-specified missions. The establishment of the CNMFs is an important step, but it is only the first.

7.2 Separation of USCYBERCOM and NSA/CSS

General Keith Alexander, Commander, U.S. Cyber Command (COMUSCYBERCOM) and Director, National Security Agency (DIRNSA)/Chief, Central Security Service (CSS), argues that being dual-hatted over both of these organizations removes barriers to inter-agency information sharing and makes full-spectrum cyber operations a more efficient undertaking [3]. Alexander, however biased his opinion might be, describes USCYBERCOM's co-location with National Security Agency (NSA) as promoting "intense and mutually beneficial collaboration" [119] and indeed, both organizations have significant cyber responsibilities toward the same ultimate purpose. Some CNE is certainly required to enable both Computer Network Defense (CND) or Defensive Cyber Operations (DCO) and Computer Network Attack (CNA) or OCO[1]. It is also true that significant cyber expertise exists within NSA and that as a mature organization, it can impart many positive characteristics on the young USCYBERCOM. For example, woven into the fabric of NSA is a culture of security as well as a regime of careful oversight. Because of the close relationship between CNE and both DCO and OCO, the USCYBERCOM-NSA working relationship must continue to be one of incredible synchronicity [87]. However, there are subtle differences between Computer Network Operations (CNO) for intelligence purposes and that for military preparations. USCYBERCOM must be able to control their own resources or effectively task those of NSA in order to cultivate the latter.

> Discovering which of an adversary's system and network components are useful targets requires full-spectrum intelligence support. Intelligence support assets are almost always in short supply and, in the case of those needed to support offensive cyber planning, the shortage is even more acute. In some cases, a component of the system or network of interest may already have been fitted with some level of access arising from non-offensive cyber intelligence priorities. Such access may be helpful

[1]CNA is sometimes defined as specifically having a physically destructive effect, while OCO more generally refers to cyber operations for offensive purposes that may or may not include CNA

> but still not offer the granularity needed for precise military targeting. For example, an intelligence agency may have access on a network used for intelligence exploitation and USCYBERCOM may desire to develop an order of battle plan against that target. Intelligence interest may stop at a server or router in the network, to conduct intelligence operations at those points. USCYBERCOM's mission requires situational awareness and access down to the terminal or device level in order to support attack plans. USCYBERCOM would need to work with intelligence agencies to ensure the portions of the system they disable don't disable critical intelligence assets. In other cases, no pre-existing access will be in place and the access effort must start from scratch. History shows that such situations can take a long time (i.e., months or years) to achieve results. USCYBERCOM, and its supporting Service Component Commands, must be the driving force to surface the doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF)/Unity-of-Effort gaps and advocate for requisite gap-closure actions. The Intelligence Community (IC) and other United States Government Departments and Agencies, with distinct and overlapping authorities, also have key supporting responsibilities. Given the nation's cyber defensive posture, time is of the essence in developing a broader offensive cyber capability. [45, pp. 49-50]

In his 2010 Senate confirmation hearings as the nominated COMUSCYBERCOM, General Alexander explained that "there will be, by design, significant synergy between NSA and USCYBERCOM, each organization will have a separate and distinct mission with its own identity, authorities, and oversight mechanisms" [80]. However, this does not mean a dual-hatted commander is necessary or appropriate. USCYBERCOM needs to build capabilities far beyond the functions of NSA. Despite synergies, each organization has significant and potentially conflicting responsibilities as well as enormous capability and influence, which could translate to the stretching of boundaries for expediency or, more likely considering the oversight regime, *perceived* abuses of those boundaries.

Equities or Intelligence Gain-Loss (IGL) valuation is built into the planning process, with a recommendation made by the supported COCOMs after risks have been articulated by the IC. General Alexander currently serves as focal point for DoD OCO in accordance with the deconfliction process directed in National Security Presidential Directive (NSPD)-38 but also as the IC representative for cyber and Signals Intelligence (SIGINT) [80, p. 218]. This may have the result of resolving issues without escalation in matters of disagreement to the National

Security Council for resolution, but it also makes it very difficult for the same commander to be on both sides of an issue, which may leave one side underrepresented.

The somewhat conflicting priorities and the diversity of their mission portfolio must make the combination of commanding USCYBERCOM simultaneous to directing NSA a difficult one to balance. Sometimes, representation of only one role is expedient or necessary while the other is not even considered. For example, GEN Alexander addressed Black Hat USA 2013 only in his role as Director of the NSA [5]. NSA/CSS is already the combination of a Combat Support Agency (CSA) with National level functions and the SIGINT capabilities of the military services. This is a complex and little understood enterprise to an outsider, and one burdened by everything from infrastructure development to significant intelligence oversight requirements. COMUSCYBERCOM, on the other hand, not only has the responsibility to operate and defend the DoDIN, consisting of all networked DoD assets in approximately 15,000 DoD network enclaves [6], but now, also to act as the strategic-level commander of the newly-established operational-level CNMFs and, as a sub-unified commander, has another layer in his reporting chain through U.S. Strategic Command (USSTRATCOM) to the Secretary of Defense (SECDEF), as compared to DIRNSA who reports directly to the Undersecretary of Defense for Intelligence. The three organizations have been tied together by the very experienced and well-respected General Alexander and perhaps necessarily so for USCYBERCOM's infancy. But in the long run, these organizations and their mission portfolios are too diverse and of significant technical depth to be effectively led by one person.

Simultaneously, while their authorities complement each other and are bound by personality, USCYBERCOM's significant dependence on NSA/CSS forces and capabilities severely handicaps USCYBERCOM's ability to operate effectively. The USCYBERCOM-NSA dual-hatting arrangement should be only a temporary arrangement while USCYBERCOM gains the ability to function effectively as a COCOM staff. Some of USCYBERCOM's current challenges lay in the lack of and evolving cyber policy and force presentation as well as the relative youth of the organization under its current form and authorities. This may be adequate in the initial expansion of USCYBERCOM's own manpower and infrastructure, but in the long run will hinder USCYBERCOM from evolving into a relevant and capable Functional Combatant Command (FCC) in its own right. USCYBERCOM needs its own permanent spaces, elimination of routing through USSTRATCOM, true acquisition professionals in charge of cyber acquisitions, and better coding in general of billets as the services struggle to throw bodies at the demand. Significant growth in terms of technical training is required to develop a large pool of technically credible cyber warriors at all levels. Cyber is inherently Joint, yet all of the services have different pipelines. It

makes sense that they bring different strengths but there should be a common level of qualification and understanding when it comes to computer security and some common understanding of the whole of government functioning at the USCYBERCOM level.

It is also very difficult for USCYBERCOM to compete effectively through its service components when each service necessarily largely puts its conventional requirements (ships, planes, tanks, etc.) ahead of cyber development. As a result, USCYBERCOM cannot direct the services to staff a certain number of personnel and "each of services classifies what they consider cyber differently" [40]. For USCYBERCOM to effectively drive doctrine, training, and personnel development, a U.S. Special Operations Command (USSOCOM) model is suggested. It seems like the newly established CNMF teams provided to each GCC will perform as forces organic to USCYBERCOM, much like the USSOCOM model. But this responsibility needs to extend further, so that USCYBERCOM functions as the "DoD's primary FCC to organize, train, and equip CNA and Computer Network Defense-Response Action (CND-RA) forces" [19, p. 33]. Lt Col Dawley, ANG, also argues for the designation of USCYBERCOM as a FCC in its own right by means of the Unified Command Plan (UCP), arguing that "authority to organize, train, and equip its subordinate forces will allow it to more readily build, harness, and exploit capabilities within this newest field of warfare" [42, p. 130]. USCYBERCOM's interagency orientation also marks USSOCOM as an appropriate model. Legislative change to Title 10 United States Code (U.S.C.) could define man, train, and equip mission space, along with budgetary authority, based on the USSOCOM model, to USCYBERCOM as a FCC [42], just as USSOCOM was established in 1987 [127, 134]. In fact, the SECDEF alone could decide to promote USCYBERCOM to full COCOM status as Title 10 U.S.C. authorizes the SECDEF to direct and control all of DoD, including its organization [134].

Timing is critical. While, ideally, USCYBERCOM would have its own building and completely fielded forces before executing a separation, there are few individuals who could effectively serve as both USCYBERCOM and DIRNSA. General Alexander has served as DIRNSA since 2005, longer than any other DIRNSA, and as COMUSCYBERCOM since its Initial Operational Capability (IOC) in 2010, thus reaching the typical three-year combatant commander tenure in 2013. The duties of DIRNSA should be turned over to a three-star general or flag officer with significant experience in intelligence, specifically SIGINT, if not also cyber. Sufficient time should be allowed to complete the disjoining of staffs and offices. Once complete and upon his reassignment or retirement, General Alexander could turn-over his position as COMUSCYBERCOM to a four-star general or flag officer with significant cyber experience. Finally, the SECDEF should promote USCYBERCOM to a FCC, ideally one with the man, train, and equip missions

so that USCYBERCOM can centrally lead joint force development of cyberspace. Meanwhile, throughout a separation, consideration must be given to reiterate and further formalize the CSA supporting relationship of NSA/CSS to USCYBERCOM and the channels for collaboration, in order to preserve the benefits of the current dual-hatted relationship.

7.3 Growing the Cyber Force

7.3.1 Offensive Forces

> The best defenders will be those who understand what can be accomplished from an offensive point of view (the reverse is also true). Creating cyber warriors with expertise in offensive and defensive cyber skills should be encouraged. [45, p. 62]

In March 2013, General Alexander testified that the new CNMF teams that are being developed to respond to a national level incident would be staffed with both civilian and military personnel and operate both under orders from the SECDEF and with some authorities from NSA. The DoD and USCYBERCOM are now "integrated in the machinery for National Event responses so that a cyber incident of national significance can elicit a fast and effective response to include pre-designated authorities and self-defense actions where necessary and appropriate," which allows these actions to take place within the existing National Response Framework (NRF) and National Incident Management System. Although they will be in keeping with prior policy, the cyber additions are still evolving as the "new standing rules of engagement for cyber currently under development will comply with and support recently issued policy directives on U.S. cyber operations" [119]. This is a plan with a bright future, but necessitates DoD growth in its uniformed cyber forces as there are significant limitations insofar as legal protections for civilians and contractors involved in cyber warfare. Civilians acting as belligerents can be legally attacked by the opposing force anywhere at any time and are not protected from acts that would be prosecutable domestically as are military members acting under orders [61, p.28].

The DSB report even implies that the DoD must adopt the tactics of our adversaries, to include "using surrogates in exploitation and offensive operations" and "sharing intellectual property with local industries for economic gain" [45, p. 5]. While these tactics seem excessive, a change in focus for the DoD from defense to deterrence is required; yet we currently suffer from a lack of a national cyber deterrence strategy [121]. "Defense-only is a failed strategy" [45, p. 29]. The DoD must be able to train for cyber warfare against peer-capable entities [45, p. 9]. The growth of the CNMFs is an important step toward developing offensive capabilities. The

bottom line is that the U.S. must have a formidable offensive cyber force to preserve freedom of action in cyberspace. Clear public articulation of a comprehensive national cyber strategy is also required. Even if offensive capabilities are never deployed, they will act as a powerful deterrent.

7.3.2 Realistic Training

The DSB recommends defining incentives for personnel achieving higher levels of certifications alongside the formalization of a viable OCO career path: "Current operational exercises offer limited realism for operating with degraded cyber systems" [44, p. 99]. Realistic operator training and feedback-capable secure systems are required to develop cyber forces that can recognize, react to, and usher a system to recover from compromise or fault. In 2010, the DSB warned that degradation to any of a range of critical support systems, including communications and cyber networks, can significantly impact how and if the mission can be accomplished with the degradations [44, p. 75]. For example, while the use of 'white card' injects, in cases where the simulation of degradation is difficult, accomplishes the basic training objective, it falls short in teaching cyber forces to recognize degradation and decide when and practice how to revert to back-up systems or apply the correct Tactics, Techniques, and Procedures (TTPs) [44, p. 77]. USCYBERCOM has conducted CYBER FLAG annually since 2011 in an attempt to make cyber events as realistic as possible for exercise participants and to integrate them into other warfare areas [75, 91].

7.3.3 Certification

Cyber warfare is an inherently joint job that requires joint training, but the services are responsible for developing individual training pipelines and supplying qualified personnel to USCYBERCOM, which results in vastly different preparation in personnel between services. USSOCOM, by comparison, has been granted authority to develop strategy, execute budget proposals, train assigned forces, ensure equipment interoperability, etc., with approximately 57,000 assigned between its headquarters and various components, including four service components and a sub-unified COCOM. Of course, USSOCOM has had over twenty years to grow to its 2013 size and capability [127], but the differential demonstrates the paucity of total USCYBERCOM forces, numbering about 11,000 in 2013 [119]. This force must grow to fill the surge in demand for this developing warfare area. In building capability, however, balance must be maintained between the need to increase cybersecurity manning quickly and the prolonged timeline required to develop a cadre of skilled personnel. Unfortunately, the rapid growth in demand has resulted in

an imbalance in the number of technically demanding billets as compared to qualified personnel [22]. Rectifying this imbalance will take time and effort.

One training model would be to establish a U.S. Government (USG) Cyber Corps, with the incentives, recruiting policies, and continuing training necessary to attract and retain the necessary talent [102, p. 124]. This would require no significant realignment of service responsibilities, but personnel specializing in cyberspace operations would be formally identified within their primary career fields, similar to the Navy Space Cadre. Yet across both the services and the Federal Government, a formal and singular qualification pipeline is necessary, much like that of Acquisition Professionals. DoD 8570.01-M, a manual entitled "Information Assurance Workforce Improvement Program," is a step in the right direction for having consistent Information Assurance (IA) training pipelines according to the level of cyber interaction (i.e., user, technical, managerial, accrediting authority, architect, and CND service provider) and tracks certification compliance throughout the DoD, yet it falls short in that each of the DoD components is responsible for training and certifying its personnel instead of one entity like USCYBERCOM [16].

Although a comprehensive understanding of our changing federal structures and the policies in place takes years to develop piecemeal, training that specifically addresses current policy, problems, and organizational roles and relationships could be inculcated in cyber-related positions across the federal government. Building this kind of working-level understanding of the structures in place, despite their changing nature, would go a long way to ensure an adequately networked federal workforce and cooperation across agencies. While this should be part of the Cyber Corps concept, in terms of current efforts, such training could be housed under Track 4 (Cybersecurity Workforce Training and Professional Development) of the National Initiative for Cybersecurity Education (NICE) [101]. This training would need to involve guest speakers from trade associations and private operators of CI. It could begin with an outline of information from this paper and a small group of curriculum specialists could pull in the better-informed experts to cover everything omitted here. Besides baseline training for mid-level cybersecurity professionals across the USG, cross-imbedded personnel between departments would go a long way to connecting issues between sister offices at different agencies. USCYBERCOM could act as the joint focal point for the DoD. However, alongside training on policy, authorities, and organizational reach for mid-level career military officers is the equally important training of equivalent officials across the USG. Engendering a baseline understanding in the personal and institutional knowledge of the workforce in terms of policies, relationships, and doctrine across federal cyber responsibilities is just as critical to effective whole of government response to emerging threat scenarios as technical acumen. Civilian employees should accomplish a rotational tour, similar to

those used within the IC to cross-train and gain a firm understanding of the structure and missions of other federal organizations surrounding this mission. The cross-pollination of Department of Homeland Security (DHS) and DoD on matters of cybersecurity is particularly relevant if DoD is to be able to smoothly transition to defensive and/or offensive operations in support of a potential national response to CI attack.

It is critical that not only Enlisted personnel understand the technical details of cyber operations but also leadership at all levels of the Officer Corps. Currently, "few commanders know or understand the intricate network of devices, hardware, and software that provide them the combat capabilities they depend on to accomplish their missions" [45, p. 67]. Those holding the ultimate responsibility for cyberspace actions, especially OCO (when cyber becomes a weapons platform), need to understand the technical details of the actions they perform. Whether employed as a missile or chaff, OCO can cause real physical damage and have strategic implications of international consequence. However, unlike hitting a button to launch a missile and understanding its general capabilities in terms of range and damage potential, cyberspace actions often have uncertain and changing potential. Conventional missiles fly through air or water and impact ground or other targets; the physics is well understood. But cyberspace "missiles" travel though cyberspace, a technically intricate and changing medium. Leadership must understand the technical details of the medium and proposed action. Anything less is equivalent to delegating weapons release authority to the advice of a junior technician. Failing to understand how the weapon works and, therefore, the significance of the collateral effects it may cause or even how it might fail is simply irresponsible.

7.3.4 Retention

Although growing the cyber workforce properly will take time, several avenues should be explored to incentivize gaining and retaining a highly qualified workforce:

- Competitive pay through the use of technical pay on par with flight pay and other retention incentives for both Enlisted and Officers, such as the Navy Critical Skills Retention Bonus for Navy Surface Warfare Officer (SWO) Department Heads [32] and reenlistment bonuses for highly skilled operators [58]
- Adaptation of career progression milestones in order to assign personnel with designated cyber skills to roles demanding those skills
- Creation of Officer and Enlisted career paths that allow for multiple consecutive tours that support rotations through planning and executing CND, CNE, and CNA operations

- Financial incentives and promotions based in part on higher levels of industry-recognized certification

These incentives must be both financially and professionally enhancing. This could help stem the hemorrhages of highly trained and motivated personnel from attractive private offerings, as personnel are still in very high demand across industry despite fiscal constraints.

7.4 Federal Acquisition Regulation Update

Some hold that the series of presidential directives have done little to increase cybersecurity as "change in the U.S. is driven by three things: liability, market demand, and regulatory (usually federal) action" [21]. As a regulatory action, changes to the Federal Acquisition Regulation (FAR) could demand a higher standard in vendor security which would encourage the market at large to move in that direction with regard to CI as well as other key national security capabilities. While there are now laws that regulate both Personally Identifiable Information (PII) and Protected Critical Infrastructure Information (PCII), the only mandatory mechanism in place as of 2013 to protect sensitive government data is that which is enforceable through contractual relationships. The FAR regulates the basic language of how contracts are written across the federal government. In a world full of threat vectors, common sense dictates that an adoption of a minimum cybersecurity posture should be required before being allowed to do business with the federal government. Incorporating requirements in the FAR to adhere to a certain standard of cybersecurity, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework for CI-related contracts, would sew cybersecurity into the fabric of every government contract and would go a long way to provide mechanisms for accountability for the protection of publically-funded Intellectual Property (IP) and other sensitive data as well as the integrity of critical Information Systems (ISs).

In execution of EO 13636, CI Cybersecurity, of February 2013, the General Services Administration (GSA), DoD, DHS, and FAR Council have taken a step via a Request for Information (RFI) to the public asking for information that can be used to improve acquisition regulations related to cybersecurity [70]. Follow-through in consultation with government cybersecurity professionals as well as industry will enable the development of changes that do not create undue compliance burdens for industry while simultaneously holding private companies accountable for the loss of critical information through cyber compromise.

7.5 Standardization

Standardization of cybersecurity measures, best practices, and, perhaps most importantly, definitions poses many challenges across the CI industry, primarily because of the diversity in systems and the owning organizations. Just as the DoD Information Assurance Certification and Accreditation Process (DIACAP) exists for DoD ISs, there should be a standardized process for the Certification and Accreditation (C&A) of CI. There are several existing industry security assessment models including the American Society for Industrial Security (ASIS) general risk assessment, Center for Chemical Process Safety (CCPS), American Water Works Association (AWWA), North American Electric Reliability Corporation (NERC), Defense Sector, General Ports, Food and Agriculture Sector, Transportation Sector, NIST, and South Carolina Security Advisory Committee models, but the value added by having one overarching model for CI could provide an added level of assurance in the reliability of these and other subordinate models. John Sullivant proposes that such a model should have the following components [124, p. 59].

- Characterize mission, objectives, culture, and political and social dependencies
- Characterize physical structure, configuration of facility, and physical security features
- Characterize operational systems, functions, processes, protocols, and external and internal dependencies and influences
- Identify and categorize assets as critical or non-critical
- Define range and levels of threats and consequence of events against asset attack
- Assess vulnerability to operational systems, functions, processes, protocols, and external and internal dependencies
- Evaluate effectiveness of in-place protective measures and external and internal dependences and influences
- Evaluate effectiveness of security strategies, security organization, and security operations
- Evaluate effectiveness of proposed protective measures and cost-benefit analysis
- Identify residual vulnerability, acceptable risk, and compensatory measures
- Review assessment process, findings, observations, conclusions, and report for quality assurance
- Report assessment results and prioritized action plan, milestone schedule, and budget estimate

This is a continuous process because of how the threat landscape is ever evolving [124]. Yet a lack of standard and widely accepted cyber-related definitions continues to be the bane of policy makers, network operators, and network defenders alike. Does the term cyber relate to all aspects of ISs, just the defense aspect, or the attack and espionage aspects as well? What constitutes a cyber attack? Does it matter whether it originates from a State or non-State actor? What does active defense mean? Is it a type of attack? These terms questions and others must be answered authoritatively and they must be widely accepted for anyone to proceed effectively in cyber [29, 40, 87, 95]. Clear definitions for cyber in joint doctrine and policy are essential to formalizing and unifying the field across the services and across government. The effort led by NIST for the development of the Cybersecurity Framework should be just the beginning.

Chapter 8

Further Research

There are several other potential programs that are likely to directly or indirectly result in improved cybersecurity for Critical Infrastructure (CI), which bear further examination.

8.1 Public Awareness Campaign

In conducting security assessments, the personnel who are properly trained to operate or maintain those systems regularly are the best people to yield accurate results. Although this helps remove any misinterpretation in the assessment, it may be difficult to communicate the true state of a system with the executives of the organization if they do not also have a management-level education in Information Security (InfoSec) and Critical Infrastructure Protection (CIP). As a result, the C-level executives (i.e., Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Financial Officer (CFO), etc.) may not be able to properly conduct their enterprise level risk management decisions [124]. Increasing C-level executive general Information Technology (IT) knowledge is likely to result in better decision-making outcomes for a company; however, effective InfoSec measures necessarily require increased personnel training throughout organizations, not just in the IT departments [2]. A higher baseline of IT knowledge across the company's workforce is likely to result in less-risky computing behaviors and thus a higher level of network hygiene. This higher standard is particularly important for companies operating CI. Meanwhile, because no license is required to sit in front of a keyboard, the general public would also benefit from a better baseline understanding of InfoSec. This would enable an educated public, both more responsible online and with a voice to their elected representatives to ensure appropriate action and moderation of some of the sometimes exaggerated fears of much-needed cyber legislation. How to best conduct training, education and elevate awareness within the CI

workforce and for the general public is left for further study. Research is required to demonstrate results on a cost-effective basis.

8.2 Information Sharing Mechanisms

The Internet allows for attacks at 'cyberspeed' or in real-time so defenses and mitigations must happen just as quickly. Appropriate software can shorten human-in-the-loop delays but a lack of tool integration impedes industry's ability to protect CI from cybersecurity threats [72, p. 46]. There is a need to standardize the incident and threat reporting formats for CI toward automation to improve the timeliness of information-sharing. Although there are many formats for incident reporting, National Institute of Standards and Technology (NIST) should select one in consultation with industry and formalize it as the standard. An open and universally recognized standard for incident reporting will enable the design of interoperable automated sharing tools, significantly improving incident reporting timeliness, therefore shortening the time lapse from discovery to mitigation. In addition, there are potential improvements to be made to the organizational mechanisms currently in place enabling appropriate and timely information-sharing for coordination of CIP.

A better alignment and increased participation of CI owners and operators to information-sharing organizations like the Information Sharing and Analysis Centers (ISACs) by CI sectors would likely enhance the effectiveness of the existing construct. Some sectors have closer relationships and willingness to share than others [79], yet the ISAC participation and coordination have been measured in a scientific and effects-based manner in only very limited ways [14, 17]. A comparative evaluation between sectors' ISACs is recommended to determine effective methods to encourage participation and increase the effectiveness of their coordination both within their sectors and with government organizations. What percentage of participation is required in a CI sector to achieve critical mass in order to adequately hedge against a cyber-invoked emergency? This may vary per sector and may be measured quantitatively by percentage, including weighted percentages according to their respective sizes as well as qualitatively by for what and how they use the ISAC relationships. Certainly, active and complete participation where industry itself collaboratively self-regulates would be ideal.

8.3 Critical Infrastructure Industry Memberships for SCADA Testing

Another program to consider is that of paid-memberships to a consortium of CI companies for the purpose of funding unbiased Supervisory Control and Data Acquisition (SCADA) vulnerability research. Currently, Idaho National Laboratory (INL) conducts vulnerability testing on SCADA systems but the results are not immediately shared with CI sector industries who have those systems installed. Meanwhile, many of the industries using these systems are largely forbidden from communicating amongst themselves regarding their own vulnerabilities and compromises due to anti-trust restrictions [74]. This arrangement causes SCADA manufacturers to weight the business cost-basis of designing for security as well as creating patch updates more heavily than the potential security compromise implications for the systems in which they are installed. More substantive collaboration among CI SCADA owners and operators and SCADA/Industrial Control System (ICS) vendors on cybersecurity issues would help improve the security-by-design of SCADA systems. This is especially important in SCADA equipment, which typically have life cycles that often span 20 or more years. In this way, security issues can be identified and remediated early in the development and deployment cycles [30]. Better consumer awareness on the part of CI owners and operators through verified, unbiased testing will also help to increase SCADA manufacturers' focus on security as a critical quality attribute in everything they design. The collated funds from major CI industry players, while perhaps small compared to current investments in cybersecurity on a per company basis, would amount to significant research funding. The appropriate mechanism to create such a consortium and provide funding dollars and limited collaboration among CI owners and operators within the legal restrictions for federally sponsored lab funding and anti-trust regulation is left for further exploration.

Chapter 9

Conclusion

There will always be some malicious activity in progress in cyberspace against a U.S. Critical Infrastructure (CI) or U.S. Government (USG) entity. Some say it is only a matter of time until a major cyber attack is launched against the U.S. CI [6, 8, 94]. If our nation's CI suffers a devastating compromise or attack, the Department of Defense (DoD) likely will be asked get involved, through U.S. Northern Command (USNORTHCOM) to assist the Department of Homeland Security (DHS) as the primary agency for defense of CI. If the attack were accomplished through cyber means, DoD resources, particularly those under U.S. Cyber Command (USCYBERCOM), would be applied to the problem behind those within CI itself, those at the state level, and those at DHS. There are many demonstrated cyber means to accomplish such an attack. Cyber is the ultimate medium to strike against the homeland from afar, without the barriers of our significant traditional defenses. The organizations poised, authorities established, and efforts underway to thwart such a cyber attack against CI are manifold, complex, and distributed. Continued work is necessary, especially in terms of coordination mechanisms and working relationships that facilitate an operational understanding of inter-organizational, department, inter-government, and owner and operator capabilities. At these organizational seams, preparedness for a cyber attack aimed at CI has markedly improved, primarily through Executive level actions in the last two years, even though their effectiveness remains untested. Meanwhile, several major improvements to these efforts are required, both within Federal government and within DoD policy. Possible improvements include separating the command structure of USCYBERCOM from that of the National Security Agency/Central Security Service (NSA/CSS) and elevation of USCYBERCOM to a Functional Combatant Command (FCC), growing the cyber force offensively and defensively through more realistic training while employing civilian certification programs and retention mechanisms, updating the Federal Acquisition Regulation (FAR) to accommodate the

rapidly changing nature of cyber, and developing and mandating a cybersecurity standard of CI. Most important, however, is to recognize that "the USG does not have a monopoly on insight and ingenuity" [124, p. 39]. The public-private partnership is, therefore, critical to the successful defense of our nation's CI. Legislation is needed to enable that partnership to grow to include a critical mass of CI owners and operators while adequately handling privacy and liability protection concerns. Only then will technology-assisted information-sharing relationships together with resilient infrastructure confidently thwart attacks in real-time, bridging and evolving beyond the current awkward shared public-private responsibilities for defense of CI.

Acronyms

AFOSI Air Force Office of Special Investigations.
AOR Area of Responsibility.
APL Applied Physics Laboratory.
ASIS American Society for Industrial Security.
AWWA American Water Works Association.

BIA Business-Impact Analysis.

C2 Command and Control.
C3OIC Cyber & Communications Coordination & Operations Integration Center.
C&A Certification and Accreditation.
CBP Customs and Border Protection.
CCMT Cyber Combat Mission Team.
CCPS Center for Chemical Process Safety.
CEO Chief Executive Officer.
CERT Computer Emergency Response Team.
CERT-CC Computer Emergency Response Team Coordination Center.
CFO Chief Financial Officer.
CI Critical Infrastructure.
CI/KR Critical Infrastructure/Key Resources.
CII Critical Infrastructure Information.
CIIA Critical Infrastructure Information Act of 2002.
CIO Chief Information Officer.
CIP Critical Infrastructure Protection.
CIPA Critical Infrastructure Protection Act of 2001.
CIPAC Critical Infrastructure Partnership Advisory Council.
CMU Carnegie Mellon University.
CNA Computer Network Attack.
CNCI Comprehensive National Cybersecurity Initiative.

CND Computer Network Defense.

CND-RA Computer Network Defense-Response Action.

CNE Computer Network Exploitation.

CNMF Cyber National Mission Force.

CNMT Cyber National Mission Team.

CNO Computer Network Operations.

COCOM Combatant Command.

COMSEC Communications Security.

COMUSCYBERCOM Commander, U.S. Cyber Command.

CPT Cyber Protection Team.

CRADA Cooperative Research and Development Agreement.

CS/IA Cybersecurity and Information Assurance.

CS&C Cybersecurity & Communications.

CSA Combat Support Agency.

CSE Cyber Support Element.

CSP Commercial Service Provider.

CSS Central Security Service.

CW13 Cyber Wargame '13.

DAF Department of the Air Force.

DC3 Defense Cyber Crime Center.

DCO Defensive Cyber Operations.

DDoS Distributed Denial of Service.

DECS Defense Industrial Base (DIB) Enhanced Cybersecurity Services.

DGO DoD Global Information Grid (GIG) Operations.

DHS Department of Homeland Security.

DIACAP DoD Information Assurance Certification and Accreditation Process.

DIB Defense Industrial Base.

DIRNSA Director, National Security Agency.

DISA Defense Information Systems Agency.

DNI Director of National Intelligence.

DOC Department of Commerce.

DoD Department of Defense.

DoDD Department of Defense Directive.

DoDIN Department of Defense Information Networks.

DOJ Department of Justice.

DoN Department of the Navy.

DoS Department of State.

DOTMLPF doctrine, organization, training, materiel, leadership and education, personnel and facilities.

DSB Defense Science Board.

DSCA Defense Support of Civil Authorities.

DTN Defend the Nation.

ECPA Electronic Communications Privacy Act.

EMAC Emergency Management Assistance Compact.

EO Executive Order.

F.R. Federal Register.

FAR Federal Acquisition Regulation.

FBI Federal Bureau of Investigation.

FCC Functional Combatant Command.

FEMA Federal Emergency Management Agency.

FFRDC Federally Funded Research and Development Center.

FISMA Federal Information Security Management Act of 2002.

FOC Full Operational Capability.

FOIA Freedom of Information Act.

FOUO For Official Use Only.

FTC Federal Trade Commission.

GCC Geographic Combatant Command.

GIG Global Information Grid.

GSA General Services Administration.

HSI Homeland Security Investigations.

HSPD Homeland Security Presidential Directive.

IA Information Assurance.

IC Intelligence Community.

ICE Immigration and Customs Enforcement.

ICS Industrial Control System.

ICS-CERT Industrial Control Systems-Computer Emergency Response Team.

IDS Intrusion Detection System.

IGL Intelligence Gain-Loss.

InfoSec Information Security.

INL Idaho National Laboratory.

IOC Initial Operational Capability.

IP Internet Protocol.

IP Intellectual Property.

IPS Intrusion Protection System.

IS Information System.

ISAC Information Sharing and Analysis Center.

ISP Internet Service Provider.

IT Information Technology.

ITF Integrated Task Force.

JFCC-NW Joint Functional Component Commander for Network Warfare.

JHU Johns Hopkins University.

JTF-CND Joint Task Force-Computer Network Defense.

JTF-CNO Joint Task Force-Computer Network Operations.

JTF-GNO Joint Task Force-Global Network Operations.

MITS Master of Information Technology Strategy.

NCC National Coordinating Center for Telecommunications.

NCCIC National Cybersecurity and Communications Integration Center.

NCIJTF National Cyber Investigative Joint Task Force.

NCIRP National Cyber Incident Response Plan.

NCIS Naval Criminal Investigative Service.

NERC North American Electric Reliability Corporation.

NIAC National Infrastructure Assurance Council.

NIAC National Infrastructure Advisory Council.

NICC National Infrastructure Coordinating Center.

NICE National Initiative for Cybersecurity Education.

NIPP National Infrastructure Protection Plan.

NIST National Institute of Standards and Technology.

NLE 2012 National Level Exercise 2012.

NPPD National Protection and Programs Directorate.

NPS Naval Postgraduate School.

NRF National Response Framework.

NSA National Security Agency.

NSA/CSS National Security Agency/Central Security Service.

NSPD National Security Presidential Directive.

NSS National Security System.

OCO Offensive Cyberspace Operations.

OPE Operational Preparation of the Environment.

OPSEC Operational Security.

OSD Office of the Secretary of Defense.

OUSD(AT&L) Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

P.L. Public Law.

PCCIP President's Commission on Critical Infrastructure Protection.

PCI DSS Payment Card Industry Data Security Standard.

PCII Protected Critical Infrastructure Information.

PDD Presidential Decision Directive.

PII Personally Identifiable Information.

PLA People's Liberation Army.

PLC Programmable Logic Controller.

PPD Presidential Policy Directive.

PRC People's Republic of China.

PSBN Public Safety Broadband Network.

R&D Research and Development.

RFI Request for Information.

SASC Senate Armed Services Committee.

SBU Sensitive But Unclassified.

SCADA Supervisory Control and Data Acquisition.

SCC Sector Coordinating Council.

SECDEF Secretary of Defense.

SEI Software Engineering Institute.

SHINE SHodan INtelligence Extraction.

SIGINT Signals Intelligence.

SME Subject Matter Expert.

SSA Sector-Specific Agency.

SSN Social Security Number.

SWO Surface Warfare Officer.

TTPs Tactics, Techniques, and Procedures.

U.S.C. United States Code.

UARC University Affiliated Research Center.

UCP Unified Command Plan.

UCSD University of California at San Diego.

US-CERT U.S.-Computer Emergency Response Team.

USA PATRIOT Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

USCYBERCOM U.S. Cyber Command.

USG U.S. Government.

USNORTHCOM U.S. Northern Command.

USSOCOM U.S. Special Operations Command.

USSTRATCOM U.S. Strategic Command.

UT Dallas University of Texas at Dallas.

WMD Weapon of Mass Destruction.

Glossary

authentication utilizing digital credentials to assure the identity of users and validate their access [130].

availability ensuring timely and reliable access to and use of information [130].

Business-Impact Analysis an analysis of system or program requirements, processes, and interdependencies used to characterize contingency requirements and priorities in the event of a significant disruption [124].

Combat Support Agency an agency with a portion of its mission involving support for operating forces engaged in, planning for, or conducting military operations, including support during conflict, or in the conduct of other military activities related to countering threats to U.S. national security. This mission is focused on providing support to echelons at the Combatant Command (COCOM) level and below and may not encompass the full scope of an agency's mission [60].

confidentiality preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information through physical, technical, and electronic penetration or exploitation [124, 130].

cost-benefit analysis the comparison of options and alternatives related to the decision to commit assets or funds [124].

counterintelligence information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations [124].

Critical Infrastructure systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [38, 109, 129].

Critical Infrastructure Information information not customarily in the public domain and related to the security of CI or protected systems [130, 136].

Critical Infrastructure Information Act of 2002 subtitle B of title II of Public Law (P.L.) 107-296, Homeland Security Act of 2002 [130].

Critical Infrastructure Protection Act of 2001 §1016 of title X of P.L. 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 [129].

Cybersecurity Framework the standards framework developed by National Institute of Standards and Technology (NIST) as required by Executive Order (EO) 13636 which incorporates input from private sector; designed to provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including Information Security (InfoSec) measures and controls, to help owners and operators of CI identify, assess, and manage cyber risk [109].

Defense Support of Civil Authorities support provided by U.S. Federal military forces, DoD civilians, DoD contract personnel, DoD component assets, and National Guard forces (when the Secretary of Defense (SECDEF), in coordination with the governors of the affected states, elects and requests to use those forces in Title 32 United States Code (U.S.C.) status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. Also known as civil support [49].

Economy Act 31 U.S.C. 1535 [131].

federal agency any department, independent establishment, government corporation, or other agency of the executive branch of the federal government [135, 136].

Federal Information Security Management Act of 2002 title X of P.L. 107-296, Homeland Security Act of 2002 [130].

Freedom of Information Act 5 U.S.C. 552 [135].

Homeland Security a concerted national effort to prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recovery from attacks that do occur [135, 136].

Information Security protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, availability, and authentication [130].

integrity guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity [130].

Key Resources publicly or privately controlled resources essential to the minimal operations of the economy and government [124, 130, 136].

National Security System any information system (including any telecommunications system) used or operated by a federal agency, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, Command and Control (C2) of military forces, or equipment that is an integral part of a weapon or weapons system or is critical to the direct fulfillment of military or intelligence missions [130].

Reorganization Plan No. 3 of 1978 34 Federal Register (F.R.) 41943, 92 Stat. 3788, of Title 5 Appendix U.S.C. [135].

resilience the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, including the ability to withstand and recover from deliberate attacks, accidents, and naturally occurring threats or incidents [110].

risk the combined or weighted effect of the likelihood of the occurrence and a measured or assessed consequence given to that occurrence [38, 124].

risk assessment the process of examining a situation or elements of a program to identify and analyze threats and vulnerabilities to determine the potential for loss and identifying cost-effective protective measures and residual risks [38, 124].

risk management a continuous process of managing, through a series of mitigating actions that permeate an entity's activities, the likelihood of an adverse event happening and having a negative impact to a defined, tolerable level [38, 124].

Sector-Specific Agency the federal agency designated under Presidential Policy Directive (PPD)-21 to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated CI sector [110].

Stafford Act 42 U.S.C. 5121 et. seq. [133].

vulnerability any weakness that can be exploited by an aggressor or make an asset susceptible to hazard damage [124].

Bibliography

[1] Marshall Abrams and Joe Weiss. "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia". July 23, 2008. URL: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf (visited on 07/15/2013) (cit. on p. 6).

[2] Robert K. Ackerman. "Critical Infrastructure Ripe for Attack". In: *SIGNAL Magazine* (June 1, 2013). URL: http://www.afcea.org/content/?q=node/11120 (visited on 06/24/2013) (cit. on pp. 5, 6, 8, 9, 59).

[3] Robert K. Ackerman. "Cyber Commander Calls for Consolidated Activities". In: *SIGNAL Magazine* (June 12, 2013). URL: http://www.afcea.org/content/?q=node/11185 (visited on 06/24/2013) (cit. on pp. 1, 6, 40, 47).

[4] James Adkisson et al. "Law of Armed Conflict: Implications for Navy Cyber Strategy". MA thesis. Pittsburgh, PA: Carnegie Mellon University, Aug. 3, 2012 (cit. on p. 5).

[5] GEN Keith Alexander. *National conversation on the defense of our nation and protecting our civil liberties and privacy: A technical perspective*. Black Hat USA 2013 Briefing. July 31, 2013 (cit. on p. 49).

[6] Keith B. Alexander. *Statement of General Keith B. Alexander Commander United States Cyber Command Before the Senate Committee on Armed Services*. Mar. 27, 2012. URL: http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf (visited on 07/01/2013) (cit. on pp. 23, 25, 27, 36, 40, 49, 63).

[7] Martin Alperen. *Foundations of Homeland Security: Law and Policy*. Wiley and Sons, Hoboken, NJ, Mar. 2011 (cit. on p. 23).

[8] Paul Ames. "NATO's Geek Brigade". In: *MinnPost* (May 28, 2013). URL: http://www.minnpost.com/global-post/2013/05/natos-geek-brigade (visited on 06/19/2013) (cit. on pp. 7, 63).

[9] Ross Anderson and Tyler Moore. "The Economics of Information Security". In: *Science* 314.5799 (Oct. 27, 2006), pp. 610–613. URL: http://www.jstor.org/stable/20031627 (visited on 03/19/2013) (cit. on p. 10).

[10] Wesley R. Andrues. "What U.S. Cyber Command Must Do". In: *Joint Force Quarterly* 59 (Oct. 2010). URL: http://go.galegroup.com/ps/i.do?id=GALE%7CA275575719&v=2.1&u=cmu_main&it=r&p=AONE&sw=w (visited on 05/22/2013) (cit. on p. 46).

[11] Anonymous. “Cyber Intrusions Into Critical Infrastructure Growing, Official Says”. In: *C4I News* (Apr. 22, 2010). ISSN: 10711317. URL: http://search.proquest.com/docview/232539096?accountid=9902 (cit. on p. 2).

[12] Darrell M. Apilado. “Cybersecurity Risk of Targeted Malware to Industrial Control Systems – Latent National Security Issues”. MA thesis. Maxwell Air Force Base, AL: Air University, May 2012 (cit. on pp. 5, 9, 43).

[13] William A. Arbaugh, William L. Fithen, and John McHugh. “Windows of Vulnerability: A Case Study Analysis”. In: *IEEE Computer* 33.12 (Dec. 2000), pp. 52–59. ISSN: 0018-9162. DOI: 10.1109/2.889093 (cit. on p. 10).

[14] Ashish Arora and Rahul Telang. “Economics of Software Vulnerability Disclosure”. In: *IEEE Security & Privacy* 3.1 (2005), pp. 20–25. ISSN: 1540-7993. DOI: 10.1109/MSP.2005.12 (cit. on pp. 10, 60).

[15] Ashish Arora et al. “An Empirical Analysis of Software Vendors’ Patching Behavior: Impact of Vulnerability Disclosure”. In: *Information Systems Research* 21.1 (Mar. 2010). ISSN: 1047-7047. DOI: 10.1287/isre.1080.0226 (cit. on p. 10).

[16] Assistant Secretary of Defense for Networks and Information Integration and Department of Defense Chief Information Officer. *Department of Defense Manual 8570.01-M. Information Assurance Workforce Improvement Program*. Change 3. Jan. 24, 2012 (cit. on p. 53).

[17] Walter S. Baer and Andrew Parkinson. “Cybersecurity in IT Security Management”. In: *IEEE Security & Privacy* 5.3 (2007), pp. 50–56. ISSN: 1540-7993. DOI: 10.1109/MSP.2007.57. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4218551 (cit. on p. 60).

[18] Stewart Baker et al. *In the Dark. Crucial Industries Confront Cyberattacks*. Report. McAfee, 2012 (cit. on pp. 5, 44).

[19] M. Bodine Birdwell and Robert Mills. “War Fighting in Cyberspace: Evolving Force Presentation and Command and Control”. In: *Air & Space Power Journal* 25.1 (2011), pp. 26–36. ISSN: 1555385X. URL: http://search.proquest.com/docview/868336793?accountid=9902 (cit. on pp. 24, 50).

[20] Black Hat USA. *Briefings Schedule Black Hat USA 2013*. URL: https://www.blackhat.com/us-13/briefings.html#Alexander (visited on 07/28/2013) (cit. on p. 35).

[21] Joel F. Brenner. “Privacy and Security Why Isn’t Cyberspace More Secure?.” In: *Communications of the ACM* 53.11 (2010), pp. 33–35. ISSN: 00010782. URL: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=55063010&site=ehost-live (cit. on p. 55).

[22] Pablo C. Breuer. Personal Interview. LCDR, U.S. Navy, July 12, 2013 (cit. on pp. vii, 53).

[23] Elisabeth Bumiller. “Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks”. In: *The New York Times* (Jan. 27, 2013), A7. URL: http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=0 (visited on 03/18/2013) (cit. on p. 6).

[24] George Bush. *Executive Order 13231. Critical Infrastructure Protection in the Information Age*. Oct. 16, 2001 (cit. on p. 15).

[25] George Bush. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Report. The White House, Feb. 2003 (cit. on p. 17).

[26] George Bush. *The National Strategy to Secure Cyberspace*. Report. The White House, Feb. 2003 (cit. on pp. 15, 17).

[27] George Bush. *Executive Order 12333. United States intelligence activities*. July 31, 2008. URL: http://www.archives.gov/federal-register/codification/executive-order/12333.html (visited on 06/14/2013) (cit. on p. 25).

[28] George W. Bush. *Homeland Security Presidential Directive-7. Critical Infrastructure Identification, Prioritization, and Protection*. Dec. 17, 2003. URL: http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html (visited on 06/19/2013) (cit. on p. 18).

[29] Matthew Butkovic. Personal Interview. Pittsburgh, PA: Computer Emergency Response Team Division, Software Engineering Institute, July 3, 2013 (cit. on pp. vii, 9, 40, 57).

[30] Matthew Butkovic. Personal Email. Computer Emergency Response Team Division, Software Engineering Institute, July 5, 2013 (cit. on pp. vii, 61).

[31] Jimmy Carter. *Executive Order 12127. Federal Emergency Management Agency*. Mar. 31, 1979 (cit. on p. 13).

[32] Chief of Naval Operations N1. *NAVADMIN 156/12. FY-12 Revisions to Surface Warfare Officer Critical Skills Retention Bonus and Surface Warfare Officer Continuation Pay Programs*. May 7, 2012. URL: http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2012/NAV12156.txt (visited on 07/23/2013) (cit. on p. 54).

[33] Mina Cikara, Emile G. Bruneau, and Rebecca R. Saxe. "Us and Them: Intergroup Failures of Empathy". In: *Current Directions in Psychological Science* 20.3 (2011), pp. 149–153. DOI: 10.1177/0963721411408713. eprint: http://cdp.sagepub.com/content/20/3/149.full.pdf+html. URL: http://cdp.sagepub.com/content/20/3/149.abstract (cit. on p. 45).

[34] Logan A. Clark. Personal Email. U.S. Cyber Command, July 15, 2013 (cit. on pp. vii, 46).

[35] Richard A. Clarke and Robert K. Knake. *Cyber War. The Next Threat to National Security and What to do About It*. New York: Harper-Collins, 2010. ISBN: 978-0-06-196223-3 (cit. on pp. 9, 33).

[36] William J. Clinton. *Executive Order 13010. Critical Infrastructure Protection*. July 15, 1996 (cit. on p. 13).

[37] William J. Clinton. *Executive Order 13130. National Infrastructure Assurance Council*. July 14, 1999 (cit. on p. 15).

[38] William J. Clinton and Richard A. Clarke. *National Plan for Information Systems Protection Version 1.0. Defending America's Cyberspace*. An Invitation to a Dialogue. The White House, 2000 (cit. on pp. 15, 71, 73).

[39] Sean M. Condron. "Getting it right: Protecting American critical infrastructure in cyberspace". In: *Harvard Journal of Law & Technology* 20.2 (2007), pp. 403–422. ISSN: 08973393. URL: http://go.galegroup.com/ps/i.do?id=GALE%7CA197364705&v=2.1&u=cmu_main&it=r&p=AONE&sw=w (visited on 05/22/2013) (cit. on p. 9).

[40] Claire Cuccio. Personal Phone Interview. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, July 3, 2013 (cit. on pp. vii, 34, 45, 50, 57).

[41] Michael Daniel. "Collaborative and Cross-Cutting Approaches to Cybersecurity". In: (Aug. 1, 2012). URL: http://www.whitehouse.gov/blog/2012/08/01/collaborative-and-cross-cutting-approaches-cybersecurity?utm_source=related (visited on 06/13/2013) (cit. on p. 33).

[42] Shawn M. Dawley. "A Case for a Cyberspace Combatant Command". In: *Air & Space Power Journal* 27.1 (2013), pp. 130–142. ISSN: 1555385X. URL: http://search.proquest.com/docview/1318929520?accountid=9902 (cit. on p. 50).

[43] Defense Cyber Crime Center. *Fact Sheet: Defense Cyber Crime Center (DC3)*. May 1, 2013. URL: http://www.dc3.mil/dc3/DC3%20Fact%20Sheet%202013%2004%2030.pdf (visited on 06/14/2013) (cit. on p. 26).

[44] Defense Science Board. *Enhancing Adaptability of U.S. Military Forces*. Report. Department of Defense: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, Jan. 2013 (cit. on pp. 46, 52).

[45] Defense Science Board. *Resilient Military Systems and the Advanced Cyber Threat*. Task Force Report. Department of Defense: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, Jan. 2013 (cit. on pp. 2, 3, 9, 10, 29, 48, 51, 54).

[46] Dorothy E. Denning. "Stuxnet: What Has Changed?" In: *Future Internet* 4.3 (2012), pp. 672–687. ISSN: 1999-5903. DOI: 10.3390/fi4030672. URL: http://www.mdpi.com/1999-5903/4/3/672 (cit. on pp. 5, 6, 9).

[47] Department of Defense. *Strategy for Operating in Cyberspace*. Report. Department of Defense, July 2011. URL: http://www.defense.gov/news/d20110714cyber.pdf (cit. on p. 19).

[48] Department of Defense. *Fact Sheet: Defense Industrial Base (DIB) Cybersecurity Activities*. May 11, 2012. URL: http://www.defense.gov/news/d20120512dib.pdf (visited on 03/18/2013) (cit. on p. 36).

[49] Department of Defense. *Department of Defense Dictionary of Military and Associated Terms*. June 2013 (cit. on p. 72).

[50] Department of Homeland Security. *About the National Cybersecurity and Communications Integration Center*. URL: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (visited on 07/31/2013) (cit. on p. 28).

[51] Department of Homeland Security. *Council Members, Critical Infrastructure Partnership Advisory Council*. URL: http://www.dhs.gov/council-members-critical-infrastructure-partnership-advisory-council (visited on 07/12/2013) (cit. on p. 27).

[52] Department of Homeland Security. *National Infrastructure Protection Plan. Partnering to enhance protection and resiliency*. 2009. URL: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (cit. on pp. 18, 30).

[53] Department of Homeland Security. *National Cyber Incident Response Plan*. Sept. 2010. URL: http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf (visited on 07/06/2013) (cit. on p. 27).

[54] Department of Homeland Security. *Blueprint for a Secure Cyber Future*. Report. Department of Homeland Security, Nov. 2011 (cit. on p. 27).

[55] Department of Homeland Security. *Fact Sheet: National Level Exercise 2012*. June 5, 2012. URL: http://www.dhs.gov/news/2012/06/05/fact-sheet-national-level-exercise-2012 (visited on 06/17/2013) (cit. on pp. 26, 37).

[56] Department of Homeland Security ICS-CERT. *Control Systems Analysis Report CSAR-10-025-01 Analysis of Shodan – Computer Search Engine*. May 8, 2013. URL: http://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01 (visited on 06/26/2013) (cit. on p. 7).

[57] Department of Homeland Security National Cyber Security Division. *Catalog of Control Systems Security: Recommendations for Standards Developers*. 2011. URL: http://ics-cert.us-cert.gov/sites/default/files/CatalogofRecommendationsVer7.pdf (cit. on p. 39).

[58] Deputy Secretary of Defense. *Department of Defense Directive 1304.21. Policy on Enlistment Bonuses, Accession Bonuses for New Officers in Critical Skills, Selective Reenlistment Bonuses, and Critical Skills Retention Bonuses for Active Members*. Jan. 31, 2005 (cit. on p. 54).

[59] Deputy Secretary of Defense. *Department of Defense Directive 3025.18. Defense Support of Civil Authorities (DSCA)*. Change 1. Sept. 21, 2012 (cit. on pp. 11, 38).

[60] Deputy Secretary of Defense. *Department of Defense Directive 3000.06. Combat Support Agencies (CSAs)*. June 27, 2013. URL: http://www.dtic.mil/whs/directives/corres/pdf/300006p.pdf (visited on 07/01/2013) (cit. on pp. 25, 71).

[61] Charles J. Dunlap Jr. "Some reflections on the intersection of law and ethics in cyber war". In: *Air & Space Power Journal* 27.1 (2013), pp. 22–43. ISSN: 1555385X. URL: http://go.galegroup.com/ps/i.do?id=GALE%7CA316664176&v=2.1&u=cmu_main&it=r&p=AONE&sw=w (visited on 05/23/2013) (cit. on pp. 8, 51).

[62] Caitlin Durkovich. Personal Email. Department of Homeland Security, July 9, 2013 (cit. on pp. vii, 27, 28, 30).

[63] Caitlin Durkovich. *Remarks at Panel on Strategies for Protecting Critical Services and Infrastructure*. Carnegie Mellon University Washington Speaker Series. May 30, 2013 (cit. on pp. 28, 31).

[64] Timothy J. Evans. Personal Email. Johns Hopkins University Applied Physics Laboratory, July 3, 2013 (cit. on p. vii).

[65] Federal Bureau of Investigation. *Addressing Threats to the Nation's Cybersecurity*. URL: http://www.fbi.gov/about-us/investigate/cyber/cyber-task-

forces-building-alliances-to-improve-the-nations-cybersecurity-1 (visited on 07/09/2013) (cit. on p. 26).

[66] Federal Bureau of Investigation. *Cyber Task Forces*. URL: http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1 (visited on 07/09/2013) (cit. on p. 26).

[67] Federal Bureau of Investigation. *InfraGard Frequently Asked Questions*. Dec. 12, 2011. URL: https://www.infragard.org/9o31KtPHgBItBjzYqNMbWZ6BbHcZIkg16x0XBmBeOjQ%25253D! (visited on 07/09/2013) (cit. on p. 26).

[68] Federal Bureau of Investigation. *FBI Cyber Crime Homepage*. June 19, 2013. URL: http://www.fbi.gov/about-us/investigate/cyber (visited on 07/09/2013) (cit. on p. 26).

[69] Eric A. Fischer. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions. R42114*. Report. Congressional Research Service, June 20, 2013. URL: http://www.fas.org/sgp/crs/natsec/R42114.pdf (visited on 07/15/2013) (cit. on pp. 33, 43).

[70] General Services Administration. "Joint Working Group on Improving Cybersecurity and Resilience through Acquisition". In: *The Washington Post* (May 26, 2013). URL: https://www.federalregister.gov/articles/2013/05/13/2013-11239/joint-working-group-on-improving-cybersecurity-and-resilience-through-acquisition?utm_campaign=email+a+friend&utm_medium=email&utm_source=federalregister.gov (visited on 06/06/2013) (cit. on p. 55).

[71] Richard M. 'Dickie' George. Personal Email. Johns Hopkins University Applied Physics Laboratory, July 2, 2013 (cit. on pp. vii, 29).

[72] Torsten George. "Cyber Attack!" In: *Public Utilities Fortnightly* 149.7 (2011), pp. 44–48. ISSN: 10785892. URL: http://search.proquest.com/docview/878225054?accountid=9902 (cit. on pp. 33, 60).

[73] Bill Gertz. "The Cyber-Dam Breaks: Sensitive Army database of U.S. dams compromised; Chinese hackers suspected". In: *The Washington Free Beacon* (May 1, 2013). URL: http://freebeacon.com/the-cyber-dam-breaks/ (visited on 05/29/2013) (cit. on p. 6).

[74] Glenn Haddox. Personal Interview. Director Cybersecurity & Compliance, Southern California Edison, June 20, 2013 (cit. on p. 61).

[75] Andrew P. Hansen et al. "Cyber Flag: A Realistic Training Environment for the Future". In: *Air & Space Power Journal* 22.3 (2008), pp. 42–48. ISSN: 1555385X. URL: http://search.proquest.com/docview/217773887?accountid=9902 (cit. on p. 52).

[76] Steven Hart and James D. Ramsay. "A Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses". In: *Homeland Security Affairs* 7.1 (2011). URL: http://search.proquest.com/docview/1266215283?accountid=9902 (cit. on pp. 13, 18).

[77] Oona Hathaway et al. “The Law of Cyber-Attack”. In: *California Law Review* 100.817 (2012) (cit. on pp. 5, 9, 10).

[78] Jason Healey. “A Brief History of US Cyber Conflict”. In: *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Ed. by Jason Healey. .1. USA: Cyber Conflict Studies Association (CSSA), 2013, pp. 14–87. ISBN: 978-0-9893274-1-1 (cit. on pp. 24, 33).

[79] Jason Healey. *Above My Pay Grade: Cyber Response at the National Level*. Black Hat USA 2013 Briefing. Aug. 1, 2013 (cit. on pp. 34, 60).

[80] *Hearing on the Nominations of VADM James A. Winnefeld Jr., USN to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Command; and LTG Keith B. Alexander, USA to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command, S. Comm. on the Armed Services, 105th Cong. 10*. 2010. URL: http://www.gpo.gov/fdsys/pkg/CHRG-111shrg65070/pdf/CHRG-111shrg65070.pdf (cit. on pp. 11, 23, 25, 34, 48).

[81] David M. Hollis. “USCYBERCOM: The Need for a Combatant Command versus a Sub-unified Command”. In: *army.mil* (June 29, 2010). URL: http://www.army.mil/article/41585 (visited on 05/30/2013) (cit. on p. 24).

[82] Homeland Security Project. *Cyber Security Task Force: Public-Private Information Sharing*. Report. Washington, D.C.: Bipartisan Policy Center, July 2012 (cit. on pp. 40–44).

[83] J. Nicholas Hoover. *Thousands Of Industrial Control Systems At Risk: DHS Study*. Jan. 11, 2013. URL: http://www.informationweek.com/government/security/thousands-of-industrial-control-systems/240146091 (visited on 06/26/2013) (cit. on p. 7).

[84] Internet Archive Way Back Machine. *NSA/CSS Mission*. Mar. 2, 2011. URL: http://web.archive.org/web/20110302112117/http://www.nsa.gov/about/mission/index.shtml (visited on 07/28/2013) (cit. on p. 25).

[85] Robert Kolasky. *Closing Plenary: Remarks by the Director of DHS Integrated Task Force*. Cybersecurity Framework Workshop. University of California San Diego, July 12, 2013 (cit. on p. 35).

[86] Jake Kouns and Daniel Minoli. *Information Technology Risk Management in Enterprise Environments. A Review of Industry Practices and a Practical Guide to Risk Management Teams*. Hoboken, NJ: Wiley-Interscience, 2010. ISBN: 978-0-471-76254-6 (cit. on p. 17).

[87] Jose R. Latimer, Timothy J. Evans, and Richard M. ‘Dickie’ George. Personal Interview. Columbia, MD: Johns Hopkins University Applied Physics Laboratory, July 2, 2013 (cit. on pp. vii, 9, 29, 47, 57).

[88] Maryann Lawlor. “Cyber Command Moves Into Position”. In: *afcea.org* (May 6, 2010). URL: http://www.afcea.org/content/?q=node/2290 (cit. on p. 24).

[89] Robert M. Lee. “The interim years of cyberspace”. In: *Air & Space Power Journal* 27.1 (2013), pp. 58–79. ISSN: 1555385X. URL: http://go.galegroup.com/ps/i.do?id=GALE%7CA316664178&v=2.1&u=cmu_main&it=r&p=AONE&sw=w (visited on 05/23/2013) (cit. on p. 6).

[90] Mandiant Corporation. *APT1 - Exposing one of China's Cyber Espionage Units*. Tech. rep. Mandiant Corporation, Mar. 6, 2012. URL: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (cit. on p. 8).

[91] Scott McNabb. *AF competes in second 'Cyber Flag'*. Tech. rep. Federal Information & News Dispatch, Inc, Nov. 30, 2012. URL: http://search.proquest.com/docview/1220994624?accountid=9902 (cit. on p. 52).

[92] M. Granger Morgan. *Remarks at Panel on Strategies for Protecting Critical Services and Infrastructure*. Carnegie Mellon University Washington Speaker Series. May 30, 2013 (cit. on p. 10).

[93] John D. Moteff. *Critical Infrastructure: Background, Policy, and Implementation. RL30153*. Report. Congressional Research Service, June 7, 2010. URL: http://assets.opencrs.com/rpts/RL30153_20100607.pdf (cit. on pp. 13, 15, 17, 18, 42).

[94] Ellen Nakashima. "Homeland Security tries to shore up nation's cyber defenses". In: *The Washington Post* (Oct. 1, 2011). URL: http://www.washingtonpost.com/world/national-security/homeland-security-tries-to-shore-up-nations-cyber-defenses/2011/09/27/gIQAtQ6bDL_print.html (visited on 06/20/2013) (cit. on pp. 5, 63).

[95] Ellen Nakashima. "When is a cyberattack a matter of defense?" In: *The Washington Post* (Feb. 27, 2012). URL: http://www.washingtonpost.com/blogs/checkpoint-washington/post/active-defense-at-center-of-debate-on-cyberattacks/2012/02/27/gIQACFoKeR_blog.html#pagebreak (visited on 06/20/2013) (cit. on pp. 44, 57).

[96] Ellen Nakashima. "White House, NSA weigh cybersecurity, personal privacy". In: *The Washington Post* (Feb. 7, 2012). URL: http://www.washingtonpost.com/world/national-security/white-house-nsa-weigh-cyber-security-personal-privacy/2012/02/07/gIQA8HmKeR_print.html (visited on 06/20/2013) (cit. on pp. 41, 44).

[97] Ellen Nakashima. "White House's cybersecurity official retiring". In: *The Washington Post* (May 16, 2012). URL: http://www.washingtonpost.com/world/national-security/white-houses-cybersecurity-official-retiring/2012/05/16/gIQAX6fmUU_print.html (visited on 06/20/2013) (cit. on p. 33).

[98] Janet Napolitano. *Cybersecurity Protection Keynote at the Woodrow Wilson International Center for Scholars*. June 20, 2013. URL: http://www.c-spanvideo.org/program/SecNa (visited on 06/24/2013) (cit. on pp. 27, 28, 35, 36, 39, 41, 43).

[99] National Council of ISACs. *Member ISACs*. URL: http://www.isaccouncil.org/memberisacs.html (visited on 07/16/2013) (cit. on pp. 29, 30).

[100] National Security Agency/Central Security Service. *About NSA - Mission*. Apr. 11, 2011. URL: http://www.nsa.gov/about/mission/index.shtml (visited on 06/14/2013) (cit. on p. 25).

[101] National Security Council - Cybersecurity. *National Initiative for Cybersecurity Education (NICE) Relationship to President's Education Agenda*. Report. The White House, Apr. 19, 2010. URL: http://www.whitehouse.gov/sites/default/

files/rss_viewer/cybersecurity_niceeducation.pdf (visited on 06/13/2013) (cit. on p. 53).

[102] Kevin P. Newmeyer. "Who Should Lead U.S. Cybersecurity Efforts?" In: *Prism : a Journal of the Center for Complex Operations* 3.2 (2012), pp. 115–126. ISSN: 21570663. URL: http://search.proquest.com/docview/1011482876?accountid=9902 (cit. on pp. 13, 15, 34, 53).

[103] North American Electric Reliability Corporation. *Critical Infrastructure Protection Standards*. URL: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (visited on 07/12/2013) (cit. on p. 29).

[104] Michael H. Noyes. *CG 13-1 Legal Briefing: Uses and Limitations of Title 10 Forces and State (T32 or SAD) Forces in Cyber DOMOPS*. Fort Meade, MD, July 11, 2013 (cit. on p. 38).

[105] *Obama: My Plan Makes Electricity Rates Skyrocket*. San Francisco Chronicle. Jan. 2008. URL: http://www.youtube.com/watch?v=HlTxGHn4sH4 (visited on 07/03/2013) (cit. on p. 40).

[106] Barack Obama. *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*. Tech. rep. The White House, Mar. 29, 2009. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (cit. on pp. 1, 34).

[107] Barack Obama. *Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities*. May 11, 2012. URL: http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf (visited on 06/13/2013) (cit. on pp. 36, 37).

[108] Barack Obama. *Taking the Cyberattack Threat Seriously*. July 23, 2012. URL: http://www.whitehouse.gov/blog/2012/07/20/taking-cyberattack-threat-seriously?utm_source=related (visited on 06/13/2013) (cit. on pp. 34, 37).

[109] Barack Obama. *Executive Order 13636. Improving Critical Infrastructure Cybersecurity*. Feb. 12, 2013 (cit. on pp. 5, 20, 34, 35, 41, 71, 72).

[110] Barack Obama. *Presidential Policy Directive-21. Critical Infrastructure Security and Resilience*. Feb. 12, 2013. URL: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infras%5C%5Ctructure-cybersecurity (visited on 05/28/2013) (cit. on pp. 19, 20, 30, 34, 73).

[111] George Orwell. *Nineteen Eighty-Four. A Novel*. New York: Harcourt, Brace, 1949 (cit. on p. 44).

[112] David K. Owens. *Remarks at Panel on Strategies for Protecting Critical Services and Infrastructure*. Carnegie Mellon University Washington Speaker Series. May 30, 2013 (cit. on p. 43).

[113] Leon E. Panetta. "Defending the Nation from Cyber Attack". Speech as Delivered to Business Executives for National Security. New York, NY, Oct. 11, 2012. URL: http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728 (cit. on p. 6).

[114] Marcus J. Ranum. “Cyber War: You’re Doing it Wrong! The Relationship between Four Threats in the 21st Century”. Seminar Lecture. Pittsburgh, PA, Nov. 12, 2012 (cit. on p. 9).

[115] David Rice. *Geekonomics. The Real Cost of Insecure Software*. Upper Saddle River, NJ: Addison-Wesley, 2008. ISBN: 978-0-321-73597-3 (cit. on pp. 10, 29).

[116] Scott A. Rothermel. “The Department of Defense’s Role in Supporting Cybersecurity of Critical Infrastructure”. MA thesis. Maxwell Air Force Base, AL: Air University, May 2012 (cit. on pp. 11, 42).

[117] Kori Schake. *National Security in a Time of Austerity*. University Lecture. Oct. 17, 2012 (cit. on p. 45).

[118] Howard A. Schmidt. “Building Cybersecurity Capability in the Electricity Sector”. In: *The White House Blog* (May 25, 2012). URL: http://www.whitehouse.gov/blog/2012/05/25/building-cybersecurity-capability-electricity-sector?utm_source=related (visited on 06/13/2013) (cit. on p. 34).

[119] *Senate Armed Services Committee Hearing*. Mar. 12, 2013. URL: http://search.proquest.com/docview/1316575988?accountid=9902 (cit. on pp. 47, 51, 52).

[120] Suzanne E. Spaulding and Jason Healey. “15th Anniversary of PDD-63: History of Cyber Critical Infrastructure Protection”. Remarks and Discussion. Hosted by Atlantic Council’s Cyber Statecraft Initiative. Washington, D.C., May 22, 2013. URL: http://www.acus.org/event/15th-anniversary-pdd-63-history-cyber-critical-infrastructure-protection (visited on 06/19/2013) (cit. on pp. 13, 15, 16).

[121] Tim Stevens. “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”. In: *Contemporary Security Policy* 33.1 (2012), pp. 148–170. DOI: 10.1080/13523260.2012.659597. eprint: http://www.tandfonline.com/doi/pdf/10.1080/13523260.2012.659597. URL: http://www.tandfonline.com/doi/abs/10.1080/13523260.2012.659597 (cit. on p. 51).

[122] Brett Stohs. “Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 Will Degrade the Freedom of Information Act”. In: *Duke Law & Technology Review* 1 (2011), pp. 1–8 (cit. on p. 42).

[123] Keith Stouffer, Joe Falco, and Karen Scarfone. *Guide to Industrial Control Systems (ICS) Security*. Revision 1. National Institute of Standards and Technology. May 2013. DOI: 10.6028/NIST.SP.800-82r1. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (cit. on p. 30).

[124] John Sullivant. *Strategies for Protecting National Critical Infrastructure Assets. A Focus on Problem-Solving*. Hoboken, NJ: John Wiley & Sons, Inc., 2007. ISBN: 978-0-471-79926-9 (cit. on pp. 2, 17, 30, 40, 56, 57, 59, 64, 71–73).

[125] The White House. *Comprehensive National Cybersecurity Initiative*. Sept. 2010. URL: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (visited on 07/06/2013) (cit. on pp. 18, 19).

[126] Under Secretary of Defense for Intelligence. *Department of Defense Manual 5200.01-V3. DoD Information Security Program: Protection of Classified Information*. Feb. 24, 2012 (cit. on p. 42).

[127] United States Special Operations Command. *About USSOCOM*. 2013. URL: http://www.socom.mil/Pages/AboutUSSOCOM.aspx (visited on 06/14/2013) (cit. on pp. 50, 52).

[128] United States Strategic Command. *Fact Sheet: United States Cyber Command*. 2011. URL: http://www.stratcom.mil/factsheets/Cyber_Command/ (visited on 07/06/2013) (cit. on p. 24).

[129] U.S. Congress. *Public Law 107-56. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*. Oct. 26, 2001 (cit. on pp. 16, 71).

[130] U.S. Congress. *Public Law 107-296. Homeland Security Act of 2002*. Nov. 25, 2002 (cit. on pp. 13, 16, 17, 20, 71, 72).

[131] U.S. Congress. *Title 31 U.S.C.: Money and Finance*. 2011 (cit. on p. 72).

[132] U.S. Congress. *Title 32 U.S.C.: National Guard*. 2011 (cit. on p. 38).

[133] U.S. Congress. *Title 42 U.S.C.: The Public Health and Welfare*. 2011 (cit. on p. 73).

[134] U.S. Congress. *Title 10 U.S.C.: Armed Forces*. 2012 (cit. on pp. 38, 50).

[135] U.S. Congress. *Title 5 U.S.C.: Government Organizations and Employees*. 2012 (cit. on pp. 13, 41, 72).

[136] U.S. Congress. *Title 6 U.S.C.: Domestic Security*. 2012 (cit. on pp. 13, 20, 71, 72).

[137] U.S. Department of Defense Information. "Gates establishes U.S. Cyber Command and names first commander". In: *Federal Information & News Dispatch, Inc* (2010-05-21). URL: http://search.proquest.com/docview/310867622?accountid=9902 (cit. on p. 24).

[138] U.S. Department of Defense Office of the Assistant Secretary of Defense (Public Affairs). *DoD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities*. May 11, 2012. URL: http://www.defense.gov/releases/release.aspx?releaseid=15266 (visited on 06/13/2013) (cit. on p. 36).

[139] USCYBERCOM. *Cyber Wargame 13. Seminar Handout*. June 3, 2013. URL: https://www.fbcinc.com/e/WarGame/default.aspx (visited on 06/07/2013) (cit. on p. 37).

[140] USCYBERCOM. *Cyber Wargame 13. Agenda*. June 3, 2013. URL: https://www.fbcinc.com/e/WarGame/agenda.aspx (visited on 06/07/2013) (cit. on p. 37).

[141] USCYBERCOM. *Cyber Wargame 13. Capture Template*. June 3, 2013. URL: https://www.fbcinc.com/e/WarGame/default.aspx (visited on 06/07/2013) (cit. on p. 38).

[142] Utilities Telecom Council. *2013 Critical Infrastructure Communications Policy Summit & 700 MHz Workshop*. June 20–21, 2013. URL: http://www.utc.org/event/2013-critical-infrastructure-communications-policy-summit-700-mhz-workshop (visited on 06/18/2013) (cit. on p. 35).

[143] Suzanne M. Vautrinot and Charles E. Beard. “Cyber Professionals in the Military and Industry—Partnering in Defense of the Nation”. In: *Air & Space Power Journal* 27.1 (2013), pp. 4–21. ISSN: 1555-385X. URL: http://search.proquest.com/docview/1318929574 (cit. on p. 6).

[144] Kim Zetter. “Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software”. In: *wired.com* (Jan. 19, 2012). URL: http://www.wired.com/threatlevel/2012/01/scada-exploits/ (visited on 05/29/2013) (cit. on p. 10).