REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
17-06-2011	Master's Thesis	26-07-2010 to 25-04-2011

4. TITLE AND SUBTITLE
EXPANDING THE DEPARTMENT OF DEFENSE'S ROLE IN CYBER CIVIL SUPPORT

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Kevin M. Donovan
Lt Col, U.S. Air Force

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER
JFSC

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release, distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The 2010 *National Security Strategy* identifies cybersecurity as one of the most serious security, public safety, and economic challenges faced by the United States today. The Nation's information and communications infrastructure, inextricably linked to U.S. economic prosperity, social well-being, and innovation, is not secure and poses a serious national security risk. Preventing cyber attacks against America's critical infrastructures and reducing vulnerability to cyber attacks are extraordinary challenges requiring a concerted national effort among the federal government, state and local government, and the private sector. Although tasked in a supporting role, the Department of Defense (DoD) can and should do more to help protect the Nation's critical infrastructure against cyber threats. The thesis of this paper is that the Department of Defense, beyond its current role, should leverage the unique organization, skills, and demographics of the Reserve Component to assist civil authorities in securing and defending the national critical infrastructure against a major cyber attack. The research will establish the significance of the cyberspace threat and examine existing strategy, policy, roles, and responsibilities to assess gaps and shortfalls in the DoD's capability to support civil authorities in protecting the Nation's critical infrastructure. Finally, the research provides recommendations on how the Reserve Component, in particular the National Guard, can best be used to accomplish the expanded critical infrastructure civil support mission.

15. SUBJECT TERMS
Critical Infrastructure, Cyber, Cyberspace, Civil Support

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Unclassified Unlimited	88	19b. TELEPONE NUMBER (*Include area code*)
Unclassified	Unclassified	Unclassified			757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

EXPANDING THE DEPARTMENT OF DEFENSE'S ROLE IN CYBER CIVIL SUPPORT

By

Kevin M. Donovan

Lt Col, USAF

EXPANDING THE DEPARTMENT OF DEFENSE'S ROLE IN CYBER CIVIL SUPPORT

by

Kevin Donovan

Lt Col, USAF

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: _____
2 June 2011

Thesis Adviser:

Signature: _____
Mr. Benjamin Wible

Approved by:

Signature: _____
Dr. Bryon E. Greenwald, PhD, Committee Member

Signature: _____
CDR James Joyner, Committee Member

Signature: _____
Joanne M. Fish, CAPT, USN, Director, Joint Advanced Warfighting School

This Page Intentionally Blank

ABSTRACT

The 2010 *National Security Strategy* identifies cybersecurity as one of the most serious security, public safety, and economic challenges faced by the United States today. The Nation's information and communications infrastructure, inextricably linked to U.S. economic prosperity, social well-being, and innovation, is not secure and poses a serious national security risk.

Preventing cyber attacks against America's critical infrastructures and reducing vulnerability to cyber attacks are extraordinary challenges requiring a concerted national effort among the federal government, state and local government, and the private sector. Although tasked in a supporting role, the Department of Defense (DoD) can and should do more to help protect the Nation's critical infrastructure against cyber threats.

The thesis of this paper is that the Department of Defense, beyond its current role, should leverage the unique organization, skills, and demographics of the Reserve Component to assist civil authorities in securing and defending the national critical infrastructure against a major cyber attack.

The research will establish the significance of the cyberspace threat and examine existing strategy, policy, roles, and responsibilities to assess gaps and shortfalls in the DoD's capability to support civil authorities in protecting the Nation's critical infrastructure. Finally, the research provides recommendations on how the Reserve Component, in particular the National Guard, can best be used to accomplish the expanded critical infrastructure civil support mission.

This Page Intentionally Blank

TABLE OF CONTENTS

TABLES & FIGURES

TABLES

FIGURES

This Page Intentionally Blank

CHAPTER 1: INTRODUCTION

The 2010 *National Security Strategy* identifies cybersecurity as one of the most serious security, public safety, and economic challenges faced by the United States today.[1] Once the milieu of engineers and computer scientists, cyberspace and its global network of information systems are now integral to daily life.[2] However, the Nation's digital infrastructure, inextricably linked to U.S. economic prosperity, social well-being, and innovation, is not secure and poses a serious national security risk.

Speaking to cybersecurity professionals at a recent Black Hat[3] information security conference, retired General Michael V. Hayden, former Director, Central Intelligence Agency and Deputy Director, National Security Agency likens the Internet to the Great European Plain. "You guys made the cyber world look like the north German plain, and then you bitch and moan because you get invaded. We all get treated like Poland on the web, invaded from the west on even-numbered centuries, invaded from the east on odd-numbered centuries."[4] He goes on to explain, "The inherent geography of this domain [cyberspace] plays to the offense. We made it flat; we gave all advantages to the offense

[1] Barak H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27.

[2] Throughout this thesis, cyberspace refers to the definition provided by Dan Kuehl in "From Cyberspace to Cyberpower" which is broader than the DoD definition and better characterizes the electronic and electromagnetic aspects of critical infrastructure. Kuehl defines cyberspace as "an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures." Dan Kuehl, "From Cyberspace to Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington, DC: National Defense University Press and Potomac Books, 2009), 26.

[3] Black Hat is a premier cybersecurity conference attended by industry leaders, government sector representatives, and ethical hackers to share relevant, actionable knowledge on information security.

[4] Michael V. Hayden, "Black Hat USA 2010: Cyber war: Are we at war? And if we are, how should we fight it?" *YouTube*, http://www.youtube.com/watch?v=XXnIvBBASLI&feature=relate (accessed March 6, 2011).

… there is almost nothing inherent in the domain that plays to the defense."[5] It is this distinct offensive advantage adversaries are exploiting to impose risk on the Nation's critical infrastructure.

The cybersecurity threat is not new. In 2003, in response to a dramatic rise in cyber attacks and recognizing the strategic vulnerability posed by debilitating disruptions of the Nation's critical infrastructure, President George W. Bush signed the *National Strategy to Secure Cyberspace*.[6] This strategy establishes three main strategic objectives: "prevent cyber attacks against America's critical infrastructures, reduce national vulnerability to cyber attacks, and minimize damage and recovery time from cyber attacks that do occur."[7] The extraordinary challenge in achieving these national objectives lies in the fact that the private sector owns and operates most of the Nation's critical infrastructure and success therefore relies on a coordinated effort from all elements of the federal government, state and local government, and the private sector.[8]

At the federal government level, the Department of Homeland Security is the lead agency for protecting the Nation's critical infrastructure with many other departments and agencies, including the Department of Defense (DoD), playing key roles in the effort. In addition to being the lead coordinating agency for the Defense Industrial Base (DIB) sector, the DoD is tasked with providing defense support of civil authorities under the auspices of the *National Response Plan*.

Although tasked in a supporting role, the Department of Defense can and should do more to help protect the Nation's critical infrastructure against cyber threats. The thesis

[5] Hayden.
[6] George W. Bush, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), cover page.
[7] Ibid., viii.
[8] Ibid., 2.

of this paper is that the Department of Defense, beyond its current role, should leverage the unique organization, skills, and demographics of the Reserve Component to assist civil authorities in securing and defending the national critical infrastructure against a major cyber attack.

This research will establish the significance of the cyberspace threat and examine existing strategy, policy, roles, and responsibilities to assess gaps and shortfalls in the DoD's capability to support civil authorities in protecting the Nation's critical infrastructure. The basis of this assessment are the five key principles of response doctrine contained in the *National Response Framework*: (1) engaged partnership, (2) tiered response, (3) scalable, flexible, and adaptable operational capabilities, (4) unity of effort through unified command, and (5) readiness to act.[9] Finally, the research will provide recommendations on how the Reserve Component, and in particular the National Guard, should be best used to accomplish the expanded critical infrastructure civil support mission.

> That the nation and the world are now critically dependent on the cyber infrastructure is no longer a matter of debate. Evidence continues to build showing that our systems for power (nuclear and conventional), water, banking, and credit, as well as our national security and public safety systems rely on complex and sophisticated computer and telecommunications technology. That information infrastructure is vulnerable to threats not just from nation states but also from individuals and small groups who seek to do us harm or wish to exploit our weaknesses for personal gain.[10]

Recognizing these vulnerabilities, President Obama directed the National Security Council and Homeland Security Council to conduct a top-to-bottom review of the federal

[9] U.S. Department of Homeland Security, *National Response Framework* (Washington, DC: U.S. Department of Homeland Security, January 2008), 9.

[10] Karen Evans and Franklin Reeder, *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters, Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, November 2010), 1.

government's efforts to defend the Nation's information and communications infrastructure. In a speech announcing the results, the President declared America's digital infrastructure a "strategic national asset" and that protecting this infrastructure would be a "national security priority."[11]

"The first responsibility of any government and its defense establishment is to protect the lives and safety of its people."[12] Given the fact that the cyber threat is one of the most serious security, public safety, and economic challenges faced by the United States today, it is incumbent on the DoD to take a more proactive role in supporting DHS and other civilian authorities to protect the Nation's critical infrastructure.

The DoD has long relied on the Reserve Component to support civil authorities during times of crisis and domestic emergencies. Expanding this role to help protect against and respond to threats in the cyber domain is a much needed and natural fit. Addressing information technology professionals during a February 2011 Internet security conference, Deputy Defense Secretary William J. Lynn III commented on the DoD's efforts to maximize its use of cyber expertise within the National Guard and Reserve. "Many reservists have a high level of IT knowledge they use in their civilian jobs," Lynn said. To make better use of those skills, he added, "DoD will increase the number of Guard and Reserve units dedicated to cyber missions."[13] Secretary Lynn's announcement is a positive development in the effort to secure cyberspace, however, to make *best* use those skills of which he speaks, this thesis argues that the DoD should

[11] The White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, http://www.whitehouse.gov/briefing-room/speeches-and-remarks (accessed August 15, 2010).

[12] U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: U.S. Department of Defense, February 2010), 18.

[13] Karen Parrish, "Lynn Urges Partnership Against Cyber Threat," *American Forces Press Service*, February 15, 2011, http://www.defense.gov/News/NewsArticle.aspx?ID=62827 (accessed February 18, 2011).

dedicate select Reserve Component units to the national security priority of protecting America's digital infrastructure.

This Page Intentionally Blank

CHAPTER 2: BACKGROUND – CRITICAL INFRASTRUCTURE AND NATIONAL SECURITY

The purpose of this chapter is to explore and gain a better understanding of critical infrastructure in the strategic context of national security. The chapter defines critical infrastructure and its relationship to or impact on the goals and objectives set forth in the 2010 *National Security Strategy*. The final portion of the chapter examines three key events that shaped today's planning process regarding the use of offensive cyber actions and the overall vulnerability of this very crucial domain. They include the Y2K problem, the Estonia cyber-attacks in 2007, and the role of cyber in the Russian-Georgia conflict in 2008. Individually these events talk to the past, yet by placing them in historical context, they create a roadmap for the future. They provide a narrative on the progression of the art of cyber warfare. The linkages described move the discussion from yesterday to today and underscore the importance of defending the Nation's network dependent critical infrastructure.

Often thought of in terms of public works such as highways, schools, and dams or utilities such as power, water, and sewer, infrastructure is much more. In its broadest definition, infrastructure is "the underlying foundation or basic framework of a system or organization."[1] It is the core fabric upon which all else is built, intrinsically essential to the proper functioning of the larger system.

In the context of this larger system being a nation, the infrastructure or lack thereof, separates the weak from the strong, the developed from the developing, and the rich from

[1] Merriam-Webster, http://www.merriam-webster.com/dictionary/infrastructure (accessed January 17, 2011).

the poor. Healthy and secure infrastructures, both physical and organizational (governmental), are absolute prerequisites for a strong, prosperous and secure nation. As such, the 2010 *National Security Strategy* identifies a secure national infrastructure as a key component of "Building Our Foundation," the first priority in the strategic approach to achieving the world the United States seeks.[2]

Defining Critical Infrastructure

In U.S. government (USG) policy, the concept and definition of infrastructure has undergone evolutionary change since the early 1980s. Thirty years ago, the U.S. government did not explicitly define infrastructure but generally equated it to public works such as roads, bridges, public buildings, power production and distribution systems, and communications systems. Most policy focused on the health or adequacy of infrastructure. In the mid-1990s, the rise of terrorism and concerns of attacks against the U.S. homeland led to a gradual expansion of policy dialogue to include not just adequacy but also the protection of national infrastructure.[3]

The USG's increasing concern over the security of infrastructure, invariably led to dialogue and ultimately policy regarding what infrastructure was deemed critical to national security and therefore warranted priority protection. Beginning in 1996, the Clinton and Bush administrations issued a series of executive orders and presidential decision directives (PDD) defining, refining, and prioritizing critical infrastructure.[4] Of particular note was PDD-63, signed on May 22, 1998, calling for a national capability within five years to protect critical infrastructure from malicious interruption. PDD-63

[2] *National Security Strategy*, 9.

[3] John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report for Congress (Washington, DC: Congressional Research Service, October 1, 2004), 2-3.

[4] Ibid., 3.

defined critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government,"[5] marking the first time cyber infrastructure was delineated from other "physical" critical infrastructure.

In the wake of terrorist attacks on September 2001, President Bush signed Executive Order (E.O.) 13228, *Establishing the Office of Homeland Security and Homeland Security Council,* which created the new office that would eventually become the Department of Homeland Security (DHS). This E.O. also expanded the list of sectors included under the umbrella of critical infrastructure and assigned overall protection responsibilities to the Office of Homeland Security.[6]

Also in response to the terror attacks of 9/11, and to codify E.O. 13228 into law, the U.S. Congress passed the *USA Patriot Act of 2001*. This act defined critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States 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."[7] This definition stands today, adopted by reference in the *Homeland Security Act of 2002*[8], the *National Strategy for Homeland Security*, and the Homeland Security Presidential Directive (HSPD) 7: *Critical Infrastructure Identification, Prioritization, and Protection.*[9]

HSPD-7, issued December 17, 2003, is the culmination of fifteen years of government policy efforts to define, categorize, and prioritize critical infrastructure and

[5] The White House, Presidential Decision Directive 63, "Critical Infrastructure Protection" (Washington, DC: The White House, May 22, 1998).
[6] Moteff and Parfomak, 6.
[7] *USA Patriot Act of 2001*, Public Law 107-56, 107th Cong., 1st sess. (October 26, 2001), 115.
[8] The *Homeland Security Act of 2002* established the Department of Homeland Security.
[9] Moteff and Parfomak, 9.

key resources (CIKR).[10] It establishes the current list of a critical infrastructure sectors and lead federal agencies (sector-specific agencies) shown in table 1.

Table 1. Critical Infrastructures and Sector-Specific Agencies[11]

Sector-Specific Agency	Critical Infrastructure
Dept. of Agriculture Dept. of Health and Human Services	• Agriculture and Food
Dept. of Defense	• Defense Industrial Base
Dept. of Energy	• Energy
Dept. of Health and Human Services	• Healthcare and Public Health
Dept. of the Interior	• National Monuments and Icons
Dept. of the Treasury	• Banking and Finance
Environmental Protection Agency	• Water
Department of Homeland Security (DHS) - Office of Infrastructure Protection	• Chemical • Commercial Facilities • Critical Manufacturing • Dams • Emergency Services • Nuclear Reactors, Materials, and Waste
DHS - Office of Cybersecurity and Communications	• Information Technology • Communications
DHS - Transportation Security Administration	• Postal and Shipping
DHS - Transportation Security Administration United States Coast Guard	• Transportation Systems
DHS - Immigration and Customs Enforcement, Federal Protective Service	• Government Facilities

Perhaps most importantly, HSPD-7 articulates the threat and importance of critical infrastructure to national security. According to HSPD-7, "Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage

[10] The *Homeland Security Act of 2002* introduces the term "key resources," defined as publicly or privately controlled resources essential to the minimal operations of the economy and government. The Act does not specify what key resources are but affords them the same level of protection as critical infrastructure. For the purposes of this paper, the terms key resources and critical infrastructure are synonymous.

[11] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: U.S. Government Printing Office, 2009), 19.

public morale and confidence."[12] In terms of national security, "critical infrastructure and key resources provide the essential services that underpin American society…there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being."[13]

Critical Infrastructure and Centers of Gravity

At the grand strategic level, nation-states employ all means of national power to pursue the objectives of the state. These means, or instruments of national power, are expressed as diplomatic, informational, military, and economic (DIME). Employed individually or in concert, elements of DIME represent the advantage, or power, a government applies against other states or entities to pursue national interests. Essentially, DIME represents the sources of power from which a nation derives its freedom of action and compels others to act in a manner consistent with objectives of the state.

Joint doctrine defines center of gravity (COG) as the set of characteristics, capabilities, and sources of power from which a system derives its moral or physical strength, freedom of action, and will to act.[14] If DIME represents the sources of power from which a nation derives its freedom of action and compels, or wills, others to act in a manner consistent with objectives of the state, then doctrinally one could consider DIME the ultimate strategic center of gravity of any nation. Some strategists would argue there can only be one COG at any level of war and therefore DIME, the collective instruments

[12] George W. Bush, Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," in *Public Papers of the Presidents of the United States: George W. Bush, Book 02, Presidential Documents – July 1 to December 31, 2003* (Washington, DC: Government Printing Office, December 17, 2003), 1739.

[13] Ibid.

[14] U.S. Joint Chiefs of Staff, *DoD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, 2010), 113.

of national power cannot be a COG. In other words, there can be but one source of power, "the hub of all power and movement upon which everything depends."[15] This argument, however, runs contrary to joint doctrine that defines COG as a set of characteristics, capabilities, and sources of power. DIME, the instruments of national power, is that set of capabilities, the sources of power from which a system (the nation) derives its freedom of action and will to act.

Following the logic that the collective DIME is the collective COG of the nation state, the Nation's critical infrastructure fits the definition of a critical capability – "a means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s)."[16] Critical infrastructure underpins the Nation's economy, enables its military, and provides the medium for conveying informational and diplomatic strategic communications.

The interdependent nature and cyber dimension of critical infrastructure represents a critical vulnerability of national strategic importance. "Despite the long recognition that interdependencies are critical to the proper functioning of an economy and, more broadly, society in general, a deeper appreciation of their importance to economic and national security has developed only in the past decade."[17] The rapidly increasing dependence on and interconnectedness of cyber infrastructure represents a particular challenge. "Given extensive cyber interdependencies, careful attention to cyber security is essential for virtually all modern infrastructures."[18]

---

[15] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 595-596.

[16] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, December 26, 2006), IV-11.

[17] Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies," *IEEE Control Systems Magazine*, December 2001, 23.

[18] Ibid., 18.

The Year 2000 Problem and recent cyber attacks against Estonia and Georgia highlight the interdependency and cyber security vulnerabilities associated with critical infrastructure.

The Year 2000 Challenge

The Year 2000 (Y2K) problem was the result of programming decisions to designate the year in computer software in two-digits rather than four. Experts feared the two-digit convention, widely adapted by early computer programmers to save expensive memory storage space, if not mitigated, would cause widespread operational errors when computers and microprocessors failed to make the correct transition from 1999 to 2000.[19] One of the most critical concerns with Y2K was the potential cascading nature of the problem. Because of the highly interconnected nature of information systems, both in hardware and software, experts believed that failures in one industry or system would sector spill over into other systems leading to widespread outages throughout the government and private sectors.

One of the most obvious examples is a wide scale power outage. A microprocessor failure in a sub-component of the supervisory control and data acquisition (SCADA) system that monitors and regulates the power grid could disrupt load balances and trigger a cascade of overload failures across a wide swath of the U.S.[20] The power outage in turn, causes significant disruption to essential services such commerce, public health and safety, transportation, and telecommunications. As another example, telecommunications

[19] U.S. Department of Commerce, Economics and Statistics Administration, *The Economics of Y2K and the Impact on the United States* (Washington, DC: U.S. Department of Commerce, November 17, 1999), 7.

[20] Adilson E. Motter and Ying-Cheng Lai, "Cascade-based Attacks on Complex Networks," *Physical Review E* 66, no. 6 (20 December 2002), http://chaos1.la.asu.edu/~yclai/papers /PRE_02_ML_3.pdf (accessed January 24, 2010).

or banking system failures could prevent credit card transactions, causing widespread commerce disruptions.

Computer experts identified the Y2K problem as early as 1971[21] but business and government made little effort to take corrective action until the mid-19990s. This exacerbated an already challenging situation and led to near-crisis levels in the late 1990s.[22] In response to growing Y2K concerns, the U.S. Government (USG) interceded in February 1998, establishing the President's Council on Year 2000 Conversion to coordinate the overall Y2K effort for the federal government.[23]

After a two-year federally led effort, underpinned by a $3.2 billion emergency supplemental appropriation, the USG assessed Y2K readiness efforts were largely successful.[24] Although confident there would be no major critical mission system failures, government officials and the public anticipated a wide degree of lesser disruptions. On the contrary, the year 2000 ushered in vociferous millennium celebrations across the globe, but very few systems failures. In the U.S., the DoD lost contact with an intelligence satellite for several hours, some banks experienced limited credit card transaction issues, and there were localized disruptions of Medicare and unemployment insurance benefit processing.[25] Other nations experienced similar minor problems but none of the widespread failures originally anticipated.

---

[21] See R.W. Bemer, "What's the Date?" *Honeywell Computer Journal* 5, no. 4 (1971): 205-208 and Jerome T. Murray and Marilyn J. Murray, *Computers in Crisis* (New York: Petrocelli Books Incorporated, 1984).

[22] Executive Order no. 13073, "Year 2000 Conversion," Code of Federal Regulations, title 3, p. 135-137 (February 9, 1998).

[23] The White House, The President's Council on Year 200 Conversion, *The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion,* by John A. Koskin (Washington, DC: The White House, March 29, 2000), 3.

[24] Ibid., 6-7.

[25] Ibid., 20.

The negligible consequences of Y2K led some to question whether the government overestimated the severity of the problem and misspent billions of dollars on a crisis that never materialized. The Senate Special Committee on the Year 2000 Technology Problem argued the estimated $100 billion[26] spent by government and industry was a wise investment. "Minor consequences aside," its final report states, "the Y2K readiness experience has taught us valuable lessons about the Nation's technological dependencies, interconnections and vulnerabilities."[27] Whether the minor consequences were the result of intensive remediation efforts or experts overestimated the magnitude of the problem, Y2K provided valuable insight on the challenges of critical infrastructure protection (CIP). "Y2K and CIP are related to each other through the linkages-both direct and indirect-between different infrastructure systems. Disruptive effects can propagate through interdependent infrastructures."[28]

The cyberspace domain is a dynamic environment and much has changed since Y2K. In 2000, an estimated 304 million users worldwide had access to the Internet;[29] by the end of 2010, the number rose to over 1.6 billion.[30] The worldwide explosion of the cellular technology is even greater than that of the Internet. Mobile cell phone subscribers increased from 750 million in the year 2000 to over 4 billion in 2010,[31] a large portion of which use fourth generation (4G) devices, providing mobile Internet

---

[26] *The Economics of Y2K*, 24.

[27] Christopher Dorobek, "20 things in 20 years that changed government IT," *Federal Computer Week*, January 8, 2007, http://fcw.com/Articles/2007/01/08/20-things-in-20-years-that-changed-government-IT.aspx?Page=1(accessed December 18, 2010). A separate RAND Corporation study supports this assessment. See David Mussington, *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development* (Santa Monica, CA: RAND Corporation, 2002), 27.

[28] Mussington, 53.

[29] U.S. Department of Commerce, Economics and Statistics Administration, *Digital Economy 2000* (Washington, DC: U.S. Department of Commerce, June 2000), V.

[30] International Telecommunications Union, "The World in 2010: ICT Facts and Figures," http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf (accessed December 23, 2010).

[31] Ibid.

browsing, email, and text applications not available in 2000. The rapid proliferation of wired and wireless technology has had profound effects on commerce. In the third quarter of 2010, U.S. retail electronic commerce totaled $41.5 billion, up from less the $1.2 billion in the first quarter of 2000.[32] These steady advances in information technology and rapidly expanding Internet connectivity increase the likelihood and risks of disruptive effects propagating through interdependent infrastructures.

The Y2K problem served as an early warning of the complexity, interconnectedness, and interdependence of the Nation's critical infrastructure. Over the last decade, the rapid growth of the Internet and computer technology fueled the explosion of information age applications such electronic commerce, on-line banking, and social networking. Government, business, and industry leverage information technology to increase productivity and streamline processes to provide better, faster products and services. The Nation's digital infrastructure is so inextricably linked to its economic prosperity that a large-scale malicious attack could have devastating effects. Unlike the Y2K problem, such an attack would occur without warning, be far more complex than a simple date coding error, and would likely actively infect as it propagated through systems. As such, the economic damage could far exceed the $100 billion spent to remediate the Y2K problem.

Estonia Cyber Attack: "Web War I"

Events in Estonia in the spring of 2007 reveal what a large-scale cyber attack might look like in the U.S. During the period 27 April – 18 May, the country fell prey to

[32] U.S. Department of Commerce, "Quarterly Retail E-Commerce Sales 3rd Quarter 2010," *U.S. Census Bureau News*, November 17, 2010, http://www.census.gov/retail/mrts/www/data /pdf/ec_current.pdf (accessed December 23, 2010).

coordinated cyber attacks against the government, banks, news organizations, and Internet service providers. The cyber offensive began with a series of distributed denial of service (DDoS) attacks to saturate and overwhelm key government and commercial websites. Over the next several weeks, the attacks increased in volume and sophistication, eventually employing an estimated one million unwitting computers, or bots, across the globe to target Estonian e-banking, e-commerce and news media sites.[33]

The attacks, considered politically motivated, originated in Russia in response to the relocation of a Soviet era war memorial in Tallinn, Estonia. Although the Russian government denies being involved, the attack was highly coordinated and an Internet address involved in the attack belonged to an official in the administration of then President, Vladimir Putin. Russian-language forums and chat groups posted detailed instructions on how to participate in the DDoS attacks and specific Estonian websites to target.[34] Despite a formal request, the Russian government has refused to cooperate in an investigation of the incident making it increasingly unlikely Estonian officials will ever catch the perpetrators of the attack.[35]

Although the attacks did little permanent damage, for twenty-two days, unknown attackers economically and politically crippled the tiny Baltic state. Sometimes referred to as Web War I, the attacks on Estonia show how a state actor or group of organized

[33] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington Post*, 19 May 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122 .html (accessed January 3, 2011).

[34] Mark Landler and John Markhoff, "In Estonia, what may be the first war in cyberspace," *The New York Times*, 28 May 2007, http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html?pagewanted=2 (accessed January 3, 2011).

[35] Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective" (paper presented at the 8th European Conference on Information Warfare and Security, Lisbon, Portugal, 2009), 178–79. Estonian officials convicted an Estonian student of Russian descent for a DDoS attack against a political party website but the identities of the main perpetrators of the attack remain unknown.

"hacktivists" can wage a non-military war in the digital age anonymously and with near impunity.

Cyber as a Force Multiplier: Georgia Example

On 19 July 2008, various websites in the country of Georgia began to experience an increase in DDoS incidents. These cyber-events, achieved by overwhelming Web resources, prevented 'legitimate' users from gaining access to or using Internet services, authorized networks, and systems. A Georgian Internet security firm actually reported on these actions, but for the most part, they remained "weak signals" – indicators of change but largely lost in the "noisy" day-to-day Internet environment.[36] Three weeks later things would change.

On 8 August 2008, security experts observed a second, more substantial round of DDoS actions against Georgian websites. They soon realized that these incidents were actually coordinated cyber attacks that within two days successfully shut down most Georgian government websites. More alarming was the timing, as perpetrators closely synchronized their cyber attacks with Russian military operations into South Ossetia.

In response to the attacks, the Georgian government relocated critical Internet services to the U.S., Estonia, and Poland. The relocation to U.S. based servers, accomplished through the cooperation of a private information technology company, occurred unbeknownst to the U.S. government.[37] This quick reaction demonstrated government resolve and a means to lessen the real and psychological effect of disrupting Georgian Internet sites and networks. Ultimately, news and information continued to

[36] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008/2009): 60.

[37] Ibid., 60.

flow from Georgia without much interruption as instant messaging, a lifeline for many with family in the war zone, was mostly unaffected.

Yet, the Russian cyber attacks did have an effect – a lasting effect that went far beyond this minor border skirmish. Russian cyber actions introduced a new adaptation for joint operations and military action – a new integrated domain of warfare – cyber. Most of the analysis of the Georgian cyber attacks centered on identifying the perpetrators, but the larger and more important questions for today focus on net-neutrality and cyber actions as an operating principle within the art of war.[38]

Whereas the attacks against Estonia were prosecuted entirely in cyberspace, strikes against Georgian critical infrastructure show how cyber operations can be used to shape the battlefield ahead of a conventional military operation. Leading up to the 2008 Russian military invasion of South Ossetia, Georgian news and media, government, and financial institution websites were targeted with DDoS attacks.[39] The attacks, coordinated through an online forum and carried out by an army of Russian novice hackers never officially linked to the Russian government, shows how self-organizing cyber militias can be used to advance national interests.

Cyber Neutrality

The issue seems innocuous but in reality, it should be of great concern to U.S. policymakers and military strategists. Even if the United States is not engaged directly in a conflict between nations, cyber-incursions against the U.S. Internet infrastructure are likely. Private industry owns and operates the majority of the Internet system. During a

[38] Korns and Kastenberg, 61.

[39] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, (Tallinn, Estonia: Cooperative Cyber Defense Centre of Excellence, 2008), 8.

cyber conflict, the unregulated actions of third-party actors have the potential of unintentionally influencing U.S. cyber policy, including cyber neutrality. There is little, if any, modern legal precedent. The fact that American IT companies assisted Georgia during a cyber engagement, apparently without the knowledge or approval of the U.S. government, illustrates what is likely to become a significant policy issue. Although nations still bear ultimate responsibility for the acts of their citizens, applying that dictum to the modern realities of cyber conflict is a complex challenge. Georgia's unconventional response to the August 2008 DDoS attacks, supported by US private industry, adds a new element of complication for cyber strategists.[40]

Penetrations of U.S. Critical Infrastructure

According to national security officials, computer hackers from Russia, China, and other countries have penetrated and surveyed portions of the U.S. electrical grid. In addition to mapping the grid, the intruders left behind software tools to allow remote access to control, manipulate, and destroy infrastructure components.[41] The Chinese and Russian governments deny being involved in the intrusions and the U.S. has not publicly attributed activities to state-sponsored organizations, but according to former Director of National Intelligence Dennis Blair, "a number of nations, including Russia and China, can disrupt elements of the U.S. information infrastructure."[42]

The People's Liberation Army (PLA) of China, in particular, is aggressively developing strategic cyber capabilities as part of its "informatization" strategy. Of note,

[40] Korns and Kastenberg, 64-68.

[41] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *The Wall Street Journal*, April 8, 2009. Successful cyber attacks against electrical grids in other countries have plunged entire cities into darkness.

[42] Ibid.

is PLA's novel integration of reservists with specialized critical infrastructure skills in its information warfare units:[43]

> Reservists employed in the chemical industry serve in PLA chemical warfare units, and telecommunications workers serve in units specializing in information warfare and information operations. These highly skilled reservists play a growing role in China's technology-dependent national security strategy of using sophisticated cyber and electronic attacks to degrade battle networks, forward bases and maritime forces, thereby inhibiting a potential adversary's power projection capabilities.[44]

Although intrusions of U.S. critical infrastructure have yet to cause physical damage, there is growing concern that adversaries are using increasingly sophisticated surveillance and exploitation operations to lace U.S. critical infrastructure with trapdoors and logic bombs that they could use to gain strategic advantage in a future crisis or war. The motivation behind the intrusions is unclear, but the ability of one nation to disrupt or cause widespread damage to another's critical infrastructure is a powerful lever, one that might well be threatened or used to influence the targeted nation's actions.

"When change occurs outside of your organization faster than inside of your organization - the end is near."[45] These words spoken by Jack Welch, former CEO of General Electric, provide the strategic framework for defining the cyber threat today and tomorrow. It is all about technology trends and being adaptive to the future. In 1999, the Y2K problem introduced the world to the broad social, financial, psychological, and governance issues that "cyber denial" can inflict upon a nation and its populace. Y2K was the wake-up call, an early education of those preparing to enter the twenty first century. The global celebrations had a cyber-shadow – a harbinger of change. It

[43] U.S. Department of Defense, *Annual Report to Congress, Military and Security Developments Involving the People's Republic of China* (Washington, DC: Office of the Secretary of Defense, 2010), 37.

[44] John Nagl and Travis Sharp, "An Indispensable Force, Investing in America's National Guard and Reserves" (Washington, DC: Center for a New American Security, 2010), 12.

[45] Jack Welch, http://en.thinkexist.com/quotes/Jack_Welch/ (accessed March 14, 2011).

demonstrated that the Nation and the world were already moving towards a networked dependent existence. An existence nourished via a growing and vibrant cyber infrastructure that would soon be far more important and ubiquitous to everyday life than ever imagined. Seven to eight years after the Y2K event, cyber attacks in the form of denial of service events moved from the realm of "lone hackers" to being integrated with military and political actions and decisions.

In 2007, attacks were prosecuted using large networks of compromised computers — known as "botnets" — used to carry out malicious activity without the knowledge of their owners. Upon a broadcast command, or at a predetermined time, these computers begin bombarding their target websites with millions of fake requests for information, overloading them and causing real visitors to the site to experience long delays, or sometimes shutting the websites down altogether.

In 2008, while the specific cyber-attack methodologies remained similar, the cyber domain grew and began to follow a well-worn development path for technologies that went before it such as the machine gun, the airplane, and the conquering of space. Cyber became a domain of the warfighter. Cyber security became a top priority of every government on earth.

Today, there is enormous interest and study of the cyber domain and its multi-faceted appendages such as the cyber security community, the media, and policymakers. The seminal issue is quite simply to improve their understanding of and ability to act on subjects relevant to cyber-attacks, so that the government, military, and the public gain a better appreciation of the opportunity and potential peril this new domain offers to the Nation.

This dichotomy is not lost on the leadership of the United States. Senator Barack Obama, the presidential candidate, harnessed the power of the Internet and social media to raise over $500M, forever changing political elections in America.[46] Meanwhile, a foreign entity, likely from China, harnessed the security vulnerabilities of the Internet to harvest large quantities of policy and strategy files from both the Obama and McCain campaign headquarters networks.[47]

Not surprisingly, Obama made securing the Nation's digital infrastructure an early priority, launching a sixty-day cyber policy review during his first month in office. Announcing the results in May 2009, he aptly summarizes the strategic challenge:

> It is the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day.
>
> And this is also a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that cyber intruders have probed our electrical grid and that in other countries cyber attacks have plunged entire cities into darkness.[48]

The explosion of Information Age technology ushered in a new era of social interaction, electronic commerce and finance, business efficiency, and continued American military dominance. It also exposed the Nation and the world to a new type of threat. The Y2K problem at the dawn of the twenty-first century offered an early glimpse of the vulnerabilities of the Nation's digital infrastructure in a globally connected and interdependent world. Successful cyber-attacks on Estonian and Georgian digital

---

[46] Jose A. Vargas, "Obama Raised Half a Billion Online," *The Washington Post*, November 20, 2008, http://voices.washingtonpost.com/44/2008/11/20/obama_raised_half_a_billion_on.html (accessed April 2, 2011).

[47] Demetri Sevastopulo, "Cyber Attacks on McCain and Obama teams 'came from China,'" *Financial Times*, November 7, 2008, http://www.ft.com/cms/s/0/3b4001e2-ac6f-11dd-bf71-000077b07658.html#axzz1JGiSxHAF (accessed April 2, 2011).

[48] The White House, "Securing Our Nation's Cyber Infrastructure," May 29, 2009.

infrastructure demonstrated how cross-border belligerents using even unsophisticated techniques could hobble a nation with relative ease and almost guaranteed impunity. An ever-increasing number of penetrations, exploitations, and successful attacks of U.S. government and private sector networks, to include the Nation's power grids, underscore the far-reaching challenges and implications this new threat imposes on U.S. national security.

CHAPTER 3: EXISTING STRATEGY, POLICY, ROLES, AND RESPONSIBILITIES

Once insulated from much of the world by the Atlantic and Pacific Oceans, the U.S. military ensured America's security by defeating its enemies on foreign soil. In today's globalized and technology enabled world, nation-states and non-state actors now possess much greater means to reach across the vast expanses of oceans to do the nation harm. The U.S. employs a collective national effort to protect and defend against serious threats to the U.S. homeland such as terrorist attack, weapons of mass destruction, and transnational crime. The cyber threat is no different. It requires the strong cooperation among and synchronized actions of homeland security, military, and law enforcement professionals to be successful.

The 2010 *National Security Strategy* contends today's strategic environment – a shrinking world increasingly populated by lethal threats to the American way of life – is driving the U.S. "beyond traditional distinctions between homeland and national security."[1] This chapter provides an overview of the existing strategy, policy, roles and responsibilities, and interrelationships between homeland defense, homeland security, and defense support to civil authorities in the context of protecting America's digital infrastructure as a national security priority.

Homeland Defense, Homeland Security, and Defense Support of Civil Authorities

Homeland defense (HD) is the "protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and

[1] *National Security Strategy*, 10.

aggression or other threats as directed by the President."[2] Ballistic missile defense and air sovereignty alert are examples of HD missions assigned to the DoD. The DoD defines Defense Support of Civil Authorities (DSCA) as civil support provided under the auspices of the National Response Plan.[3] More simply, it is military support to U.S. civil authorities for domestic emergencies, designated law enforcement, and other activities.[4] Often considered synonymous with or a sub-set of homeland defense, DSCA is a separate and distinct mission. Homeland defense and DSCA missions are similar in nature, sometimes using the same types of forces and equipment, but there is a significant difference.

The DoD is the lead agency for homeland defense operations, but acts in a supporting role to other federal, state, and local agencies during DSCA missions. Executed together, homeland defense and DSCA are the principle ways the DoD executes its highest priority mission – securing the U.S. homeland. The Unified Command Plan (UCP) tasks U.S. Northern Command (USNORTHCOM) with the responsibility of homeland defense and for coordinating and providing forces for DSCA operations. Traditional civil support missions include domestic disaster relief; chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) consequence management; and counter-drug operations.[5] Unless directed by the President, the DoD will always act in a supporting role to assist a primary agency coordinating the federal response.

---

[2] U.S. Joint Chiefs of Staff, *Homeland Defense*, Joint Publication 3-27 (Washington, DC: U.S. Joint Chiefs of Staff, 2007), I-1.

[3] *DoD Dictionary of Military and Associated Terms*, 126.

[4] U.S. Joint Chiefs of Staff, *Civil Support*, Joint Publication 3-28 (Washington, DC: U.S. Joint Chiefs of Staff, 2007), Glossary.

[5] U.S. Department of Defense, United Sates Northern Command, "About USNORTHCOM," http://www.northcom.mil/about/index.html (accessed Oct 23, 2010).

If homeland defense and DSCA are the principle ways the DoD secures the homeland, what is homeland security and does DoD play a role? "Homeland security (HS) is a concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur."[6] An important distinction between HS and HD is that HS is a *concerted national effort* undertaken by multi-jurisdictional federal, state, and local government agencies whereas HD is almost exclusively the purview of the DoD. Figure 1 shows the interrelationships between HD, HS, and civil support missions.

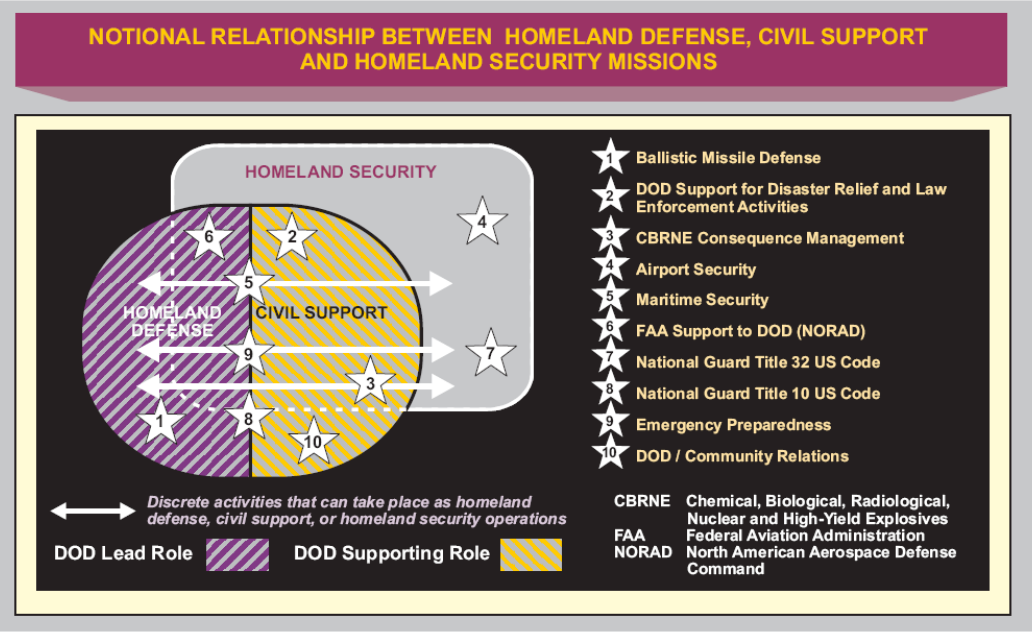

Figure 1. Notional Relationship between Homeland Defense, Civil Support, and Homeland Security Missions[7]

As depicted, the DoD primarily contributes to the homeland security mission through HD and DSCA operations, but some activities such as maritime security and those of the

[6] JP 3-28, Glossary.
[7] Ibid., I-3.

National Guard operating under Title 32 US Code[8] can occur outside the realm of HD and DCSA. Emergency preparedness, measures taken by DOD in advance of an emergency to reduce the loss of life and to protect property and the Nation's institutions, occurs along the entire continuum of HD, civil support, and homeland security. This simple illustration shows the complexities of establishing roles, responsibilities, authorities, and command relationships during homeland operations.

Adding to the complexity is the role law enforcement plays in homeland operations. The U.S. prides itself on adhering to stringent rules of law to protect citizens' physical and civil liberties. As such, virtually all incidents occurring within the homeland will entail a law enforcement aspect. Figure 2 illustrates the interrelationship of law enforcement with homeland defense, homeland security, and DCSA operations. Some events, such as bank robbery, are clearly criminal activities falling under the jurisdiction of local, state, or federal law enforcement authorities. Other threats, such as those posed by transnational terrorist organizations, are not as clear-cut with overlapping responsibilities between the DoD, DHS, and the Department of Justice (DOJ).[9] As will be shown, threats to the Nation's critical infrastructure fall into this latter category with critical infrastructure protection requiring shared responsibility and partnerships between multiple departments and agencies at the federal, state, and local levels.

[8] National Guard forces operating under Title 32 US Code, often referred to as Title 32 status, are not federalized and operate under the control of the state governor.

[9] U.S. Joint Chiefs of Staff, *Homeland Defense and Civil Support Joint Operating Concept*, (Washington, DC: U.S. Joint Chiefs of Staff, October 1, 2007), 13-14.

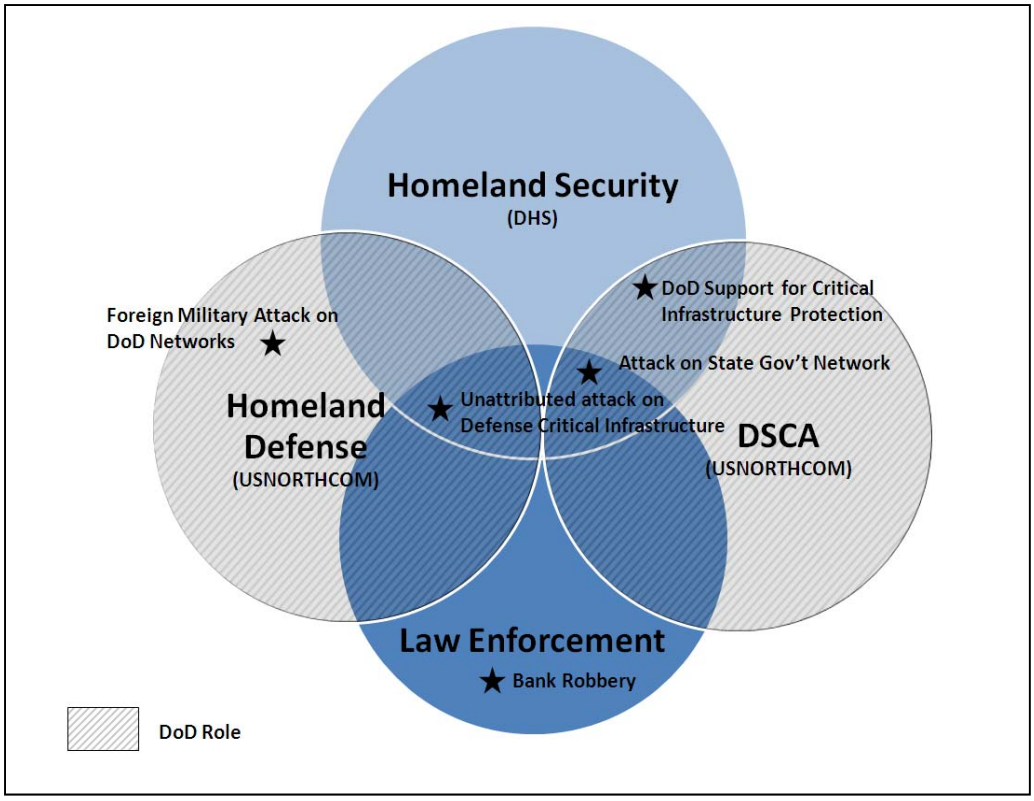

Figure 2. Law Enforcement Relationship to Homeland Operations[10]

Critical Infrastructure Protection/Critical Resource Protection

Per HSPD-7, the Department of Homeland Security is responsible for coordinating the national effort to enhance the protection of critical infrastructure and key resources (CIKR) in the United States. In 2006 and again in 2009, DHS published the *National Infrastructure Protection Plan* (NIPP), establishing the framework for cooperation between federal, state, and local governments and the private sector to mitigate the risks to the Nation's critical infrastructure. The goal of the NIPP is to:

> Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid

[10] *Homeland Defense and Civil Support JOC*, 6-13.

> recovery of CIKR in the event of an attack, natural disaster, or other emergency.[11]

The NIPP identifies the following four objectives for achieving this goal: understanding and sharing threat information; building partnerships to share information and implement protection and resiliency programs; implementing a risk management program to protect CIKR, respond to threats and recover from events that are not preventable; and maximizing efficient use of resources for CIKR protection.[12]

The NIPP and its eighteen supporting Sector-Specific Plans rely largely on volunteer effort among and between sector stakeholders to protect and manage risks to national critical infrastructure. More a common framework than a directive plan, the NIPP calls for participants to promote, coordinate, facilitate, and support each other in such activities as building partnerships, increasing cooperation, and enhancing information sharing. As depicted in Table 1 (page 10), the DoD is the sector-specific agency (SSA) for the defense industrial base (DIB). Consistent with the roles and responsibilities of other the SSAs, the NIPP tasks DoD to collaborate with and encourages risk management strategies among DIB partners, but it is not directive in nature.[13]

DoD Responsibilities for Defense Critical Infrastructure

The Defense Critical Infrastructure Program (DCIP) is the DoD's risk management program for assuring the availability of defense critical infrastructure (DCI) to execute military operations. DCI is the "composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. The DCIP

[11] *NIPP*, 1.
[12] Ibid, 13.
[13] Ibid, 18. *DoD Policy and Responsibilities for Critical Infrastructure*, DODD 3020.40, defines the DIB as the DoD, U.S. Government, and private sector worldwide industrial complex with the capabilities to perform research, development, and design and to produce and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

establishes the defense industrial sector, comprised of ten subsectors (such as the DIB, financial services, global information grid (GIG) and transportation) that encompasses all DoD and non-DoD owned assets deemed essential to the execution of the National Defense Strategy.[14] Tied directly to the Nation's defense, all non-DoD owned portions of the defense industrial sector fall into the category of critical infrastructure as defined by HSPD-7.

The Under Secretary of Defense for Policy (USD(P)) is tasked with overall responsibility for the DCIP, with combatant commanders responsible for preventing or mitigating the loss or degradation of the DoD owned portion of the defense industrial sector within their areas of responsibility. For non-DoD owned portions of the defense industrial sector, the DoD, through USD(P), is tasked to coordinate and collaborate protective efforts with private sector partners, federal agencies (with DHS as the lead federal agency), and state and local governments.[15]

DoD Role in Protecting Civilian Critical Infrastructure

Beyond DoD's role as the lead agency for the DCIP and the sector-specific agency for the DIB, there is little formal guidance on DoD's role in protecting civilian critical infrastructure. The following document review summarizes current DoD policy, roles and responsibilities in this area:

[14] U.S. Department of Defense, *DoD Policy and Responsibilities for Critical Infrastructure*, Department of Defense Directive 3020.40 (Washington, DC: U.S. Department of Defense, January 14, 2010), 14, 17.

[15] Ibid., 5-6.

Joint Publication 3-28, *Civil Support* specifies that DoD is responsible for the defense critical infrastructure and acknowledges that the President or SecDef "may instruct DoD to provide support to another agency."[16]

The *National Response Framework (NRF)* lists DoD as the SSA for the DIB and states that when requested and approved, provides DSCA during domestic incidents.[17] Although the NRF provides little specific guidance for the DoD during a cyber incident, it is an important document in that it establishes the framework for how federal, state, and local agencies plan and respond to all domestic incidents. The specific details of the NRF are beyond the scope of this thesis, but the key premise is that authorities shall handle all incidents at the lowest jurisdictional level possible.

The *National Cyber Incident Response Plan (NCIRP)*[18] provides the most comprehensive guidance to date on DoD roles and responsibilities during a cyber incident:

- The NSA, through the NSA/CSS Threat Operations Center (NTOC), provides information assurance (IA) and Network Threat Operations support to DHS for non-national security systems.[19]

- Recognizes under extraordinary circumstances, the DoD may conduct military operations against cyberspace threats to the U.S. In these instances, DoD is the lead federal agency supported by DHS and other agencies as appropriate.[20]

- When requested and approved, the DoD "can provide technical assistance to gather and analyze information to characterize the attack and to gain attribution of the cyber threat, offer mitigation techniques, perform network intrusion diagnosis, provide technical expertise, and take action to deter or defend against cyber

[16] JP 3-28, III-10.
[17] *NRF*, CIKR-28.
[18] The NCIRP is the result of the 2009 National Cyberspace Policy Review directing DHS to develop a cybersecurity incident response plan. The first publication of the document is the September 2010 interim version.
[19] U.S. Department of Homeland Security, *National Cyber Incident Response Plan* (Washington, DC: U.S. Department of Homeland Security, September 2010), 6.
[20] Ibid., 10.

attacks that pose an imminent threat to national security, where authorized by applicable law and policy. DOD provides DSCA when requested."[21]

- **"At the *State and Local* levels**, and when directed by the Secretary of Defense, DOD provides DSCA when requested and, in close coordination with DHS, shares threat information with the State National Guard and other State-level partners in accordance with applicable statutory authorities and established protocols."[22]

The NCIRP provides a level of detail and specificity well beyond that of the NRF and other incident response plans. Perhaps this is the case because it is the most recently published document on the subject or that it focuses solely on a cyber rather than all-hazards response, but it may be a sign of a more focused national effort to defend the Nation's digital infrastructure against a proliferating cyber threat. Figure 3 summaries the various DoD critical infrastructure roles in the context of homeland defense, homeland security, defense support of civil authorities.

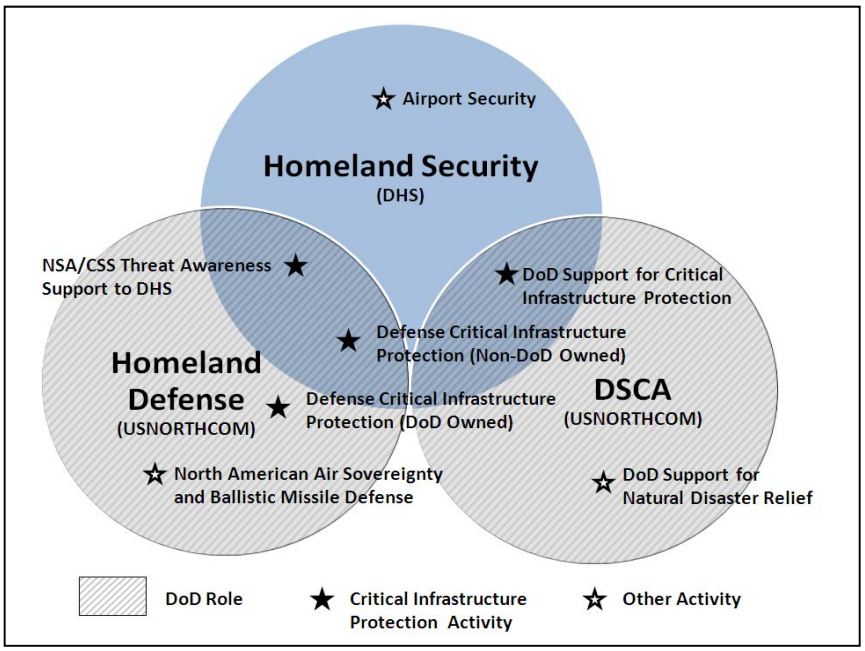

Figure 3. DoD Critical Infrastructure Protection Roles[23]

[21] *NCIRP*, C-2.
[22] Ibid.
[23] *Homeland Defense and Civil Support JOC*, 6.

This chapter provided an overview of the strategy, roles, and responsibilities for defending the Nation's critical infrastructure. The Department of Homeland Security (DHS) is the lead agency for critical infrastructure protection. The DoD, through USNORTHCOM supports DHS through the defense support to civil authority. DHS and DoD share overlapping responsibilities in the area defense critical infrastructure program (DCIP). In this area, DoD is responsible for protecting all DoD owned critical infrastructure, but coordinates closely with DHS to assure risk management of non-DoD owned critical infrastructure deemed essential to national defense. In summary, protection of the Nation's critical infrastructure is an extremely complex endeavor that blurs the traditional lines between homeland security and homeland and requires strong interdepartmental cooperation through all levels of government to be successful.

CHAPTER 4: GAPS, SHORTFALLS, and CHALLENGES

Having explored the cyber dependencies on and complexities of critical infrastructure protection, this chapter analyzes the gaps, shortfalls, and challenges of cyber DSCA in the context of key principles of response doctrine outlined in the *National Response Framework (NRF)*. The NRF and its underlying key principles of response provide the common framework for achieving the goals of *National Strategy for Homeland Security*.[1] The five key principles are: (1) engaged partnership, (2) tiered response, (3) scalable, flexible, and adaptable operational capabilities, (4) unity of effort through unified command, and (5) readiness to act.[2] The final sections of the chapter address seams between the DoD's homeland security and homeland defense roles in cyberspace and explore the challenges of cyber DSCA through the lens of the *Deterrence Operations Joint Operating Concept*.

Principle 1: Engaged Partnership

According to the NRF, the principle of engaged partnership involves developing shared goals and layered, mutually supporting capabilities at all levels of government to plan in times of calm to respond effectively in times of crisis.[3] At the federal level, the DoD is engaged proactively in partnerships with DHS and the public and private sectors

[1] *NRF*, 12. The four goals of the *National Strategy for Homeland Security* are (1) prevent and disrupt terrorist attacks; (2) protect the American people and our critical infrastructure and key resources; (3) respond to and recover from incidents that do occur; and (4) continue to strengthen the foundation to ensure our long-term success.

[2] Ibid., 9. The *National Response Framework* establishes a comprehensive, national, all-hazards approach to domestic incident response.

[3] Ibid.

through a myriad of councils, working groups, and liaison efforts.[4] At the regional level, the DoD relies on ten Defense Coordinating Elements (DCEs) assigned to each Federal Emergency Management Agency (FEMA) region as shown in figure 4.

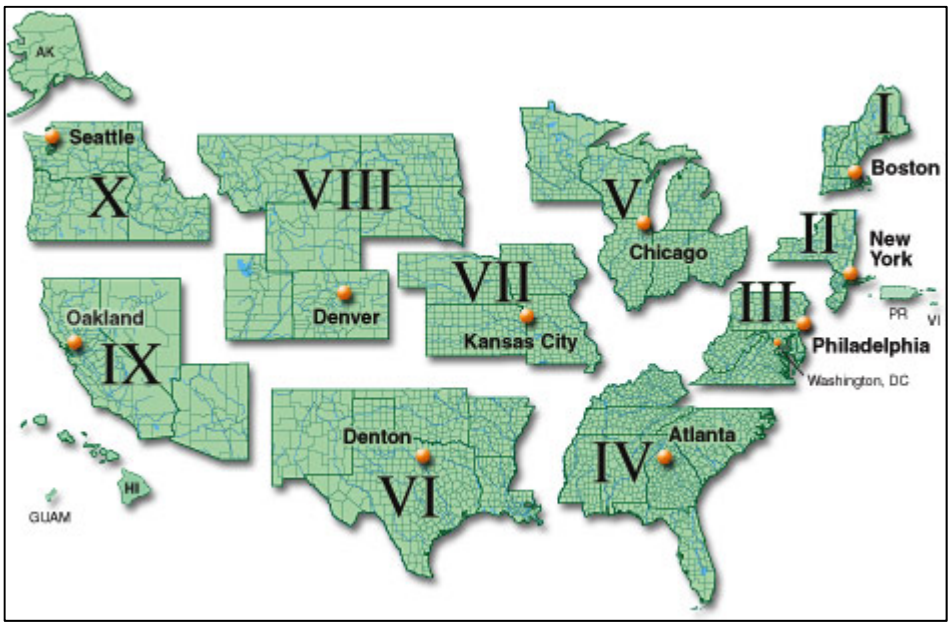

Figure 4. Federal Emergency Management Agency Regions[5]

In addition to the DCEs, the Services provide Emergency Preparedness Liaison Officers (EPLOs) at the state level to coordinate the military response to civil emergency situations and maintain effective communications between the DoD, state, and federal agencies. The U.S. Army, Navy, and Air Force generally provide one EPLO per state and territory. Given such thin staffing at regional and state levels, the Government Accountability Office contends the DoD may "not have the appropriate mix of staff…potentially limiting DoD's ability to provide an optimally coordinated response to

[4] See *NIPP*, Chapter 4 and DoDD 3020.40 for a description of CIKR organizations, councils, working groups, and liaison positions.

[5] U.S. Department of Homeland Security, Federal Emergency Management Agency, "Regional Operations," http://www.fema.gov/about/regions/index.shtm (accessed April 1, 2011).

civil authorities with multiservice capabilities."[6] Even if current staffing levels were adequate to provide a coordinated response to an event, one EPLO per Service in each state and U.S. territory is likely not sufficient to provide the engaged partnerships required to effectively plan for a major cyber attack propagating across multiple infrastructure sectors.

Principle 2: Tiered Response

The basic premise of the tiered response principle is that "incidents must be managed at the lowest possible jurisdiction level and be supported by additional capabilities when needed."[7] As mentioned above, the DoD is actively engaged in partnerships at the national level, but lacks a deep understanding of state-led cybersecurity preparedness, response, and recovery procedures needed to offer an effective and timely response. This is not unexpected, as the DoD currently only responds in a DSCA role when requested and the incident mitigation and recovery exceeds the capacity or capability of local responders.

Principle 3: Scalable, Flexible, and Adaptable Operational Capabilities

National response partners must be prepared to expand rapidly the number, type, and sources of capabilities needed for a given incident. Flexible and adaptable responders facilitate interoperability and improve operational coordination through all phases of response and recovery operations.[8] The DoD would likely have difficulties rapidly expanding the adaptable capabilities required for a cyber DSCA. The DoD has rarely

[6] U.S. Government Accountability Office, *DoD Can Enhance Efforts to Identify Capabilities to Support Civil Authorities during Disasters*, (Washington, DC: U.S. Government Accountability Office, March 2010), 7-15. Quote is from page 7.

[7] *NRF*, 9.

[8] Ibid., 10.

made force structure or weapons system procurement decisions based on defending the homeland, let alone funding and training specialized forces for a supporting role in homeland security.[9] Rightly so, the Services posture military forces, purchase equipment, and design training programs with a primary focus on major combat operations to win the Nation's wars. In many areas though, the forces and equipment needed to wage war are also suitable for saving lives and protecting property in the wake of natural or man-made disasters. This is likely not the case in a cyber response.

The Service Components are still in the process of identifying, training, and certifying the necessary cadre of cyber forces to defend the DoD networks and if necessary exploit and attack adversaries through cyberspace. According to General Keith Alexander, Commander, U.S. Cyber Command (USCYBERCOM), "this is going to take time to generate the force. If you were to ask me what is the biggest challenge we currently face? It is generating the people that we need to do this mission. We have our command stood up, our staff stood up, but the force is what we now have to rely on."[10]

In the event of a major cyber attack requiring civil support, most of the DoD cyber force may already be engaged defending DoD networks or planning and executing offensive cyber actions. On a positive note, the DoD is looking to the Reserve Component to help fill the gap. As Lt. Gen. George Flynn, deputy Marine Corps commandant for Combat Development and Integration commented recently, "we are taking a total force look and the challenge is not only getting the active duty, but also the reserves. It's something that we can take a look at when we try to define what an

[9] Michael E. O'Hanlon, *Budgeting for Hard Power: Defense and Security Spending Under Barack Obama* (Washington, DC: Brookings Institute Press, 2009), 17.

[10] Jason Miller, "Workforce is DoD's Biggest Cyber Challenge," September 24, 2010, http://www.federalnewsradio.com/?nid=35&sid=2061303 (accessed December, 4, 2010).

operational reserve is. We also have to attract the professional civilian workforce as well."[11]

Principle 4: Unity of Effort Through Unified Command

USNORTHCOM and DHS have worked closely to resolve command and control issues between DoD and civilian responders identified during Hurricane Katrina and other relief efforts. Achieving unity of effort during multi-agency and multi-jurisdictional operations will always be a challenge, but the *National Response Framework* adequately addresses command and control relationships between the DoD and the homeland security unified command structure.[12]

Although not a unity of effort issue between Departments, one potential internal area of concern the DoD should address is the clarification of roles and responsibilities between USNORTHCOM and USSTRATCOM with respect to cyber civil defense. USNORTHCOM is specifically responsible for coordinating and providing forces for DSCA operations whereas USSTRATCOM, through USCYBERCOM, is responsible for synchronizing planning and executing cyber operations when directed.[13] Admiral James Winnefeld, USNORTHCOM commander, in recent testimony before the Senate Armed Forces Committee acknowledged these overlapping responsibilities, stating the command is "closely examining the role USNORTHCOM would play in response to a cyber attack in order to synchronize our efforts with U.S. Strategic Command and U.S. Cyber Command."[14] Maturing and codifying these roles in the near term are critical to avoiding the command

[11] Miller.
[12] *NRF*, 10-11.
[13] The White House, *Unified Command Plan 2011* (Washington, DC: The White House, April 6, 2011) 12-14, 28-30.
[14] U.S. Congress, Senate, Committee on Armed Services, *Statement of Admiral James A. Winnefeld, Jr, Commander U.S. Northern Command and North American Aerospace Defense Command*, 112th Cong., 1st sess., April 5, 2011, 9.

and control failures experienced during Hurricane Katrina and ensuring the DoD stands ready to properly assist DHS in protecting the Nation's critical infrastructure against a cyber attack.

Principle 5: Readiness to Act

"National response depends on the instinct and ability to act. A forward-leaning posture is imperative for incidents that have the potential to expand rapidly in size, scope, or complexity, and for no-notice incidents."[15] The DoD, however, does not respond in a civil support role until requested through the NRF or as directed by the President. USNORTHCOM's civil support posture, "not a minute too soon, not a second too late"[16] is too reactive for cyber DSCA events. In order to be effective, DoD forces need to be consistently engaged in the public-private CIKR partnership to be ready to act in a response role. Once again, this should not be a surprising as the DoD does not typically dedicate forces to homeland security.

The NRF focuses largely on the third goal of the *National Strategy for Homeland Security*: responding to and recovering from incidents that do occur.[17] As discussed above, the DoD, playing a supporting role to other agencies in the DSCA arena is postured solely for reactive response and recovery actions. As such, the DoD lacks the ability to act as an engaged partner, prepared to provide a flexible, adaptive response at the federal, state, and local levels. The next section explores how the DoD is approaching the cyberspace domain from a homeland defense perspective and how military cyber deterrence operations may impact critical infrastructure.

[15] *NRF*, 12.

[16] NORAD & USHORTHCOM Plans, Policy & Strategy Directorate, "NORAD and USNORTHCOM Operation Plans Summary," briefing slides, http://www.scribd.com/doc/43717734/NORAD-NORTHCOM-Plans-Summary-Interagency (accessed March 6, 2011).

[17] *NRF*, 12.

Overlap between DoD's Homeland Security and Homeland Defense Roles in Cyberspace

The DoD has taken the emerging cyber threat seriously. Recognizing the increasing importance of cyberspace as war fighting domain, the United States Secretary of Defense directed U.S. Strategic Command to establish a sub-unified command for cyberspace operations. On 21 May 2010, U.S. Cyber Command (USCYBERCOM) achieved initial operational capability, its mission to "direct the operations and defense of specified DoD…networks and…when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains."[18] Although organized for full-spectrum computer network operations, the impetus for establishing USCYBERCOM was a series of increasingly sophisticated and successful attacks against DoD unclassified and classified networks.[19]

As USCYBERCOM and the Services continue to harden the DoD network against the millions of daily probes and attacks against it, adversaries will seek alternate means to deny or disrupt U.S. military actions in cyberspace. An indirect approach is to target critical infrastructure. Successful attacks against the broader U.S. telecommunications, energy, transportation, and financial sectors could achieve many of same effects as attacking DoD networks.

The major problem is that the DoD does not own the critical non-DoD infrastructure, nor does it have primary responsibility for it. Certainly, the DoD can provide military forces to help physically protect critical infrastructure. An example is Operation Noble Eagle, where the DoD provided Reserve Component forces to assist in securing airports,

[18] U.S. Department of Defense, U.S. Cyber Command Public Affairs, "U.S. Cyber Command Fact Sheet," http://www.stratcom.mil/factsheets/cc/ (accessed 15 August 2010).

[19] Ellen Nakashima, "Pentagon Cyber Unit Prompts Questions," *The Washington Post*, June 13, 2009.

seaports, federal facilities, large dams, and other critical infrastructure. The DoD is well suited for this type of physical security and can quickly mobilize without requiring any special training beyond rules of engagement familiarization.

In the same way that DoD could be called upon to provide physical protection of critical infrastructure, the DoD should be prepared to assist in defending against virtual threats as well. Virtual protection against a cyberspace threat is a far more complex and specialized undertaking than providing physical protection. It is in this area, providing defense support of civil authorities to protect the Nation's critical digital infrastructure, that the DoD needs to make a more concerted effort.

Cyber Deterrence

John Mearsheimer in *Conventional Deterrence* notes that "deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[20] Since World War II, a key element of U.S. national strategy has been deterrence and the threat of retribution by way of an overwhelming nuclear arsenal and a dominant conventional military force. The strategy of deterrence by retribution has generally served the U.S. well, but that may be changing in cyberspace. "For deterrence to work the threat of retaliation must be credible enough to alter the cost-benefit analysis of our adversaries. However, the realities of the cyber realm undermine the credibility of response."[21]

There are numerous problems associated with mounting a response to a cyber attack. The first challenge is attribution. As the Estonia and Georgia examples show, attacks can

[20] John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), 14.
[21] Eugene E. Habiger, *Cyberwarfare and Cyberterrorism: The Need For A New U.S. Strategic Approach* (Washington, DC: The Cyber Secure Institute, 2010), 3.

originate from hijacked computers and servers across the globe, the open and anonymous nature of the Internet makes it easy for sophisticated hackers to cover their trail, and it is difficult to ascertain the purpose of the attack – criminal, vandalism, espionage, or an act of war.[22]

The second problem is the risk of collateral damage. Due to the highly interconnected, interdependent nature of networks comprising cyberspace, a preemptive or retaliatory attack against an adversary could easily disrupt or damage civilian infrastructure or spill over to a neutral country. For example, leading up the U.S. invasion of Iraq in 2003, "military planners considered a computerized attack to disable the networks that controlled Iraq's banking system, but they backed off when they realized that those networks were global and connected to banks in France."[23]

Another deterrence challenge is that the U.S. is at an asymmetric disadvantage with many of its potential foes in cyberspace. The U.S. economy and military are heavily dependent on technology and digital infrastructure making it an appealing, target rich environment for adversaries. Less technically developed nations and non-state actors may not be deterred from attacking the U.S. in cyberspace because there is little damage the U.S. could cause through a cyber response action. North Korea, for example, is a nation with so little dependence on cyberspace it is largely impervious to a large-scale cyber attack.[24] Non-state actors are even more difficult to deter. Operating overtly or

[22] John Markoff, David Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times*, November 13, 2009.

[23] Shane Harris, "The Cyberwar Plan," *National Journal*, November 13, 2009, http://www.proquest.com/ (accessed March 6, 2011).

[24] Richard A Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins Publishers, 2010), 149. North Korea is the suspected source of denial of service attacks against the U.S. and South Korea in July 2009.

covertly in another nation's territory, they have little or no digital infrastructure the U.S. can directly attack.[25]

The issues described above are but a few examples of the challenges the U.S. faces in pursuing a deterrence by retribution strategy in defending the Nation's critical infrastructure.[26] This is not to say the U.S. should not pursue offensive cyber capability. On the contrary, according to Deputy Secretary of Defense, William J. Lynn III, "In cyber, offense is dominant. A fortress mentality will not work. We cannot retreat behind a Maginot line of firewalls. In this way cyber is much like maneuver warfare, in which speed and counterattack matter most. If we stand still for a minute, our adversaries will overtake us."[27] Yet, despite the widely recognized view the U.S. possesses "pre-eminent offensive cyber capabilities,"[28] it has done little to dissuade adversaries from attacking in cyberspace.

Beyond imposing costs, another way the U.S. can influence an adversary's decision-making calculus is to deny the benefits of a hostile action.[29] The principle means for denying adversary benefits are pre-emptive offensive operations and defensive action, both active and passive. Offensive actions, sometimes referred to as dynamic or pro-

[25] Habiger, 26.

[26] For a more detailed discussion of cyber deterrence see Martin J. Libicki, *Cyberdeterrence and Cyberwar*, (Washington, DC: RAND Corporation, 2009), 39-73 and Richard L. Kugler, *Cyberpower and National Security* (Washington, DC: National Defense University Press and Potomac Books, 2009), 309-342.

[27] William J. Lynn III, "Remarks delivered at STRATCOM Cyber Symposium," May 26, 2010, http://www.defense.gov/speeches/speech.aspx? speechid=1477 (accessed February 28, 2011).

[28] James A. Lewis, "Korean Cyber Attacks and Their Implications for Cyber Conflict," October 2009, http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf (accessed February 5, 2011).

[29] U.S. Joint Chiefs of Staff, *Deterrence Operations Joint Operating Concept*, (Washington, DC: U.S. Joint Chiefs of Staff, December 2006), 5. The third way of affecting the adversary's decision calculus is to encourage adversary restraint. The U.S. can advance cyber restraint using the information and diplomatic instruments of power to establish international norms or treaties governing cyber conflict.

active defense, aim to discover and thwart attackers outside the U.S. These actions are the purview of USCYBERCOM and are outside this research topic.

DHS is the primary agency responsible for defensive actions to protect and defend critical infrastructure, but like all effective deterrence operations, it is a team effort. As the *Deterrence Operations Joint Operating Concept* points out, "Deterrence is most likely to be effective when the actions and capabilities of the joint force are integrated with those of the interagency and as necessary, non-state and multinational partners."[30]

This chapter described how the DoD, given the current policy and guidance for DCSA operations, is not well postured to support DHS in defending the Nation's critical infrastructure. Specifically, the DoD is lacking in four of the five key principles of response doctrine outlined in the *National Response Framework* necessary for advancing the goals of the *National Strategy for Homeland Security*. It also explored the critical infrastructure problem through the lens of deterrence operations, highlighting the challenges the U.S. faces in effectively deterring adversaries in the cyber domain. The next chapter makes provides recommendations on how the DoD can better team with DHS to strengthen security and resilience at home against large-scale cyber attacks.[31]

[30] *Deterrence Operations JOC*, 9.
[31] *National Security Strategy*, 18.

This Page Intentionally Blank

CHAPTER 5: FINDINGS AND RECOMMENDATIONS

Scores of U.S. government officials including the President, recognizing the strategic importance of the Nation's critical infrastructure and key resources (CIKR), have increasingly called for a concerted national effort to protect and defend against a cyber attack. This is not a notional threat. Over 100 countries have or are actively developing offensive cyber capability with the potential to disrupt another nation's digital infrastructure.[1] Adversaries have already threatened U.S. national security and economic prosperity by penetrating and inserting malicious code in U.S. electric grids and exfiltrating terabytes of sensitive USG, DoD and private sector intellectual data.

The Department of Homeland Security (DHS), the lead federal agency for defending non-DoD government infrastructure and coordinating efforts to protect private sector CIKR, faces significant challenges executing this tremendously complex mission. Some even argue that DHS is ill-suited to lead in a conflict against foreign militaries or intelligence agencies.

> Securing cyberspace is no longer an issue defined by homeland security or critical infrastructure protection. This is far too narrow a scope. Cybersecurity is no longer (if it ever was) a domestic issue. It is an issue of international security in which primary actors are the intelligence and military forces of other nations. Cybersecurity requires harnessing U.S. international efforts, along with offensive capabilities and strong intelligence action to support comprehensive national security strategy.[2]

Recognizing these complex challenges, the *National Security Strategy* calls for strong partnerships throughout all levels of government and the private sector to address

[1] *Homeland Security Newswire*, "Chertoff calls for cyber-deterrence doctrine," October 15, 2010, http://homelandsecuritynewswire.com/chertoff-calls-cyber-deterrence-doctrine (accessed March 15, 2011).

[2] Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency," (Washington, DC: Center for Strategic and International Studies, December 2008), 35, http://csis.org /files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed August 3, 2010).

the cybersecurity problem.[3] This chapter provides recommendations that if implemented will strengthen these partnerships and better support DHS in protecting the Nation's critical infrastructure.

<u>Recommendation 1:</u> The DoD should take a more proactive, homeland defense approach to protecting the U.S. critical infrastructure against a cyber attack.

The United States can no longer rely on passive, reactionary defensive means to protect the Nation's CIKR. The DoD has long recognized the importance of synchronizing the efforts of computer network defense, exploitation, and attack operations to meet its military objectives in cyberspace. To integrate all aspects of cyberspace operations more fully and achieve unity of command, Secretary Gates directed the establishment of U.S. Cyber Command, with the Commander USCYBERCOM dual-hatted as the Director, National Security Agency (DIRNSA).[4]

The United States Government must take the same comprehensive approach to defend government and private sector digital infrastructure effectively. However, DHS lacks the offensive and exploitation capabilities to accomplish adequately its mission. Attempting to duplicate the offensive capabilities of USCYBERCOM and the signals intelligence competencies of the NSA would far exceed DHS's resources and possibly its authorities. "The bottom line here is that NSA is a treasure, a national treasure. Its resources are extensive. No one I think would want the Department of Homeland Security to try to replicate those resources to carry out its responsibility to protect Federal

[3] *National Security Strategy*, 28.

[4] U.S. Secretary of Defense Robert Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," memorandum for Secretaries of the Military Departments, Washington, DC, June 23, 2009.

Government civilian networks—and civilian networks."[5] In purely budget terms, the DoD (predominantly through USCYBERCOM) projects to spend $2.3 billion in fiscal year 2012 on cyber programs, more than twice that of DHS.[6] The "national treasure" that is NSA and the highly capable, well-resourced USCYBECOM has much to offer DHS and other partners.

Acknowledging the substantial capabilities DoD brings to the cyberspace domain, Secretary Gates directed the USCYBERCOM to provide support to civil authorities.[7] Likewise, the NSA's stated role in critical information protection is to provide technical support and threat information to DHS.[8]

As previously discussed, DSCA is the primary means the military provides support to non-DoD partners. However, the DSCA framework fails in the cyber arena on at least two accounts. The time lapse between a request for support and the actual response is too long to be effective in cyberspace. Attacks often occur with little or no warning and require a real time response to attribute and, if required, respond offensively against the source of the attack. Essentially, proactively defending the Nation's critical infrastructure against a cyber attack is as much homeland defense (HD) as it is support to civil authorities. The United States must view threats against the Nation's critical infrastructure through cyberspace in the same manner it would than any other attack in or through the physical land, air, and sea domains.

---

[5] U.S. Congress, Senate, Committee on Armed Services, *Nominations of VADM James A. Winnefeld, JR., to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Defense Command; and LTG Keith B. Alexander USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command*, 110th Cong., 2nd sess., April 15, 2010, 18. Quote is by Senator Joseph Lieberman.

[6] David Perera, "Cybersecurity Runs Deep in Fiscal 2012 Budget Request," February 16, 2011, http://www.fiercegovernmentit.com/story/cybersecurity-runs-deep-fiscal-2012-budget-request/2011-02-16 (accessed March 15, 2011).

[7] SecDef Gates, "Establishment of a Subordinate Unified U.S. Cyber Command."

[8] *Nomination of LTG Alexander*, 18.

"Success in the HD mission is defined as detecting, deterring, preventing, and if necessary, defeating a direct attack upon the Homeland."[9] Applying this definition of success in protecting CIKR, the DoD can best support civil authorities by leveraging NSA's vast signals intelligence enterprise and USCYBERCOM's warfighting capabilities to: detect threats outside the homeland; deter and prevent adversaries by imposing costs and denying benefits; and if necessary defeat by destroying adversary capabilities through kinetic or non-kinetic means. This is not to say the DoD should take the lead on CIKR protection, but rather that DoD can best support from a proactive homeland defense mindset, rather than the more traditional, reactive DSCA role. In other words, the overlap between homeland security, homeland defense, and civil support mission sets is greater in cyberspace than the other domains.

Fortunately, in the last six months, the DoD has made several promising strides toward a proactive approach to critical infrastructure protection. The 2011 *National Military Strategy* calls for U.S. Strategic Command and U.S. Cyber Command to "collaborate with U.S. government agencies, non-government entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills." Further, the strategy commits to continuing "to dedicate, fund, and train a portion of the National Guard for homeland defense and defense support of civil authorities."[10] This appears to signal an important sea change in the DoD. In the 2008 *National Defense Strategy*, the DoD while recognizing the important supporting role it plays in homeland security and civil support missions, made this case for a much more limited future role:

[9] *Homeland Defense and Civil Support JOC*, 4.

[10] U.S. Department of Defense, *The National Military Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2011), 10-11.

> In the long run the Department of Defense is neither the best source of resources and capabilities nor the appropriate authority to shoulder these tasks. The comparative advantage, and applicable authorities, for action reside elsewhere in the U.S. government, at other levels of government, in the private sector, and with partner nations.[11]

Perhaps the most significant evidence to date of the changing attitude towards DoD's role in CIKR protection is a memorandum of agreement (MOA) signed by DoD and DHS in October 2010. In an effort to work more closely to protect CIKR, the agreement embeds DoD cyber analysts within DHS and vice versa to increase interdepartmental collaboration and synchronization of DHS's homeland security and DoD's national security missions.[12] Although the MOA does not alter either Departments' assigned roles or authorities, the DoD is said to be seeking new authorities to better assist in defending the Nation's critical infrastructure.[13] These positive steps indicate a newfound interest within the DoD to partner more actively in defending the Nation's based on the reality that advanced persistent threats can negatively impact the DoD's mission through the highly interconnected, interdependent DoD and non-DoD digital infrastructures.

<u>Recommendation 2:</u> Leverage the Reserve Component to defend U.S. critical infrastructure.

As mentioned in the introduction, the Deputy Secretary of Defense has called for DoD to make better use of Reserve Component forces in dedicated cyber missions.[14] This recommendation makes an argument, in the general case, that the Reserve

[11] U.S. Department of Defense, *National Defense Strategy* (Washington, DC: U.S. Department of Defense, 2008), 7.

[12] U.S. Department of Homeland Security and U.S. Department of Defense, "Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," Washington, DC, October 13, 2010.

[13] *National Military Strategy*, 10.

[14] William J. Lynn III, "Remarks on Cyber at the RSA Conference," February 15, 2011, http://www.defense.gov/speeches/speech.aspx?speechid=1535 (accessed February 18, 2011).

Component is uniquely suited to perform an increased role in cyber DSCA missions based on the strengths of National Guard and Reserves organization, people, and mission. The final recommendation provides the more specific organizational framework for this expanded role.

Reserve Component service members' civilian backgrounds provide specialized skill sets that may be either not resident in or difficult to retain in the active duty force. "Many of these complex missions require specialized skills, and one of the strongest arguments in favor of maintaining a strong operational Reserve Component is the opportunity for the U.S. military to draw upon cutting-edge skills and knowledge from the civilian world."[15] These skills, including network forensics and deep packet analysis, are in short supply throughout the federal and private sector workforce. It requires a skilled and adaptable workforce, more than simply the latest suite of security tools, to defend successfully against advanced persistent threats.[16] The Reserve Component can help provide this adaptable, technical adept workforce as well as provide a vehicle to retain highly skilled cyber operators leaving active duty.

In addition to providing specialized capabilities that may not be widely available throughout the Active Component, the Reserve Component provides additional capacity and continuity to the cyber DSCA mission. Active Component cyber forces will likely already be committed to defending DoD critical infrastructure when DSCA is required. Even if active duty forces are available, the Reserve Component provides a "local face" through a community-based force, more attuned to the local environment and therefore

[15] Nagl and Sharp, 14.
[16] Evans and Reeder, 2.

more readily integrated than federal responders. As the *National Response Framework* notes,

> one of the challenges to effective response is the relatively high turnover and short tenure among elected and appointed officials responsible for response at all levels. Effective response hinges upon well-trained leaders and responders who have invested in response preparedness, developed engaged partnerships, and are able to achieve shared objectives.[17]

The Reserve Component, with deep community roots and longevity of the force, can provide the continuity and experience that may be lacking in elected and appointed officials.

The National Guard, operating in Title 32 status, provides an additional advantage over active duty and reserve forces in the DSCA arena. When not federalized, National Guard personnel are under the control of state Governors and not subject to the Posse Comitatus Act which prohibits the military from engaging in law enforcement activities. Effectively employed, the National Guard can help eliminate the seam between military and law enforcement operations without the risk of violating established authorities.[18] This is particularly important in the cyberspace domain, where attribution is difficult, driving most incidents, at least initially, to law enforcement jurisdiction.

Another rationale for expanding the Reserve Component's role to help protect the Nation's digital infrastructure is its wide geographical distribution throughout the United States. The National Guard alone "is located in more than 3,300 communities around the nation providing an indispensable link between the military and the citizens"[19] Add to this, the Army, Navy, Air Force, and Marine Reserve training centers, and virtually every

---

[17] *NRF*, 2.

[18] *Homeland Defense and Civil Support JOC*, 15.

[19] Craig R. McKinley, *Chief National Guard Bureau in Statement before the Senate Appropriations Committee on the Fiscal Year 2011 Guard and Reserve Budget*, Statement presented to the 111th Cong., 2nd sess. (Washington, DC: The National Guard Bureau, March 24, 2010).

area of the country is covered. The DoD will certainly not constitute cyber DSCA organizations in all these locations, but it provides opportunity and a wide range of options for posturing forces to most effectively support civil authorities.

One such example of how the DoD can take advantage of location is to organize specialized units in geographic proximity to cyberspace and critical infrastructure research and innovation communities. These Reserve Component units, over time, will develop relationships with government, academic, and industry partners such as national laboratories, NSA/DHS accredited universities,[20] and federally funded research and development centers (FFRDCs) providing a valuable conduit for cooperation, technology transfer, and information sharing. This type of initiative supports the strengthening partnerships and employing new technology themes in the *National Security Strategy* by applying "the ingenuity of public and private sectors … (to) help us protect our citizens and advance U.S. national security priorities."[21]

Additionally, the DoD should leverage and shape already existing Reserve Component capabilities and programs to provide more engaged partnerships, improve unity of effort, and expand the Department's scalable adaptable response force to better support the cyber DSCA mission. These capabilities and programs include the Joint Force Headquarters-State, the Emergency Management Assistance Compact, and the Critical Infrastructure Program.

[20] *The National Security Agency Information Assurance Web Page*, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml (accessed February 15, 2011. The NSA and DHS jointly sponsor the National Centers of Academic Excellence in IA Education (CAE/IAE) and CAE-Research (CAE-R) programs. The goal of these programs is to reduce vulnerability in national information infrastructure by promoting higher education and research in information assurance.

[21] *National Security Strategy*, 31.

Joint Force Headquarters-State: Although the last chapter established that the *National Response Framework* adequately addresses unity of command versus unity of effort between DoD and non-DoD responders, the National Guard's Joint Force Headquarters-State (JFHQ-State) construct ensures DoD unity of command within states and territories. The JFHQ-State provides command and control of all National Guard forces in the state or territory, acts as an information channel to the National Guard Bureau and combatant commanders, and during contingency operations, can also act as a joint headquarters for national-level response efforts.[22]

The JFHQ-State is particularly important in a cyber event because, as was recognized in the Y2K response, many interdependencies exist between physical and cyber infrastructures. During a major cyber incident, the JFHQ-State, having command of all state level NG forces can integrate and synchronize the overall efforts of both cyber and physical infrastructure responders. The following finding from DHS's 2009 Cyber Storm II exercise reinforces the need to consider these interdependencies during planning and crisis response:

> Cyber events have consequences outside the cyber response community, and non-cyber events can impact cyber functionality. Fully understanding this reality is critical to refining comprehensive contingency plans and response capabilities. It is necessary to continue to converge and integrate response procedures tailored for physical crises with those developed for cyber events. The unique activities related to cyber response activities must be highlighted in cyber response processes and procedures to clearly reflect the inherent differences between cyber response and traditional/physical crisis response activities.[23]

[22] National Guard Bureau, The National Guard Media Factsheets, "Joint Force Headquarters-State," http://www.ng.mil/media/factsheets/JFHQ-State.pdf 9 (accessed September 15, 2010). In the case of the District of Columbia, the Secretary of the Army provides command of National Guard forces.

[23] Department of Homeland Security, Office of Cybersecurity and Communications, National Cyber Security Division, *CYBER STORM II Final Report* (Washington, DC: Department of Homeland Security, July 2009), 11.

Emergency Management Assistance Compact (EMAC): Local response capacity is often quickly overwhelmed during a disaster. Through a Congressionally-ratified mutual aid agreement called the Emergency Management Assistance Compact (EMAC), the Governor of a disaster-affected state can request state-to-state assistance during declared states of emergency.[24] The primary strength of EMAC is that it allows a fast and flexible response to meet immediate shortfalls in both capacity and capability. In response to a cyber DCSA incident, specialized National Guard capabilities from neighboring states can quickly respond in a state role or Title 32 capacity to assist local authorities with mitigation and recovery efforts, often faster than a federal response force is available on scene.

Critical Infrastructure Protection Program: The National Guard, through an existing partnership with DHS, provides all-hazard risk assessments on prioritized Federal and State critical infrastructure in support of DHS and the DoD Defense Critical Infrastructure Program (DCIP).[25] The 2005 *Defense Authorization Act* modified U.S. Title 32 code allowing the National Guard to provide military protection of national infrastructure.[26] National Guard Critical Infrastructure Protection – Mission Assurance Assessment (CIP-MAA) Teams currently support the DoD and DHS by conducting vulnerability and mission assurance assessments of designated critical infrastructure sites such as public works, communications and transportation facilities, industrial sites and electrical power systems. CIP-MAA teams successfully conducted over 200 assessments

[24] National Guard Bureau, The National Guard Media Factsheets, "Emergency Management Assistance Compact," http://www.ng.mil/media/factsheets/EMAC.pdf (accessed September 10, 2010).

[25] National Guard Bureau, "The National Guard's Role in Homeland Defense, Critical Infrastructure Protection-Mission Assurance Assessments," http://www.ng.mil/features/HomelandDefense/cip-maa/index.html (accessed September 10, 2010).

[26] *Defense Authorization Act of Fiscal Year 2005*, Public Law 108-375, § 901, *Homeland Defense Activities Definitions*, § 902, *Homeland Defense Activities: Funds*.

in FY10 and anticipate doing the same in FY11.[27] Currently focused primarily on physical security assessments, the teams are comprised of utilities, transportation, security, and emergency management specialists.[28] Current DoD policy authorizes the program to consider "cyber issues,"[29] so DoD and DHS should consider expanding the CIP program to include information assurance and network security.

The *National Security Strategy, Quadrennial Defense Review, National Military Strategy* (NMS), NRP, and NIPP all recognize DoD's vital role in homeland security and the need to strengthen partnerships and cooperation horizontally and vertically with all levels of government and with the private sector. As identified above, the Reserve Component possesses unique strengths, characteristics, and existing programs that can be easily adapted to bolster DoD support to civil authorities during cyber events. Perhaps most importantly, the Reserve Component provides decisive linkages, the connective tissue between local and federal government, between the public and private sector, and between the government and its citizens that is needed to protect and defend the Nation's infrastructure against a cyber attack. Having established *why* the Reserve Component is the right force for the cyber DSCA mission, the final recommendation addresses *how* the DoD can organize units to perform the mission.

[27] National Guard Bureau, "2012 National Guard Bureau Posture Statement," 29, http://www.ng.mil/features/ngps/2012_ngps.pdf (accessed March 8, 2009).

[28] National Guard Bureau, "National Guard Critical Infrastructure Protection Assessment Teams (CIP) Teams," July 17, 2008, http://www.ng.mil/features/ngps/2011/National%20Guard%20Critical%20Infrastructure%20Protection%20Assessment.pdf (accessed August 15, 2010).

[29] DODD 3020.40, 14.

<u>Recommendation 3.</u> Apply the DoD Chemical, Biological, Radiological, Nuclear and high-yield Explosive (CBRNE) Consequence Management model to Cyber DSCA.

In most cases, the DoD uses dual role capabilities to support both its overseas and homeland missions. However, there are certain specialized capabilities dedicated solely to the homeland. Most notable are the forces performing the North American Aerospace Defense Command (NORAD) homeland defense mission. Under NORAD, active duty, reserve, and NG units throughout the United States provide aerospace monitoring, ensure air sovereignty, and provide an integrated air defense capability for the National Capital Region (NCR).[30]

Less common are DoD units dedicated to the homeland security mission. In this arena, the DoD, through USNORTHCOM, provides a highly specialized consequence management force to support civil authorities during chemical, biological, radiological, nuclear and high-yield explosive (CBRNE) disasters. CBRNE response is in many ways similar to a cyber DSCA response and therefore the CBRNE Consequence Management Enterprise, summarized in table 2, offers an organizational framework that the DoD should consider for cyber DSCA.

[30] North American Aerospace Defense Command, "About NORAD," http://www.norad.mil/about/index.html (accessed February 8, 2011).

Table 2. CBRNE Consequence Management Enterprise[31]

Capability	Number Postured	Mission	Size	Composition/C2
Defense CBRNE Response Force (DCRF)	1	• 24-24 hr Response • CBRNE operations, medical, aviation	5200	DoD (T10)/Federal Task Organized
Consequence management Command & Control Element (C2CRE)	2	• 24-24 hr Response • Medical, Search & Extraction, Decon, Security, C2	1500	DoD (T10)/Federal Task Organized
CBRNE Enhanced Response Force Package (CERFP)	17	• 6-12 hr response • Medical, Search & Extraction, Decon, C2	~170	NG (T32/SAD) Task Organized
Homeland Response Force (HRF)	10	• 6-12 hr response • Medical, Search & Extraction, Decon, Security, C2	~570	NG (T32/SAD) Task Organized
WMD-Civil Support Team (CST)	57	• First Response • Initial Assessment	22	NG (T32) Unit Organized

The backbone of the CBRNE response force is a small Weapons of Mass Destruction Civil Support Team (WMD-CST), resident in each state and territory to provide first response and initial assessments after an attack or incident.[32] Larger CBRNE Enhanced Response Force Packages (CERFPs) and CBRNE Consequence Management Response Force (CCMRF) teams are postured regionally to provide a follow-on capability. There are currently seventeen operational CERFPs. The DoD originally envisioned three CCMRFs but during the 2010 *Quadrennial Defense Review* determined only one would be fielded with the second and third replaced by smaller units capable of responding more rapidly to multiple, simultaneous incidents.[33]

These smaller units, ten in total assigned to the National Guard (NG), are called Homeland Response Forces (HRFs). Each HRF, aligned to one of the ten Federal Emergency Management Agency (FEMA) regions, will consist of about 570 medical,

[31] U.S. Department of Defense, "Department of Defense Homeland Response Force (HRF) Fact Sheet," http://www.defense.gov/news/d20100603HRF.pdf, (accessed February 8, 2010).

[32] *The U.S. Northern Command Joint Task Force Civil Support Home Page*, http://www.northcom .mil /About/index.html#JTFCS (accessed February 8, 2011).

[33] *Quadrennial Defense Review*, 19.

search and extraction, decontamination, command and control and security personnel.[34] The HRF element is part of the larger DoD CBRNE Consequence Management enterprise that numbers about 18,000 personnel.[35] "HRFs will increase the focus on DoD Chemical, Biological, Radiological, Nuclear, and High explosive (CBRNE) Consequence Management Response forces on lifesaving objectives and increase operational flexibility while recognizing the primary role that the governors play in controlling the response to CBRNE incidents that occur in their states."[36]

Cyberspace Homeland Response Force

The HRF concept grew from the DoD's efforts to reshape the Reserve Component to better meet today's security challenges. The 2010 QDR states, "The challenges facing the United States today and in the future will require us to employ National Guard and Reserve forces as an operational reserve to fulfill requirements for which they are well-suited in the United States and overseas."[37] The HRF is an economical way to leverage the NG as an operational force to counter the very real threat of WMD to the homeland.

The restructured CBRNE Consequence Management Enterprise accounts for the lead role that Governors and other state officials play in controlling and responding to incidents that occur in their jurisdiction. According to Christine Wormuth, Principal Deputy Assistant Secretary of Defense for Homeland Defense and America's Security Affairs, "we felt it was important to recognize the political reality that nine times out of ten an event is going to be controlled at the state level by the governor, and as a result, we

[34] "DoD HRF Fact Sheet."
[35] Ibid.
[36] Ibid.
[37] *Quadrennial Defense Review*, 53.

really needed to rebalance our DoD forces to reflect that reality and be able to work in any number of those scenarios."[38]

Similarly, the DoD should leverage the Reserve Component to counter the very real cyberspace threat to the Nation's critical infrastructure. According to the 2011 *National Military Strategy*, "assured access to and freedom of maneuver within the global commons – shared areas of sea, air, and space – and globally connected domains such as cyberspace are being increasingly challenged by both state and non-state actors."[39] Furthermore, "should a larger-scale cyber intrusion or debilitating cyber attack occur, we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable."[40] Unlike the other warfighting domains, the cyberspace domain is man-made, overwhelmingly owned and operated by the private sector. To assure access to and freedom of maneuver in this globally connected domain, one of the "broad range of options" the DoD must consider is establishing a *dedicated* force to assist civil authorities in defending the Nation's critical digital infrastructure. Emulating the CBRNE model, the DoD could call this new capability the Cyberspace Homeland Response Force.

Critical infrastructure/key resource (CIKR) protection is foremost a local issue. Like all other national incident response scenarios, the local and state government is responsible for first response. Fundamentally, a man-made cyber incident is no different than the response to a natural disaster such as a hurricane, earthquake, or floods. The

[38] Christine Wormuth, Principle Deputy Assistant Secretary of Defense for Homeland Defense and America's Security, speaking at National Guard Bureau Domestic Operations Workshop, National Harbor, MD, March 23, 2010, http://www.army.mil/-news/2010/03/24/36269-dod-relooks-at-plans-for-guard-response-capabilities/ (accessed March 15, 2011).

[39] *National Military Strategy*, 3.

[40] Ibid.

NIPP mandates States to develop and implement statewide CIKR protection programs to include coordination of protective and emergency response activities, information sharing framework, and vulnerability assessments.

Similar to WMD-CSTs, state level Cyber Civil Support Teams, federally resourced, trained, and certified would operate under the command and control of the state Governor (Title 32, U.S. Code) to:

- Assist with implementing statewide CIKR protection programs
- Assess current and projected CIKR vulnerabilities and consequences
- Provide Defense Industrial Base (DIB) vulnerability assessments and when required assist with mitigation efforts
- Advise on effective response measures
- Provide network forensics and malware analysis capabilities
- Assist with appropriate requests for State and Federal support

Cyber Civil Support Teams would train, certify, and interact closely with USCYBERCOM and the NSA to leverage the vast federal experience and technical expertise at the state level similar in the way General Alexander envisions supporting geographic combatant commands:

> Billions and billions of dollars have gone into it [NSA]. Over the last 5 years we've had the privilege of having the joint functional component command net warfare and NSA together, so we could leverage that infrastructure and that talent. What I think this does for the U.S. Cyber Command is it puts our soldiers, sailors, airmen, and marines, the young folks that are coming in, with this experienced group for training, and when we deploy these folks forward to support regional combatant commands we have folks that know the best in the world that they can reach out [to]—they operate at the tactical operational level and can talk to the strategic level, *because in cyber space it's one network and we have to operate as one team* [emphasis added].[41]

[41] *Nomination of LTG Alexander*, 28.

Due to the interconnected, interdependent nature of cyberspace and DoD's increasing reliance on civilian infrastructure one can make the case that the tactical level operations of which Gen Alexander speaks apply equally to public and private sector digital infrastructures as they do to the DoD Global Information Grid.

Returning to the CBRNE Consequence Management Enterprise model, CBRNE Enhanced Response Force Packages (CERFPs) provide regionally based, FEMA aligned forces to provide specialized capabilities to support local, state, and federal authorities for response to CBRNE incidents.[42] CERFPs are task-organized units with combat support and service support mission essential elements (casualty search and extraction, medical triage, casualty decontamination, and civil engineering) designed to fill the six to seventy-two hour gap in capabilities between the first response and the Federal response following a CBRNE incident.

Loosely modeled after the CERFP concept, the DoD should consider establishing regional Cyber Civil Support Teams. These teams would be what the NIPP calls a Regional Organization, working to evaluate regional and cross-sector CIKR interdependencies. These units would recruit and develop individuals with deep expertise in specific CIKR sectors critical to national defense such as energy, transportation, and information technology communications. They would specialize in supervisory control and data acquisition (SCADA), industrial control systems, and cross-sector/system independencies, providing a level of expertise beyond that available in the state civil response teams.

[42] National Guard Bureau, *National Guard CBRNE Enhanced Response Force Package Management*, National Guard Regulation 500-4/ANGI 10-2504 (Arlington, VA: National Guard Bureau, October 16, 2009), 2.

The DoD must also consider expanding intelligence capabilities in the cyber DSCA arena. The DoD, through the Joint Reserve Intelligence Program (JRIP), provides equipment and facilities for geographically distributed Reserve Component forces to train and support DoD intelligence requirements. The facilities, called Joint Reserve Intelligence Centers (JRICs), are joint intelligence production and training activities located within military owned Sensitive Compartmented Information Facilities (SCIFs) to provide Reserve Component intelligence personnel access to the DoD intelligence community network enterprise. Primarily used to support DoD intelligence production, the JRIP also promotes fulltime use of facilities by non-DoD elements on a not-to-interfere basis.[43]

The DoD should consider establishing units at some or all of the twenty-eight JRICs throughout the country to provide more robust intelligence support to cyberspace operations. The ANG is establishing units to provide cyber ISR forensics, known as Digital Network Intelligence (DNI) and associate ISR units at National Security Agency Central Security Service centers to expand analysis and targeting capacity.[44] In partnership with DHS, the DoD should consider similar units to provide forensics and analysis capabilities for critical infrastructure.

Implementation Challenges

Recommendations are nothing more than good ideas without the resources to implement them. Establishing a cyber civil support force, or any new DoD program,

[43] U.S. Department of Defense, *Joint Reserve Intelligence Program (JRIP)*, Department of Defense Instruction 3305.07 (Washington, DC: U.S. Department of Defense, March 27, 2007), 3.

[44] Air National Guard, "ANG Flight Plan," January 29, 2010, https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1356090FB5E044080020E329A9/Files/editorial/ANG%20Flight%20Plan.pdf?channelPageId=s6925EC1356090FB5E044080020E329A9&programId=t6925EC2D2CE30FB5E044080020E329A9 (accessed August 5, 2010).

poses a significant challenge in today's constrained fiscal environment. However, given the significant economic and national security threat individual actors, terrorist organizations, and nation-states pose to United States critical infrastructure through cyberspace attack, it is a challenge the U.S. can ill-afford to ignore.

From a staffing perspective, the Reserve Component can realign existing force structure to mitigate personnel costs. As operations in Iraq and Afghanistan wind down, the DoD will address force sizing and force shaping to meet future defense needs. The Air Force is substantially reducing its fleet of older fourth-generation fighter aircraft and will not see a one-to-one replacement of F-35s. The limited production C-17 cargo fleet is not enough to modernize the existing mobility aircraft inventory. These realities will inevitably result in a reduction of flying missions in the Air Force Reserve and Air National Guard. Recent Secretary of Defense comments at West Point portend reductions in U.S. Army heavy combat capability. The Navy and Marines are also likely to see cuts in their combat systems. These major DoD force transformations should provide more than enough force structure to establish the required cyber civil support units.

The DoD can avoid major infrastructure costs by reutilizing existing facilities made available by mission transitions. Cyber civil support teams are a knowledge workforce requiring specialized network forensics and diagnostic equipment and access to Sensitive Compartmented Information Facilities (SCIFs), but such facilities and operations and maintenance expenditures are minimal compared to costs of the legacy aviation and heavy combat missions these units will be replacing.

Beyond funding, the presentation of forces could be problematic, in that the DoD will be providing standing forces for a homeland security DoD mission. USCYBERCOM or NORTHCOM would in essence be presenting cyber forces in a supporting role to DHS. The Services and Reserve Components most likely will not embrace the concept because it is a dedicated, homeland only mission. The Services much prefer dual use capabilities that can be used both stateside and in overseas contingency operations. Homeland security missions are particularly scrutinized because in this arena, the Department is tasked in a supporting role to DHS and other federal and state agencies. The service components already have a long list of unfunded requirements for their primary warfighting mission, let alone funding units solely dedicated to a secondary homeland security mission.

Likewise, the Reserve Component avoids homeland only missions because funding is tenuous at best and for relevance and advocacy considerations, the Reserve Component tends not to stray too far from their active duty brethren. For these reasons, DoD units dedicated to homeland security units are the exception rather than the rule.

Building a cyber civil support force will be difficult, but it is not insurmountable even in today's tight budget environment. On the contrary, one could view it as an imperative given the current environment. "There seems to be a general recognition and agreement that you can't have a strong defense on a weak economy."[45] An adversary bent on undermining or delaying U.S. military action could asymmetrically target an already troubled economy through widely distributed and sustained attacks against U.S. infrastructure.

[45] Arnold Punaro, "Reducing Overhead and Improving DoD's Business Operations," Defense Business Board Quarterly Meeting, July 22, 2010, http://www.govexec.com/pdfs/073010whats.pdf (accessed March 8, 2011).

More so than DSCA in the physical domains, an effective DSCA response in the complex, interdependent world of cyberspace demands a dedicated DoD force. The recommendations provided in this chapter offer an integrated solution for establishing and employing such a force. Based largely on the CBRNE civil support construct, they are very likely executable under existing authorities but further analysis is required beyond this research effort.

This Page Intentionally Blank

CHAPTER 6: CONCLUSION

Cybersecurity is clearly one of the most serious security, public safety, and economic challenges faced by the United States today. Attacks against the Nation's digital infrastructure including the power grid, transportation systems, and financial sector could lead to "physical damage and economic disruption on a massive scale."[1] Potential adversaries possess the technical skills to carry out debilitating cyber attacks and have demonstrated intent by penetrating U.S. critical infrastructure and introducing malicious software capable of disrupting or causing physical destruction.

The Y2K challenge offered an early glimpse of the vulnerabilities of the Nation's digital infrastructure in a globally connected and interdependent world. The successful cyber-attacks on Estonian and Georgian digital infrastructure demonstrated how cross-border belligerents using even unsophisticated techniques could hobble a nation with relative ease and almost guaranteed impunity. In the U.S., an ever-increasing number of penetrations, exploitations, and successful attacks of government and private sector networks, to include the Nation's power grids, underscore the far-reaching challenges and implications this new threat imposes on U.S. national security.

The U.S. has equal and probably better offensive cyber capabilities than any other nation in the world, yet this powerful tool has done little to deter to would be adversaries. Threats are more pervasive; adversaries are growing bolder and more sophisticated in their attack and exploitation techniques. The relative anonymity and low barriers to entry make cyberspace the domain of choice for asymmetric warfare against the United States.

[1] Lynn, "Remarks delivered at STRATCOM Cyber Symposium."

Within the domain, the interdependent nature of critical infrastructure presents an attractive strategic target affecting all instruments of national power. Critical infrastructure underpins the economy, enables military operations, and provides the primary medium for conveying information throughout society and diplomatic strategic communications with the rest of the world. As such, protecting the America's critical infrastructure, a vital strategic asset, requires a concerted national effort.

The Department of Homeland Security, lead agency for protecting the Nation's critical infrastructure, cannot alone shoulder the cybersecurity burden. The traditional distinctions between homeland and national security, particularly in the cyberspace domain, are increasingly disappearing, demanding strong cooperation and synchronized actions among homeland security, military, and law enforcement professionals to protect, defend, and respond against attacks on the Homeland.

As assessed against the key principles of response doctrine contained in the *National Response Framework*, the DoD is not optimally postured to support civil authorities effectively in protecting the Nation's digital against a major cyber attack.

For its part, the DoD must:

Take a more proactive, homeland defense approach to protecting the U.S. critical infrastructure against a cyber attack. The United States should view threats against the Nation's critical infrastructure through cyberspace in the same manner it would than any other attack in or through the physical land, air, and sea domains. The DoD can best support civil authorities by leveraging NSA's vast signals intelligence enterprise and USCYBERCOM's warfighting capabilities to: detect threats outside the homeland; deter and prevent adversaries by imposing costs and denying benefits; and if

necessary defeat by destroying adversary capabilities through kinetic or non-kinetic means.

Leverage the Reserve Component to defend U.S. critical infrastructure. The DoD has long relied on the Reserve Component to support civil authorities during times of crisis and domestic emergencies. Expanding this role to help protect against and respond to threats in the cyber domain is a much needed and natural fit. The DoD can better team with DHS to strengthen security and resilience at home against large-scale cyber attacks by leveraging the Reserve Component to help defend U.S. critical infrastructure. Reserve Component service members' civilian backgrounds provide specialized skill sets that may either not resident or difficult to retain in active duty force. The Reserve Component will provide the adaptable, technical adept workforce invested in response preparedness and engaged partnerships necessary for cyber DSCA mission success at the state and local level.

Consider applying the DoD Chemical, Biological, Radiological, Nuclear and high-yield Explosive (CBRNE) Consequence Management model to Cyber DSCA. Similar in the way the CBRNE enterprise provides an economical means to leverage the Reserve Component as an operational force to counter WMDs to the homeland, the DoD must consider establishing a dedicated force to assist civil authorities in defending the Nation's critical digital infrastructure.

Critical infrastructure/key resource (CIKR) protection is foremost a local issue. Like all other national incident response scenarios, the local and state government is responsible for first response. In order to rapidly assist in the response, the DoD should consider establishing Cyber Civil Support Teams, federally resourced, trained, and

certified that would operate under the command and control of the state Governor (Title 32, U.S. Code) to bridge the gap between federal and state authorities. Working in close coordination with USCYBERCOM and the NSA, these cyber civil support teams will leverage the vast federal experience and technical expertise to provide a much-needed defense in depth capability at the state and local level.

When asked last fall what keeps him up at night, Deputy Defense Secretary William J. Lynn III responded, "No. 1 is the cyber threat. If we don't maintain our capabilities to defend our networks in the face of an attack, the consequences for our military, and indeed for our whole national security, could be dire." [2] "Our networks" include not only the defense global information grid, but also the public and private sector digital infrastructure, the virtual interstate highway system that transports the Nation's business, commerce, and public safety information. It is only through a concerted national effort, including a more integrated, proactive DoD involvement at the federal, state, and local levels, that the U.S. will successfully stave off the dire consequences of a major cyber attack against the homeland. Research and analysis of the issue clearly indicates that DoD should dedicate select Reserve Component units as an operational homeland force to team with the federal, state, and local government authorities to protect America's digital infrastructure against pervasive and increasingly lethal cyber threats.

[2] John J. Kruzel, "Cybersecurity Seizes More Attention, Budget Dollars," February 4, 2010, http://www.defense.gov/news/newsarticle.aspx?id=57871 (accessed September 16, 2010).

BIBLIOGRAPHY

Air National Guard. “ANG Flight Plan.” January 29, 2010. https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1356090FB5E044080020E329A9/Files/editorial/ANG%20Flight%20Plan.pdf?channelPageId=s6925EC1356090FB5E044080020E329A9&programId=t6925EC2D2CE30FB5E044080020E329A9 (accessed August 5, 2010).

Bemer, R.W. “What’s the Date?” *Honeywell Computer Journal* 5, no. 4 (1971): 205-208.

Bush, George W. *The National Strategy to Secure Cyberspace*. Washington, DC: The White House, February 2003.

———. Homeland Security Presidential Directive 7. “Critical Infrastructure Identification, Prioritization, and Protection.” in *Public Papers of the Presidents of the United States: George W. Bush, Book 02, Presidential Documents – July 1 to December 31, 2003.* Washington, DC: Government Printing Office, December 17, 2003.

Center for Strategic and International Studies. “Securing Cyberspace for the 44th Presidency.” Washington, DC: Center for Strategic and International Studies, December 2008. http://csis.org /files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed August 3, 2010).

Clarke, Richard A. and Robert K. Knake. *Cyber War*. New York: Harper Collins Publishers, 2010.

Clausewitz, Carl von. *On War*. trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984) .

Dorobek, Christopher. “20 things in 20 years that changed government IT.” *Federal Computer Week*, January 8, 2007. http://fcw.com/Articles/2007/01/08/20-things-in-20-years-that-changed-government-IT.aspx?Page=1 (accessed December 18, 2010).

Evans, Karen and Franklin Reeder. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters, Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, November 2010.

Finn, Peter. “Cyber Assaults on Estonia Typify a New Battle Tactic.” *Washington Post*, 19 May 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122 .html (accessed January 3, 2011).

Gorman, Siobhan. “Electricity Grid in U.S. Penetrated By Spies.” *The Wall Street Journal*, April 8, 2009.

Habiger, Eugene E. *Cyberwarfare and Cyberterrorism: The Need For A New U.S. Strategic Approach.* Washington, DC: The Cyber Secure Institute, 2010.

Harris, Shane. "The Cyberwar Plan." *National Journal.* November 13, 2009, http://www.proquest.com/ (accessed March 6, 2011).

Hayden, Michael V. "Black Hat USA 2010: Cyber war: Are we at war? And if we are, how should we fight it?" *YouTube*. http://www.youtube.com/ watch?v =XXnIvBBASLI (accessed March 6, 2011).

Homeland Security Newswire. "Chertoff calls for cyber-deterrence doctrine." October 15, 2010. http://homelandsecuritynewswire.com/chertoff-calls-cyber-deterrence-doctrine (accessed March 15, 2011).

International Telecommunications Union. "The World in 2010: ICT Facts and Figures." http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf (accessed December 23, 2010).

Korns, Stephen W. and Kastenberg, Joshua E. "Georgia's Cyber Left Hook." *Parameters* 38, no. 4 (Winter 2008/2009): 60-77.

Kruzel, John J. "Cybersecurity Seizes More Attention, Budget Dollars." February 4, 2010. http://www.defense.gov/news/newsarticle.aspx?id=57871 (accessed September 16, 2010).

Kuehl, Dan. "From Cyberspace to Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, 24-42. Washington, DC: National Defense University Press and Potomac Books, 2009.

Kugler, Richard L. *Cyberpower and National Security.* Washington, DC: National Defense University Press and Potomac Books, 2009.

Landler, Mark and John Markhoff. "In Estonia, what may be the first war in cyberspace." *The New York Times*, 28 May, 2007. http://www.nytimes.com/2007 /05/28/ business/worldbusiness/28iht-cyberwar.4.5901141.html?pagewanted=2 (accessed January 3, 2011).

Lewis, James A. "Korean Cyber Attacks and Their Implications for Cyber Conflict." October 2009, http://csis.org/files/publication/091023_Korean_Cyber_Attacks _and_Their_Implications_for_Cyber_Conflict.pdf (accessed February 5, 2011).

Libicki, Martin J. *Cyberdeterrence and Cyberwar.* Washington, DC: RAND Corporation, 2009.

Lynn, William J. III. "Remarks delivered at STRATCOM Cyber Symposium." May 26, 2010. http://www.defense.gov/speeches/speech.aspx? speechid=1477 (accessed February 28, 2011).

———. “Remarks on Cyber at the RSA Conference.” February 15, 2011. http://www.defense.gov/speeches/speech.aspx?speechid=1535 (accessed February 18, 2011).

Markoff, John, David Sanger, and Thom Shanker, “In Digital Combat, U.S. Finds No Easy Deterrent.” *The New York Times*, November 13, 2009.

McKinley, Craig R. *Chief National Guard Bureau in Statement before the Senate Appropriations Committee on the Fiscal Year 2011 Guard and Reserve Budget.* Statement presented to the 111th Cong., 2nd sess. Washington, DC: The National Guard Bureau, March 24, 2010.

Mearsheimer, John J. *Conventional Deterrence.* Ithaca: Cornell University Press, 1983.

Miller, Jason. “Workforce is DoD’s Biggest Cyber Challenge.” September 24, 2010. http://www. federalnewsradio.com/?nid=35&sid=2061303 (accessed December, 4, 2010).

Moteff, John and Paul Parfomak. *Critical Infrastructure and Key Assets: Definition and Identification.* CRS Report for Congress. Washington, DC: Congressional Research Service, October 1, 2004.

Motter, Adilson E. and Ying-Cheng Lai. “Cascade-based Attacks on Complex Networks.” *Physical Review E* 66, no. 6 (20 December 2002). http://chaos1.la.asu. edu/~yclai/papers /PRE_02_ML_3.pdf (accessed January 24, 2010).

Murray, Jerome T. and Murray, Marilyn J. *Computers in Crisis*. New York: Petrocelli Books Incorporated, 1984.

Mussington, David. *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development*. Santa Monica, CA: RAND Corporation, 2002.

Nagl, John and Travis Sharp. “An Indispensable Force, Investing in America’s National Guard and Reserves.” Washington, DC: Center for a New American Security, 2010.

Nakashima Ellen. “Pentagon Cyber Unit Prompts Questions.” *The Washington Post*, June 13, 2009.

National Guard Bureau. “2012 National Guard Bureau Posture Statement.” http://www .ng.mil/ features/ngps/2012_ngps.pdf (accessed March 8, 2009).

———. *National Guard CBRNE Enhanced Response Force Package Management.* National Guard Regulation 500-4/ANGI 10-2504. Arlington, VA: National Guard Bureau, October 16, 2009.

———. “National Guard Critical Infrastructure Protection Assessment Teams (CIP) Teams.” July 17, 2008. http://www.ng.mil/features/ngps/2011/National %20Guard%20Critical%20 Infrastructure%20Protection%20Assessment.pdf (accessed August 15, 2010).

———. The National Guard Media Factsheets. “Emergency Management Assistance Compact.” http://www.ng.mil/media/factsheets/EMAC.pdf (accessed September 10, 2010).

———. The National Guard Media Factsheets. “Joint Force Headquarters-State.” http://www.ng.mil/media/factsheets/JFHQ-State.pdf 9 (accessed September 15, 2010).

———. “The National Guard’s Role in Homeland Defense, Critical Infrastructure Protection-Mission Assurance Assessments.” http://www.ng.mil/ features/HomelandDefense/cip-maa/index.html (accessed September 10, 2010).

The National Security Agency Information Assurance Web Page. http://www.nsa.gov/ia/ academic _outreach/nat_cae/index.shtml (accessed February 15, 2011).

NORAD & USHORTHCOM Plans, Policy & Strategy Directorate. “NORAD and USNORTHCOM Operation Plans Summary.” Briefing slides. http://www.scribd.com/doc/43717734/NORAD-NORTHCOM-Plans-Summary-Interagency (accessed March 6, 2011).

North American Aerospace Defense Command. “About NORAD.” http://www.norad .mil/ about/index.html (accessed February 8, 2011).

Obama, Barack H. *National Security Strategy*. Washington, DC: The White House, May 2010.

O’Hanlon, Michael E. *Budgeting for Hard Power: Defense and Security Spending Under Barack Obama*. Washington, DC: Brookings Institute Press, 2009.

Ottis, Rain, “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective.” Paper presented at the 8th European Conference on Information Warfare and Security, Lisbon, Portugal, 2009.

Parrish, Karen. “Lynn Urges Partnership Against Cyber Threat.” *American Forces Press Service*, February 15, 2011. http://www.defense.gov/News/NewsArticle .aspx?ID=62827 (accessed February 18, 2011).

Perera, David, “Cybersecurity Runs Deep in Fiscal 2012 Budget Request.” February 16, 2011. http://www.fiercegovernmentit.com/story/cybersecurity-runs-deep-fiscal-2012-budget-request/2011-02-16 (accessed March 15, 2011).

Punaro, Arnold. “Reducing Overhead and Improving DoD’s Business Operations.” Defense Business Board Quarterly Meeting, July 22, 2010. http://www.govexec .com/pdfs/073010whats.pdf (accessed March 8, 2011).

Rinaldi, Steven M., James P. Peerenboom, and Terrence K Kelly. “Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies.” *IEEE Control Systems Magazine*, December 2001.

Sevastopulo, Demetri. “Cyber Attacks on McCain and Obama teams ‘came from China.’” *Financial Times.* November 7, 2008. http://www.ft.com/cms/s/0/3b4001e2-ac6f-11dd-bf71-000077b07658 .html#axzz1JGiSxHAF (accessed April 2, 2011).

Tikk, Eneken, et al. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn, Estonia: Cooperative Cyber Defense Centre of Excellence, 2008.

U.S. Congress. Senate. Committee on Armed Services. *Nominations of VADM James A. Winnefeld, JR., to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Defense Command; and LTG Keith B. Alexander USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command*. 111th Cong., 2nd sess., April 15, 2010.

———. Committee on Armed Services. *Statement of Admiral James A. Winnefeld, Jr, Commander U.S. Northern Command and North American Aerospace Defense Command*, 112th Cong., 1st sess., April 5, 2011.

———. Committee on the Year 2000 Technology Problem. *Testimony by John S. Tritak, Director of Critical Infrastructure Assurance Office, before the Committee on the Year 2000 Technology Problem.*105th Cong., 2nd sess., July 29, 1999.

U.S. Department of Commerce. Economics and Statistics Administration, *Digital Economy 2000*. Washington, DC: U.S. Department of Commerce, June 2000.

———. Economics and Statistics Administration. *The Economics of Y2K and the Impact on the United States.* Washington, DC: U.S. Department of Commerce. November 17, 1999.

———. National Telecommunications and Information Administration. *Exploring the Digital Nation: Home Broadband Internet Adoption in the United States.* Washington, DC: U.S. Department of Commerce, November 2010.

———. “Quarterly Retail E-Commerce Sales 3rd Quarter 2010.” *U.S. Census Bureau News.* November 17, 2010, http://www.census.gov/retail/mrts /www/data /pdf/ec_current.pdf (accessed December 23, 2010).

U.S. Department of Defense. “Department of Defense Homeland Response Force (HRF) Fact Sheet.” http://www.defense.gov/news/d20100603HRF.pdf (accessed February 8, 2010).

———. *Annual Report to Congress, Military and Security Developments Involving the People's Republic of China*." Washington, DC: Office of the Secretary of Defense, 2010.

———. *DoD Policy and Responsibilities for Critical Infrastructure.* Department of Defense Directive 3020.40. Washington, DC: U.S. Department of Defense, January 14, 2010.

———. *Joint Reserve Intelligence Program (JRIP).* Department of Defense Instruction 3305.07. Washington, DC: U.S. Department of Defense, March 27, 2007.

———. *National Defense Strategy*. Washington, DC: U.S. Department of Defense, 2008.

———. *The National Military Strategy of the United States of America*. Washington, DC: U.S. Department of Defense, 2011.

———. *Quadrennial Defense Review Report*. Washington, DC: U.S. Department of Defense, February 2010.

———. United States Northern Command. "About USNORTHCOM." http://www.northcom.mil/about/index.html (accessed Oct 23, 2010).

———. U.S. Cyber Command Public Affairs. "U.S. Cyber Command Fact Sheet," http://www.stratcom.mil/factsheets/cc/ (accessed 15 August 2010).

U.S. Department of Homeland Security and U.S. Department of Defense. "Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity." Washington, DC, October 13, 2010.

U.S. Department of Homeland Security. *National Cyber Incident response Plan.* Washington, DC: U.S. Department of Homeland Security, September 2010.

———. *National Infrastructure Protection Plan*. Washington, DC: U.S. Government Printing Office, 2009.

———. *National Response Framework*. Washington, DC: U.S. Department of Homeland Security, January 2008.

———. Federal Emergency Management Agency. "Regional Operations." http://www.fema.gov/about/regions/index.shtm (accessed April 1, 2011).

———. Office of Cybersecurity and Communications. National Cyber Security Division, *CYBER STORM II Final Report.* Washington, DC: Department of Homeland Security, July 2009.

U.S. Government Accountability Office. *DoD Can Enhance Efforts to Identify Capabilities to Support Civil Authorities during Disasters*. Washington, DC: U.S. Government Accountability Office, March 2010.

U.S. Joint Chiefs of Staff. *Civil Support*. Joint Publication 3-28. Washington, DC: U.S. Joint Chiefs of Staff, 2007.

———. *Deterrence Operations Joint Operating Concept*. Washington, DC: U.S. Joint Chiefs of Staff, December 2006.

———. *DoD Dictionary of Military and Associated Terms.* Joint Publication 1-02. Washington, DC: U.S. Joint Chiefs of Staff, 2010.

———. *Homeland Defense*. Joint Publication 3-27. Washington, DC: U.S. Joint Chiefs of Staff, 2007.

———. *Homeland Defense and Civil Support Joint Operating Concept.* Washington, DC: U.S. Joint Chiefs of Staff, October 1, 2007.

———. *Joint Operation Planning*, Joint Publication 5-0. Washington, DC: U.S. Joint Chiefs of Staff, December 26, 2006.

The U.S. Northern Command Joint Task Force Civil Support Home Page. http://www. northcom .mil /About/index.html#JTFCS (accessed February 8, 2011).

U.S. Secretary of Defense Robert Gates. "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations." Memorandum for Secretaries of the Military Departments. Washington, DC, June 23, 2009.

Vargas, Jose A. "Obama Raised Half a Billion Online." *The Washington Post.* November 20, 2008. http://voices.washingtonpost.com/44/2008/11/20/obama_raised_half_ a_billion_on.html (accessed April 2, 2011).

Welch, Jack. http://en.thinkexist.com/quotes/Jack_Welch/ (accessed March 14, 2011).

The White House. "Remarks by the President on Securing Our Nation's Cyber Infrastructure." May 29, 2009. http://www.whitehouse.gov/briefing-room/speeches-and-remarks (accessed August 15, 2010).

———. Presidential Decision Directive 63. "Critical Infrastructure Protection." Washington, DC: The White House, May 22, 1998.

———. The President's Council on Year 200 Conversion. *The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion* by John A. Koskin. Washington, DC: The White House, March 29, 2000.

———. *Unified Command Plan 2011*.Washington, DC: The White House, April 6, 2011.

Wormuth, Christine. Principal Deputy Assistant Secretary of Defense for Homeland Defense and America's Security. Speaking at National Guard Bureau Domestic Operations Workshop, National Harbor, MD, March 23, 2010. http://www.army.mil/-news/2010/03/24/36269-dod-relooks-at-plans-for-guard-response-capabilities/ (accessed March 15, 2011).

VITA

Lieutenant Colonel Kevin M. Donovan is a senior service school student in the Joint Advanced Warfighting School at the Joint Forces Staff College in Norfolk, Virginia. He is a 1988 graduate of Clarkson University with a Bachelor of Science degree in Electrical Engineering. After commissioning through the Reserve Officer Training Corps, he entered the United States Air Force (USAF) as an Air Battle Manager. His service includes assignments in USAF and NATO Airborne Warning and Control System (AWACS) squadrons and ground based air control squadrons. In 1999, he joined the Maine Air National Guard and served as Commander of the 243rd Engineering Installation Squadron. Most recently, he served as the Chief, Cyberspace Policy and Resources Division in the Communications and Information Directorate (A6) at the National Guard Bureau, Arlington, VA. He holds a Master of Science degree in Management Information Systems from Bowie State University and is a graduate of the Air Force Squadron Officer School and the Air Command and Staff College.