# NATIONAL GUARD FORCES IN THE CYBER DOMAIN

A Monograph

by

MAJ Murry McCullouch

United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2015-001

| | |
|---|---|
| **REPORT DOCUMENTATION PAGE** | *Form Approved*<br>*OMB No. 0704-0188* |

| | | |
|---|---|---|
| **1. REPORT DATE** *(DD-MM-YYYY)*<br>16-05-2014 | **2. REPORT TYPE**<br>Master’s Thesis | **3. DATES COVERED** *(From - To)*<br>JUN 2014 – MAY 2015 |

| | |
|---|---|
| **4. TITLE AND SUBTITLE**<br>National Guard Forces in the Cyber Domain | **5a. CONTRACT NUMBER** |
| | **5b. GRANT NUMBER** |
| | **5c. PROGRAM ELEMENT NUMBER** |
| **6. AUTHOR(S)**<br>MAJ Brent McCullouch | **5d. PROJECT NUMBER** |
| | **5e. TASK NUMBER** |
| | **5f. WORK UNIT NUMBER** |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**<br>U.S. Army Command and General Staff College<br>ATTN: ATZL-SWD-GD<br>Fort Leavenworth, KS 66027-2301 | **8. PERFORMING ORG REPORT NUMBER** |
| **9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**<br>Advanced Operational Arts Studies Fellowship, Advanced Military Studies Program. | **10. SPONSOR/MONITOR’S ACRONYM(S)** |
| | **11. SPONSOR/MONITOR’S REPORT NUMBER(S)** |

**12. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for Public Release; Distribution is Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The National Guard has played a vital role in the defense of this nation’s threats since the country’s inception. Over 200 years ago, the militia helped George Washington strike a blow against the British after they forced him from New York and pursued the Continental Army across New Jersey. Today the nation faces the new challenge of how to best defend itself against cyber attacks. Just as the militia, forbearers to the National Guard, enabled George Washington’s attack against Trenton, the National Guard stands ready today to work with Department of Defense (DoD) to counter the growing cyber threat. Given the challenges facing the US to develop a comprehensive cyber strategy, the question is why and how should DoD integrate the National Guard into the national cyber forces. DoD should integrate the National Guard into the national cyber forces because of the cyber threats and the need for assistance at the state level. In addition, existing Guard cyber capabilities, Presidential, Congressional, and Department of Homeland Security mandates to protect critical infrastructure, and US Army doctrine points to full integration as the best path to seize, retain, and exploit the initiative to gain and maintain a position of relative advantage.

**15. SUBJECT TERMS**
National Guard; Reserve Component; cyber domain; Unified land operations; cyber threats; cyber mission forces; Cyber Protection Team; Computer Network Defense Team; Critical Infrastructure; Industrial Control System

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON**<br>MAJ Murry McCullouch |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | **19b. PHONE NUMBER** *(include area code)* |
| (U) | (U) | (U) | (U) | 47 | |

**Standard Form 298 (Rev. 8-98)**
**Prescribed by ANSI Std. Z39.18**

Monograph Approval Page

Name of Candidate: MAJ Murry B. McCullouch

Monograph Title: National Guard Forces in the Cyber Domain

Approved by:

__________________________________, Monograph Director
Barry M. Stentiford, PhD

__________________________________, Seminar Leader
Robert J. Hallett, LtCol

___________________________________, Director, School of Advanced Military Studies
Henry A. Arnold III, COL, IN

Accepted this 22nd day of May 2015 by:

___________________________________, Director, Graduate Degree Programs
Robert F. Baumann, PhD

The opinions and conclusions expressed herein are those of the student author, and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

## Abstract

National Guard Forces in the Cyber Domain, by MAJ Murry McCullouch, 47 pages.

The National Guard has played a vital role in the defense of this nation's threats since the country's inception. Over 200 years ago, the militia helped George Washington strike a blow against the British after they forced him from New York and pursued the Continental Army across New Jersey. Today the nation faces the new challenge of how to best defend itself against cyber attacks. Just as the militia, forbearers to the National Guard, enabled George Washington's attack against Trenton, the National Guard stands ready today to work with Department of Defense (DoD) to counter the growing cyber threat. Given the challenges facing the United States to develop a comprehensive cyber strategy, the question is why and how should DoD integrate the National Guard into the national cyber forces. DoD should integrate the National Guard into the national cyber forces because of the cyber threats and the need for assistance at the state level. In addition, existing Guard cyber capabilities, Presidential, Congressional, and Department of Homeland Security mandates to protect critical infrastructure, and US Army doctrine points to full integration as the best path to seize, retain, and exploit the initiative to gain and maintain a position of relative advantage.

## Contents

## Acronyms

| | |
|---|---|
| ARCYBER | Army Cyber Command |
| ARNG | Army National Guard |
| ANG | Air National Guard |
| C/TAA | Coordinate, Train, Advise, and Assist |
| CMF | Cyber Mission Force |
| CND-T | Computer Network Defense Teams |
| CPT | Cyber Protection Team |
| DHS | Department of Homeland Security |
| DoD | Department of Defense |
| DoDIN | Department of Defense Information Networks |
| DSCA | Defense Support of Civil Authorities |
| HLD | Homeland Defense |
| JFH | Joint Force Headquarters |
| JIE | Joint Information Environment |
| NDAA | National Defense Authorization Act |
| NDS | National Defense Strategy |
| NCIRP | National Cyber Incident Response Plan |
| NIPP | National Infrastructure Protection Plan |
| NMS | National Military Strategy |
| NGB | National Guard Bureau |
| PPD | Presidential Policy Directive |
| QDR | Quadrennial Defense Review |
| SAD | State Active Duty |
| SLTT | State, Local, Tribal, and Territorial |

| | |
|---|---|
| TAG | The Adjutant General |
| USCYBERCOM | United States Cyber Command |

## Figures

## Introduction

> The reserve component has a role in the defense of the United States against cyber threats and consideration should be given to how the reserve component might be integrated into a comprehensive national approach for cyber defense.
>
> —National Defense Authorization Act of 2015[1]

The National Guard has played a vital role in the defense of this nation's threats since the country's inception. Over 200 years ago, the militia helped George Washington strike a blow against the British after they forced him from New York and pursued the Continental Army across New Jersey. Today the nation faces a new challenge of how to defend itself against cyber attacks. Just as the militia, forbearers to the National Guard, enabled George Washington's attack against Trenton, the National Guard stands ready today to work with Department of Defense (DoD) to counter the cyber threat. Given the challenges facing the United States to develop a comprehensive cyber strategy, the question is why and how should DoD integrate the National Guard into the national cyber forces. Currently, DoD has defined a limited role for National Guard cyber forces. DoD should integrate the National Guard into the national cyber forces because of the cyber threats and the need for assistance at the state level. In addition, existing Guard cyber capabilities, Presidential, Congressional, and Department of Homeland Security mandates to protect critical infrastructure, and US Army doctrine points to full integration as the best path to seize, retain, and exploit the initiative to gain and maintain a position of relative advantage.

As one of the primary partners in the defense against cyber threats, DoD faces capable cyber enemies who possess the tools to exploit, destroy, and degrade US information networks and key systems controlling critical infrastructure. In the cyber domain, the enemy can be a

[1] National Defense Authorization Act for Fiscal Year 2015, Public Law 113-29, 113th Cong., 2nd sess. (December 19, 2014), 356.

nation state, hactivist, terrorist group, or a disgruntled insider. The enemy does not limit itself to one tactic when it launches an attack. This week malicious actors might conduct cyber espionage on a major US bank, but next week they could plant malicious software in the control system of critical infrastructure that regulates the distribution of electricity across the east coast. The number of potential cyber foes and their proven capabilities demands an all-inclusive approach to building a total force team. In the same way that the federal government incorporates DoD, Department of Homeland Security (DHS), and other federal agencies to confront cyberspace threats, DoD must utilize all available resources to meet the challenge.

A home or business computer user does not buy a computer and connect to the internet without taking precautions. Most users understand the threats and design a layered defense to protect their computer and information. This defense could include installing anti-virus software and setting passwords for the computer, router, and modem. Users also practice good security by not downloading files from unknown sources or clicking on hyperlinks included in spam email. Doing only one of these things would leave the computer vulnerable, but all together they create a strong defense against unauthorized use or viruses. In a similar manner, DoD needs to take a multi-layered approach when confronting threats in the cyber domain. The National Guard is one of those critical resources.

Cyber Soldiers within the National Guard have attended the required schools as their active duty counterparts, have participated in many of the same exercises, and have developed innovative capabilities to assist states in their response to growing cyber threats. Even though the National Guard currently fulfills a limited role in the current cyber mission force construct, Guard leadership has developed robust cyber capabilities from its Army and Air National Guard cyber Soldiers and Airmen. Many leaders such as Major General William Reddel, New Hampshire Adjutant General, saw the threat, realized the Guard could help when an attacks occurs, and began lobbying for a more defined role for Guard cyber forces. Senator Kirsten Gillibrand, D-

NY, also recognized the Guard's unique capabilities that give it the ability to serve through its dual status authorities, both Title 10 and Title 32, to work with DoD, but also with community partners in the state to help secure cyber networks.[2]

The current dynamics in the cyber domain point to the need for designing a total force concept that results in an effective strategy to combat the emerging cyber threat. Cyber actors have become proficient at penetrating networks and exploiting them for gain. Sometimes the penetration is for financial purposes such as the 2007 hack on 7-Eleven Citibank ATM machines, which resulted in a two million dollar loss over a two-week period.[3] Other times it is for political purposes as seen when extremist groups such as the Syrian Electronic Army hack into web sites spreading their ideology. The more dangerous possibility is a cyber actor's penetration of a system that controls critical parts of a state's infrastructure found in the emergency services, water, or power sectors. Cyber actors have shown they possess the skill sets to conduct any variation on these types of attacks.

As governors observed the increased threats, they realized the need to increase their cyber capabilities to protect their state from a range of threats to include a network penetration of a state agency to an attack that damages critical infrastructure.[4] Presidential policy and DHS recognized the same threats and published guidance calling for increased cooperation between federal, state,

[2] Ron Jensen, "Cyber Sense," *National Guard* 67, no. 6, June 2013, 21, accessed February 13, 2015, http://nationalguardmagazine.com/article/Cyber_Sense/1425297/162672/article.html.

[3] Kevin Poulsen, "7-Eleven Hack From Russia Led to ATM Looting in New York," *Wired.com*, December 21, 2009, accessed December 11, 2014, http://www.wired.com/2009/12/seven-eleven/.

[4] Laura Saporito, "The Cybersecurity Workforce: State's Needs and Opportunities," (Washington, DC: National Governors Association Center for Best Practices, 2014), 1: accessed November 24, 2014, http://www.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-hsps-publications/col2-content/main-content-list/the-cybersecurity-workforce-stat.html.

local, and territorial entities. To assist with this mission, Governors began to reach out to the National Guard for help in the cyber domain in a similar way they do when threatened by a natural disaster such as flood, tornado, or hurricane. State and local leaders already view the Guard as a reliable partner capable of solving complex problems. Whether the Deepwater Horizon oil spill of 2010 or a possible earthquake along the New Madrid fault, governors expect Guard members to apply their training and expertise to develop options and help solve difficult problems. Through the National Governors Association, governors lobbied DoD to designate a specific role for the National Guard in cyber missions. The US Congress has also pressed DoD to define the role of Guard forces in this cyber environment.

When DoD formed United States Cyber Command (USCYBERCOM) and began creating teams to respond to the growing cyber threat, it did not include a specific role for the National Guard. Even without a designated role, Guard leadership looked for ways to expand and integrate their Army and Air cybersecurity capabilities within their states. In the Army National Guard (ARNG), states recruited information technology experts from the civilian sector to fill the slots on recently created computer network defense teams (CND-Ts). Within the Air National Guard (ANG), specialized squadrons were created to function in a variety of roles to include partnering with the National Security Agency (NSA) conducting analysis of computer and network intrusions as well as penetration testing of state agency networks.[5] Soldiers perform these roles in a variety of duty statuses to include Title 10, Title 32, and State Active Duty.

Another reason that DoD should fully incorporate the Guard into the future cyber mission force structure is because it is what US Army doctrine outlines as the best strategy. Current

[5] Colin Wood, "How the National Guard Is Protecting Cybersecurity," *Governing*, March 3, 2014, accessed November 11, 2014, http://www.governing.com/topics/public-justice-safety/how-the-national-guard-Is-.html.

capstone doctrine in *ADP 3-0, Unified Land Operations (ULO)*, defines the role of unified land operations as:

> *Unified land operations* describes how the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution.[6]

ULO recognizes the three-dimensional nature of modern warfare and the need to conduct a mixture of offensive, defensive, and stability operations (or defense support of civilian authorities) simultaneously.[7] While DoD could place Guard forces in a Title 10 status for offensive operations, it can immediately utilize them in their Title 32 status for defensive cyber operations. Using the Guard enables DoD to conduct cyber operations that are characterized by flexibility, integration, depth, and synchronization. As a part of the total force, the Guard provides a better way to pursue the strategic objective of defending critical infrastructure, through the arrangement of tactical actions for military and civilian networks, in time, space, and purpose.[8]

Integrating the National Guard into the national cyber forces is another step that creates a strong-layered defense for the country. The evolving cyber threat, need for additional resources, current Guard capabilities, and doctrinal guidance point towards the necessity of creating a more robust partnership between DoD and the National Guard. Similar to the Soviet bomber threat in the 1950s, the nation faces an external threat that exceeds the capabilities of the active

[6] Army Doctrine Publication (ADP) 3-0, *Unified Land Operations* (Washington, DC: Government Printing Office, 2011), 7.

[7] Ibid.

[8] US Department of Defense, *Army Directive 2012-08 (Army Total Force Policy)* (Washington, DC, 2012), 1. The term total force refers to the integration of the Active Army, Army National Guard, and the US Army Reserve. The Total Force is part of the Army's strategy and planning to fulfill national and military needs.

component.[9] These and other threats throughout the history of the country point to the need for a collaborative effort to secure the homeland. The Guard stands ready and capable to contribute to this fight.

## Literature Review

The following literature review examines the evolution of cyber attacks and the critical vulnerabilities states face in confronting attacks through the cyber domain. It also looks at policy guidance from the President, DHS, and DoD. The policy guidance confirms the seriousness that advanced cyber actors pose to US businesses and critical infrastructure. The policies uniformly call for cooperation between federal and state partners as well as military and civilian agencies to counter these emerging threats. DHS recognizes the local nature of the threat and the imperative for states to develop effective strategies. DHS also concludes that states should incorporate existing National Guard Cyber forces into these plans. Even though DoD comes to similar conclusions about the threat, it has yet to publish a strategy that incorporates the Guard into its overall cyber efforts.

Numerous books and articles examine the evolution of cyber attacks as well as the potential impacts of these attacks. John Arquilla and David Ronfeldt's *In Athena's Camp* is a good representation of thoughts in the 1990s on cyber attacks and the potential damage from future attacks. They believed that cyberwar in the 21st century would be similar to the Nazi Germany's blitzkrieg operations.[10] They argued that as societies relied more on computer technologies and networked systems with their numerous vulnerabilities, there was the potential

[9] Michael D. Doubler and John W. Listman, *The National Guard: An Illustrated History of America's Citizen-Soldiers* (Washington, DC: Brassey's, 2003), 244.

[10] Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012), 13.

for cyber attacks to cause catastrophic damages.[11] Other analysts viewed the problem differently and argued that while cyber attacks could be disruptive, they would not be capable of producing widespread damage or political coercion to another nation. Martin Libicki's *In Conquest of Cyberspace* and Dr. Collin Gray in *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* represented the views of this camp of thought.[12]

Around 2006, cyber attacks evolved from mere disruptive attacks that destroyed data on computers or compromised computer operating systems, to attacks that had the potential to cause serious damage.[13] Derek Reveron in *Cyberspace* highlighted the fact that even though countries and cyber actors have not used cyber to cause significant damage or political coercion, they did begin using cyber attacks to accompany traditional warfare with limited impacts.[14] Richard Clark in *Cyber War* discussed these more advanced attacks to include the Russian attacks on Estonia and Georgia and the impact they had on shaping government policies.[15] Both Reveron and Clark trace the increasing sophistication of these attacks as nation states began using cyber as a weapon against an increasingly broader set of targets. Herbert Lin in *Cyberspace* looks at the new sets of

[11] Ibid.

[12] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 41; Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 13.

[13] Disruptive attacks include the LoveBug and Conficker worm. Individual hackers created the LoveBug worm in 2000, which infected over 45 million computer users. It was distributed by email, with the purpose of destroying data on computers. Conficker was a computer worm in 2009 that targeted Microsoft Windows Operating system and infected over 1.7 million computers.

[14] Reveron, 13.

[15] Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010), 112.

targets and discusses the vulnerability of systems that control and protect critical infrastructure within the United States.[16]

In the 1990s, the US government began developing a distinct national security policy to respond to threats in cyberspace. This information is in Presidential Directives, DoD Directives, and DHS Directives. President Clinton's *Presidential Decision Directive 63* in 1998 was the first significant policy that addressed the seriousness of the cyber threat to the country.[17] It looked at the cyber and physical infrastructure vulnerabilities of the Federal Government.[18] President George W. Bush issued *The National Strategy to Secure Cyberspace* in February 2003. It outlined the strategic objectives of preventing attacks against critical infrastructure, reducing vulnerabilities, and minimizing damage and recover times from cyber attacks.[19] President Obama issued further cyber guidance through *Presidential Policy Directive 20 (PPD)* and *Executive Order 13636, "Improving Critical Infrastructure Cyber Security,"* which outlined the need to enhance the resiliency and security of the nation's critical infrastructure.

With the passage of the *Homeland Security Act of 2002,* Congress designated DHS as the cybersecurity lead, with DoD and DoJ as supporting members.[20] As the lead agency for domestic incident management and cyber response, DHS released numerous publications that

[16] Reveron, 43.

[17] William J. Clinton, Presidential Decision Directive 63, "Critical Infrastructure Protection," *Federal Register* 63, no. 150 (August 5, 1998): 41804.

[18] William J. Clinton, "Fact Sheet: Presidential Decisional Directive 63, "Critical Infrastructure Protection," (May 22, 1998), 1.

[19] US Department of Homeland Security, *National Strategy to Secure Cyberspace* (Washington, DC, February 13, 2003), viii.

[20] Homeland Security Act of 2002, Public Law 107-296, US Statutes at Large 116 (2002); 2163-64, codified at US Code 6 (2002), §§ 101 et seq.

provided strategic guidance for federal, state, and local authorities. In the *2010 National Cyber Incident Response Plan* (NCIRP), DHS recognized the National Guard was in "in a unique position to assist in information sharing, situation awareness, secure communications, and incident response" for cyber incidents.[21] The *2013 National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience* (NIPP) highlighted the need for federal partnerships with multiple organizations to manage the risks from cyber threats and hazards.[22]

DoD defined its cyber policy goals and priorities primarily through *National Defense Strategy* and the *Quadrennial Defense Review*. The following documents outline DoD's view of cyber and potential strategies for the active component: *2005 National Defense Strategy* (NDS), *2008 NDS, 2010 Quadrennial Defense Review* (QDR), *2011 DoD Strategy for Operating in Cyberspace, 2012 NDS* as defined in *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, and the *2014 QDR.* The *2011 DoD Strategy for Operating in Cyberspace* is the only document that specifically mentioned the National Guard. It states that developing National Guard and Reserve capabilities could be a paradigm shift that builds greater capacity, expertise, and flexibility.[23] There is no other mention in these strategic guidance documents on potential roles for the National Guard or specific recommendations on how they will integrate the Guard into the total force.

[21] US Department of Homeland Security, *National Cyber Incident and Response Plan* (Washington DC, September 2001), H-1.

[22] The 2013 NIPP includes the following entities when describing the community involved in managing risks to critical infrastructure: Owners and operators; Federal, State, local, tribal, and territorial governments; regional entities; non-profit organizations; and academia.

[23] US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC, July 2011), 11.

In an effort to strengthen the nation's efforts to protect the homeland from a cyber attack on critical infrastructure, Congress passed *The National Cybersecurity and Critical Infrastructure Protection Act of 2013* (NCCIP). Members of Congress also proposed the *Cyber Warrior Act of 2013* to increase the capability of governors to respond to cyber attacks through use of the National Guard. Due to DoD's lack of guidance to the National Guard concerning cyber missions or specified roles, Congress tasked DoD in the *2014 National Defense Authorization Act* (NDAA) to examine how the Guard could best be incorporated into the overall DoD cyber force.[24] The Council of Governors included a letter to DoD in conjunction with the section 933 request, that echoed the interest of Congress to ensure the National Guard is used to support "both state and federal cyber mission requirements."[25]

Within the National Guard, the *2013 Concept of Operation for Computer Network Defense Teams* provides guidance on manning, roles, and responsibilities for Guard cyber forces. In the absence of direct DoD guidance, the National Guard Bureau developed this product for the computer network defense teams (CND-Ts) in the 54 states, territories, and the District of Columbia.[26] Most literature concerning current National Guard cyber initiatives is located within

[24] National Defense Authorization Act for Fiscal Year 2014, Public Law 113-66, 113th Cong., 1st sess. (December 26, 2013), 396.

[25] "Cyber Letter from Council of Governors," Terry E. Branstad and Martin O'Malley to Deputy Secretary of Defense, August 15, 2014. *Executive Order 13528* established the Council of Governors, to strengthen the partnership between the federal government and state governments to protect the Nation against all types of hazards. The bipartisan Council is composed of ten state governors selected by the President to review matters involving the National Guard, homeland defense, and civil support activities.

[26] US Department of Defense, *Department of Defense Directive 5105.77: National Guard Bureau* (Washington, DC, 2008), 1. Future references to the states, US Virgin Islands, Guam, Puerto Rico, and the District of Columbia will be collectively referred to as "states." NGB is the focal point at the strategic level for National Guard matters not under the authority of the Secretaries of the Army and Air Force.

third-party published documents. The magazine, *National Guard*, highlighted numerous areas where Guard units are involved in cyber operations beyond the designated CND-Ts.[27] The bi-partisan National Governors Association has identified the Guard as a key resource for governors and has published numerous papers through its Center for Best Practices to include: *Call to Action*, *State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure,* and *The Cybersecurity Workforce: States' Needs and Opportunities.*[28]

## Part 1

## Evolving Cyber Attacks

Governors have grown increasingly concerned about the different cyber challenges facing them. They realize the need to develop strategies to respond and counter the growing number of attacks both aimed at the business sector and against critical infrastructure located within their states. While cyber criminal attacks against businesses have increased, the potential for attacks against critical infrastructure has also risen steadily. The attack against the South Carolina Department of Internal Revenue in 2012 was a wake-up call for states that did not think they needed to spend funds and worry unnecessarily about cyber attacks.

It is helpful to breakdown the types of cyber threats into broad categories in order to better understand the capabilities of each threat group. Steven Bucci, current Director of the

[27] William Matthews, "Cyber Uncertainty," *National Guard* 68, no. 7 (July 2014): 25, accessed September 30, 2014, https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/1552463797?accountid=28992. *National Guard* is the official publication of the National Guard Association of the United States and has been in print since 1947. It features articles about legislation and developments that affect the National Guard.

[28] Thomas MacLellan, *Act and Adjust: A Call to Action for Governors for Cybersecurity*, report (Washington, DC: National Governors Association Center for Best Practices, 2013), 6; Andrew Kambour, *Enhancing the Cybersecurity of Energy Systems and Infrastructure*, report (Washington, DC: National Governors Association Center for Best Practices, 2014), 1; Saporito, 1.

Davis Institute for National Security and Foreign Policy at the Heritage Foundation, presents a useful spectrum of threats that moves from low-level threats to high-level threats.[29] Each group has its own motivations and the ability to inflict a certain amount of damage. At the low end of the spectrum, individual hackers, small criminal enterprises, and disgruntled insiders can inflict limited damage to individuals, but are not viewed as a significant systemic threat.[30] Medium level threats include terrorist use of internet, cyber espionage, and organized crime. Each of these groups can have a "detrimental effect on a person, a business, a government, or a region."[31] These types of attacks define the majority of cyber threats today. The high-level systemic threats involve the full power of nation states.[32] Bucci also believes that some non-state entities such as terrorist and organized criminal organizations are moving towards the high-level threat portion of the spectrum. Examples of threats from the high-end of the spectrum include full-scale nation-state cyber attacks like the Russian cyber assaults on Estonia in 2007 and cyber support to the kinetic attack on Georgia in 2008.[33]

In the last decade, cyber medium-level threats have become more successful in attacking business interests. According to Symantec Corporation, there was a sixty-two percent  increase in cyber breaches that resulted in loss of personal data between 2012 and 2013.[34] 2013 saw a 700

[29] Reveron, 58.

[30] Ibid., 58.

[31] Ibid., 59.

[32] Ibid.

[33] Ibid., 60.

[34] "Symantec Corporation Internet Security Threat Report 2014," Symantec Security Response Publications, April 2014, accessed December 1, 2014, http://www.symantec.com/security_response/publications/threatreport.jsp.

percent increase in breaches that resulted in at least ten million identities being exposed from a total of one in 2012 to eight the following year. [35] From US financial institutions to retail chains, cyber criminals improved their ability to get past the organization's security systems to steal information. Attacks against the retailers Target in 2013 and Home Depot in 2014 are good examples of these types of attacks. [36] During these, hackers used various tactics to infiltrate the company's network. They implanted malicious software, which gave them back-door access to primary systems to remotely steal information. [37] In addition to dealing with the theft of information or money, companies incur ongoing costs that range from reissuing debit cards to providing credit monitoring to affected customers. In other cases of cyber crime, hackers have targeted financial institutions to include banks and a stock exchange.[38] As the internet has grown from sixteen million to over 2.9 billion users since 1995, more individuals and countries have conducted attacks through the cyber domain. [39]

[35] Ibid.

[36] "The Home Depot Reports Findings in Payment Data Breach Investigation," Home Depot Media Center, November 6, 2014, accessed December 2, 2014, https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf. Cyber criminal stole credit card information of fifty-six million shoppers throughout the US and Canada

[37] Riley Walters, "Cyber Attacks on U.S. Companies in 2014," The Heritage Foundation, October 27, 2014, accessed December 02, 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014#_ftn22. In the Target data breach, cyber criminals stole over seventy million customers' credit and debit card information.

[38] Emily Glazer, "J.P. Morgan's Cyber Attack: How The Bank Responded," MoneyBeat RSS, October 3, 2014, accessed December 02, 2014, http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/. In 2014 attack on J.P. Morgan, hackers gained access to over ninety servers which resulted in the compromise of contact information for over seventy-six million households and seven million small businesses.

[39] Introduction to Cyberthreat Analysis Course: Student Guide. Assymetric Warfare Branch, Joint Military Intelligence Training Center (DIA Headquarters: Washington, DC, 2013), 2-2.

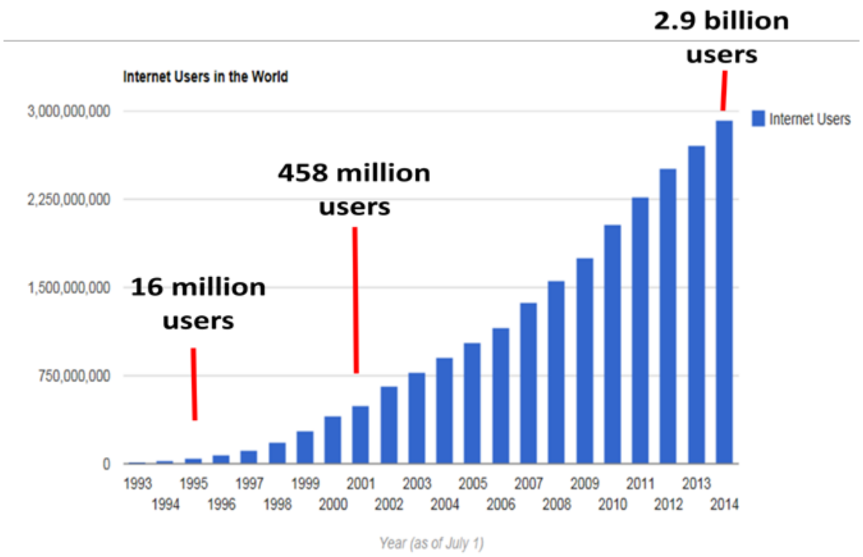

Figure 1. Internet Users in the World

*Source:* Data adapted from "Internet Users," Number of (2014), December 4, 2014, accessed December 04, 2014, http://www.internetlivestats.com/internet-users/#trend.

Cyber breaches are not limited to large US corporations and financial institutions. Numerous state agencies have also been the target of similar attacks. In 2012, a likely Russian hacker sent malware in an email searching for a username and password to the South Carolina's Department of Internal Revenue Service. When the unsuspecting employee clicked on the email, the hacker gained access to the user's administrative rights to access the department's systems and databases. Ultimately, the hacker stole 3.3 million unencrypted bank account numbers and 3.8 million tax returns containing social security numbers.[40] The attack went unnoticed for a month. No information exists on the costs to individuals whose information was stolen, but South

[40] Mathew J. Schwartz, "How South Carolina Failed to Spot Hack Attack," *Information Week*, November 26, 2012, accessed November 08, 2014, http://www.darkreading.com/attacks-and-breaches/how-south-carolina-failed-to-spot-hack-attack/d/d-id/1107515.

Carolina has paid $20 million in response to the attack. [41] In a similar case in 2012, a hacker stole information from 780,000 adults and children from the Utah Department of Health. Included in this information were 280,000 Social Security numbers.[42] Taken together, these attacks show how vulnerable many of the systems are that the US public relies on for daily activities.

As cyber crime has risen, so has cyber espionage. Cyber espionage involves stealing intellectual and technological information that provides some type of competitive advantage to the person or country committing the act. Unlike cyber crime where individual hackers are typically the culprits, nation states make up the bulk of attackers in cyber espionage. Stealing information reduces their timelines to create new technologies and allows them to maintain parity with other nations without the investment in their own research and development programs. In 2013, the Mandiant Corporation published a report highlighting China's strategy in targeting over 20 different industries in 141 countries beginning in 2006.[43]

Prior to the revelations about the Chinese cyber espionage, it became evident that attacks were not limited to stealing money or information. Nation states were beginning to leverage cyber as a potential weapon in the more traditional sense. In 2007, Russia actors with likely government support, attacked Estonia with extensive Distributed Denial of Service (DDOS) attacks.[44] These attacks occurred due to a disagreement about the Estonian relocation of a Soviet-era grave

[41] Saporito, 3. These costs include the breach investigation, mailing notifications of the breach to taxpayers, encrypting passwords at the department of revenue, and contracting to provide credit monitoring for a year to individuals who had their personally identifiable information exposed.

[42] Howard Anderson, "Utah Hack Attack: Lessons Learned," HealthcareInfoSecurity, April 13, 2012, accessed November 08, 2014, http://www.healthcareinfosecurity.com/blogs/utah-hack-attack-lessons-learned-p-1244/op, 1.

[43] "Advanced Persistence Threat 1, Exposing One of China's Cyber Espionage Units," Mandiant.com, February 2013, 2, accessed September 12, 2014, http://intelreport.mandiant.com/.

[44] Richard Clark and Robert Knake, *Cyber War* (New York: Harper Collins, 2010), 13.

marker. With the attacks, Russia disrupted the Estonian way of life for two weeks by shutting down the websites of the Estonian presidency and parliament, most of the country's government ministries, three of the country's biggest new organizations, and two of the biggest banks.[45] In 2008, Russia used cyber attacks prior to the invasion of Georgia to accompany its military aggression, effectively crippling the Georgian internet.

As nation states refined their cyber capabilities and began using it in support of kinetic attacks, state govenors became increasingly concerned about the safety of their critical infrastructure systems. This was the result of two developments. One, with the steady increase of internet capable devices, companies began to connect additional devices to the internet. Second, various attacks highlighted the vulnerabilities of these systems. The Aurora tests at the Idaho National Laboratory (INL) in 2006 demonstrated the possibility of a cyber attack causing physical damage to critical infrastructure.[46]

In 2009, Stuxnet demonstrated that an attack similar to the Aurora test could cause physical damage to a system. With Stuxnet, unknown actors used a self-replicating worm in the first known attack against a supervisory control and data acquisition system (SCADA).[47] The attack infected Iranian uranium-centrifuge machines and caused them to spin at a higher

[45] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007, accessed February 3, 2015, http%3A%2F%2Fwww.theguardian.com%2Fworld%2F2007%2Fmay%2F17%2Ftopstories3.russia.

[46] Miles Keogh and Christina Cody, *Cybersecurity for State Regulators With Sample Questions for Regulators to Ask Utilities* (National Association of Regulatory Utility Commissioners, 2013), 7. In a test named Aurora, a controlled hack into a replica of the power plant's control system resulted in a change to the operating cycle of the generator, which sent it out of control and physically damaged and disabled it.

[47] David Kushner, "The Real Story of Stuxnet," IEEE Spectrum, February 26, 2013, accessed December 03, 2014, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

frequency.[48] The change to rotor speed resulted in damage to over 1000 centrifuges.[49] The technical sophistication of Stuxnet points to the direct involvement of a nation, which would have possessed the necessary hardware and expertise to launch the attack. The Shamoon virus attack in 2012 against Saudi Arabia's gas firm, Aramco, highlighted further vulnerabilities to the private sector. [50] These attacks combined with the increase in probes of US critical infrastructure raised the importance of protecting these systems.

The Aurora test, Stuxnet, and Aramco attacks revealed the vulnerabilities to the energy sector. These attacks were the most publicized ones, but only represented a fraction of the attacks against the energy sector. General Keith Alexander, previous Director of the NSA and USCYBERCOM, stated that there was a seventeen-fold increase in cyber attacks on American infrastructure from 2009 to 2011, initiated by criminal gangs, hackers, and other nations.[51] In 2012, Secretary of Defense Leon Panetta acknowledged that he was aware of specific instances where intruders had successfully gained access to computer control systems that operate US

[48] Miles Keogh and Christina Cody, *Cybersecurity for State Regulators With Sample Questions for Regulators to Ask Utilities* (National Association of Regulatory Utility Commissioners, 2013), 7.

[49] David Albright, Paul Brannan, and Christina Walrond, "Institute for Science and International Security Reports," December 22, 2010, accessed December 6, 2014, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

[50] Christopher Bronk and Eneken Tikk, "The Cyber Attack on Saudi Aramco," Iiss.com, April 1, 2013, accessed November 8, 2014, http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272. The virus infected 30,000 window's based machines and deleted data from the hard drives.

[51] David E. Sanger and Eric Schmitt, "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure," *The New York Times*, July 26, 2012, accessed November 09, 2014, http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=3&.

chemical, electricity, and water plants.[52]

Figure 1 shows the growth of incidents reports (IR) for organizations that own and operate control systems associated with critical infrastructure.[53] Out of the 198 reported incidents in 2011, thirty-one of these involved the energy sector, which was an increase from eighteen attacks in 2010. In 2010, forty-four percent of the attacks were against the energy sector, where in 2011 forty-one percent of the attacks were in the water sector.[54] The increase in the water sector was due to a higher number of internet facing control system devices that year.[55]

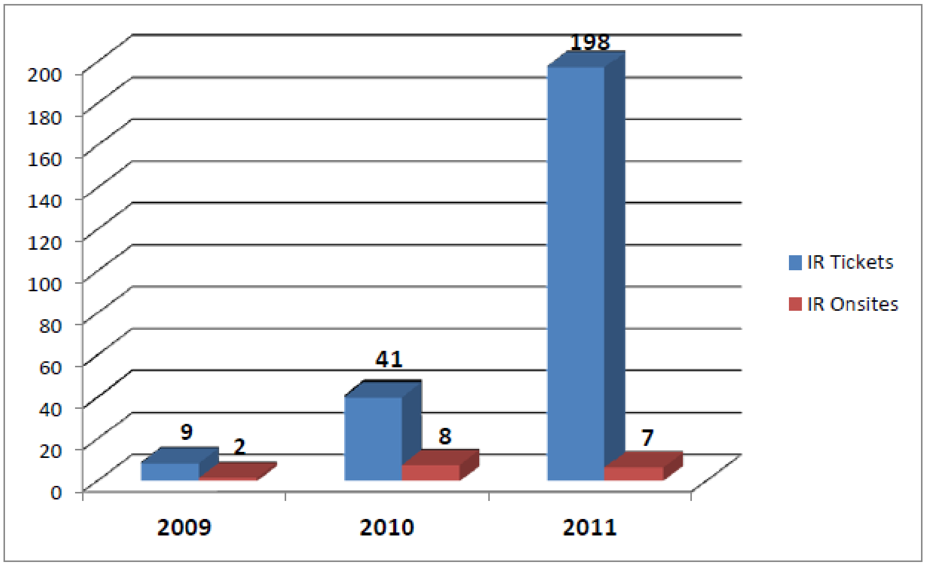

Figure 2. ICS Incidents Reported from 2009-2011.

[52] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, October 11, 2012, accessed November 09, 2014, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

[53] US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Incident Response Summary Report for 2009 Thru 2011*,2, accessed December 2, 2014, https://ics-cert.us-cert.gov/ICS-CERT-Incident-Response-Summary-2009-2011.

[54] Ibid., 3-5.

[55] Ibid.

*Source:* Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Incident Response Summary Report for 2009 Thru 2011.*

While there are significant threats to various critical infrastructure sectors, the Federal Energy Regulatory Commission (FERC) agreed that the threat of a cyber attack on the electric grid was the top threat to electricity reliability in the United States.[56] In October 2012, Defense Secretary Panetta warned that the United States was facing the possibility of a “cyber Pearl Harbor” and was increasingly vulnerable to attacks from foreign hackers who could disable the nation’s power grid and other critical infrastructure.[57] In November 2014, Admiral Michael Rogers, current USCYBERCOM commander, warned the House Intelligence Committee that nation states like China and possible others already possessed the capabilities of attacking components of the nation’s electrical grid.[58]

The electric grid is vulnerable for a couple of reasons. Like other critical infrastructure, it is composed of industrial control systems (ICS) which include SCADA systems. These SCADA systems are vital and are the brains behind US critical infrastructure.[59] Throughout the electrical grid, SCADA systems monitor and control electricity distribution by collecting data and issuing

[56] *Hearing Before the Subcommittee on Energy and Power,* American Energy Initiative, 112th Cong., 1st sess, 2011, HR, accessed October 22, 2014, 101, http://democrats.energycommerce.house.gov/sites/default/files/image_uploads/091411%20EP%20The%20American%20Energy%20Intiative%2012%20-%20Impacts%20of%20the%20Environmental%20Protection%20Agency%27s%20New%20and%20Proposed%20Power%20Sector%20Regulations%20on%20Electric%20Reliability.pdf

[57] Bumiller and Shanker.

[58] Siobhan Gorman, "NSA Director Warns of ‘Dramatic’ Cyberattack in Next Decade," *The Wall Street Journal*, November 20, 2014, accessed November 26, 2014, http://online.wsj.com/articles/nsa-director-warns-of-dramatic-cyberattack-in-next-decade-1416506197.

[59] US Department of Commerce, *Guide to Industrial Control (ICS) Security (NIST Special Publication 800-82),* by Keith Stouffer and Suzanne Lightman (2014), 1.

commands to geographically remote field sites from a centralized location.[60] Operators originally controlled SCADA systems through electrical hardware, but over time, ICS designs were modified to allow control from computers and network technologies. In the late 1990s, many companies connected their ICS systems to the internet to allow managers real-time system access. This resulted in an increased awareness about the systems and their processes, but also made ICS systems more vulnerable to computer hackers.[61]Attacks on SCADA devices give hackers direct control of operational systems.

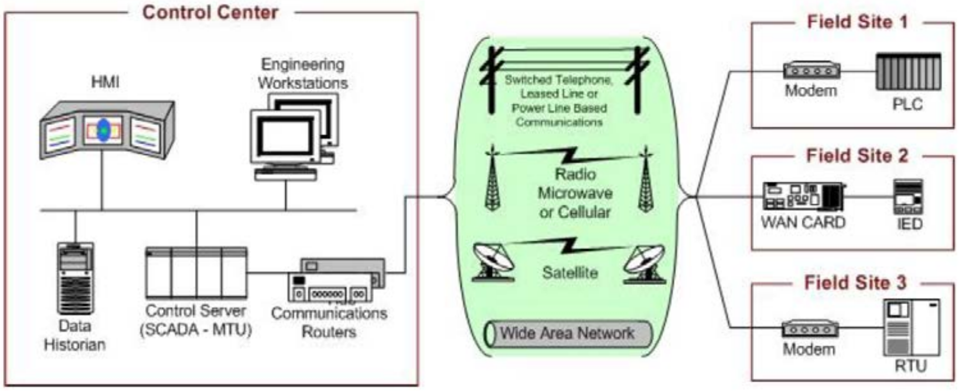

Figure 3. SCADA System General Layout 2014.

*Source:* US Department of Commerce, *Guide to Industrial Control (ICS) Security (NIST Special Publication 800-82),* Keith Stouffer and Suzanne Lightman. 2014.

In the *2014 Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence,* James Clapper, Director of National Intelligence, stated that the ICS and SCADA devices provide “an enticing target to malicious actors.”[62] He acknowledged the

[60] Ibid., 2-3.

[61] Ibid., 2-3.

[62] Select Committee on Intelligence, Worldwide Threat Assessment of the US Intelligence Community,113th Cong., 2nd sess., 2014, S. Rep, 2.

benefits of newer architectures, which provide flexibility, functionality, and resilience, but also recognized the vulnerability these systems had to attack. The so-called "internet of things" had transformed the role of information technology in the global economy, but the "complexity and nature of these systems [meant] that security and safety assurances [were] not guaranteed and that threat actors [could] easily cause security and/or safety problems in these systems."[63] In the 2013 report, Director Clapper stated, "there was a remote chance of a major cyber attack against US critical infrastructure during the next two years that would result in long-term, wide-scale disruption of services, such as a regional power outage."[64]

Governors are concerned about cyber criminal and espionage attacks, but are more concerned with an attack on critical infrastructure within their state. The fear is that terrorist or belligerent nation states will join with or employ cyber criminals to harness their skills for future attacks.[65] All indicators point to an increased interest in attacking these facilities and to the ability for conducting such sophisticated attacks. An article by *Stateline* reports that an October 2012 survey of states' Chief Information Security Officers (CISO) reveals that seventy percent of states have experienced a cybersecurity breach.[66] Only twenty-four percent of CISOs said they felt

[63] Michael Chui, Markus Loffler, and Roger Roberts, "The Internet of Things," McKinsey & Company, March 2010, accessed December 05, 2014, http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things. The term internet of things describes the growing interconnectedness of many devices that are linked through wired and wireless networks, communicating over the internet.

[64] Select Committee on Intelligence, Worldwide Threat Assessment of the US Intelligence Community,113th Cong., 1st sess., 2013, S. Rep, 1.

[65] Reveron, 13.

[66] Melissa Maynard, "The National Guard Takes On Hackers," *Stateline*, January 28, 2014, accessed December 06, 2014, http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/01/28/the-national-guard-takes-on-hackers.

"very confident" that their state assets were secure against cyber attacks, and only thirty-two percent said their staffs were capable of protecting computer networks against cyber attacks.[67]

Cyber analysts in the 1990s warned of attacks targeting critical infrastructure, but it in only within the last eight years that these attacks became more of a probability. Analysts attribute this to two main reasons. First, advanced cyber actors have demonstrated their increased ability to use cyber as a weapon against critical infrastructure. The Stuxnet attack against Iranian nuclear facilities and the Shamoon attack against Saudi Arabia Aramco facility are just two examples. Second, as the internet developed, critical infrastructure networks became more interconnected which made them more vulnerable to attacks through the cyber domain. Today, governors face the challenge of developing strategies to protect critical assets in their states from the tangible threat of a cyber attack.

## Part 2

## Responses to Cyber Threats

As cyber attacks evolved, federal and state government realized the need to develop plans to combat these threats. The federal government recognized the potential threats from the cyber domain as early as 1998 when President Clinton released *PPD 63*. Release of *PPD 63* began the process of viewing cybersecurity as a distinct national security policy. President Bush and Obama have likewise issued guidance on the cyber threats, the need for effective strategies to prevent attacks, and ways the United States can enhance its resiliency. The presidential emphasis on cyber threats and the need for effective strategies led DHS, DoD, the US Congress, and state governors to examine their roles against this emerging cyber threat.

[67] Ibid.

DoD's initial view of its role in the cyber domain is described in the *2008 NDS* where it envisioned a limited, supporting role during a cyber attack and did not see itself as the best "source of resources and capabilities."[68] This view evolved, but understanding the mindset in 2008, helps better understand the initial lack of emphasis on a total force concept that included the National Guard. In 2010, both DHS and DoD took actions to address the new threats and began issuing updated guidance on the changing threat environment. While both organizations recognized the emergence of new threats capabilities, DHS provided more guidance for states on potential future strategies, particularly the defense of critical national assets.

Governors currently look to the Guard for assistance when faced with an external threat that overwhelms local responder capabilities. Most states do not possess the necessary civilian cyber capabilities "to manage, prevent, and mitigate damage" from more sophisticated cyber attacks, but the National Guard does possess a capability that could assist them in their efforts.[69] The US Congress recognized the benefits to utilizing assets that were already at the governor's disposal and envisioned ways of increasing these assets to provide an even greater capability. Through its legislative power, Congress proposed new ways to include the National Guard in the tiered response to cyber attacks.

As a Presidential cabinet organization, DHS is responsible for security of the United States, including responses to national disasters at the federal level.[70] To accomplish this task within the cyber domain it has published numerous publications, which outline potential strategies on how the nation and states should respond to cyber incidents. DHS issued *NCIRP* in

[68] US Department of Defense, *2008 National Defense Strategy* (Washington, DC, June 2008), 7.

[69] Saporito, 1.

[70] Homeland Security Act of 2002, 2212.

2010 and the *NIPP* in 2013 to address the roles governors have in protecting critical infrastructure within their states.

The *2010 NCIRP* described how the nation should respond to significant cyber incidents and was developed in close coordination with federal, state, local, territorial, and private sector partners. It outlined a strategy for coordinating the response activities of all levels of government against threats that crossed between those levels. "The purpose of the *2010 NCIRP* is to establish the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident."[71] In the section examining the state, local, tribal, and territorial roles and responsibilities, it stated that governors "should be prepared to request additional resources from the Federal Government, including [those] under the Stafford Act, in the event of a cyber incident that exceeds their capabilities."[72] The Stafford Act authorizes the President to issue major disaster or emergency declarations in response to catastrophes that overwhelm state and local governments and provides the funding for Guard forces to work in a Title 32 status for the state. The *2010 NCIRP* also recognized the unique position of the National Guard to assist in information sharing, situation awareness, secure communications, and incident response.[73]

DHS took Presidential guidance published in President Obama's PPD-21 and developed the *2013 National Infrastructure Protection Plan (NIPP). PPD-21* is a classified document, but

[71] US Department of Homeland Security, *National Cyber Incident and Response Plan* (Washington DC, September 2010), 1.

[72] Ibid., H-1.

[73] Ibid.

the *2013 NIPP* cited unclassified sections to clarify roles and responsibilities across the Federal government and established a more effective partnership with critical infrastructure owners and operators, and state, local, tribal, and territorial governments.[74] It declared that states must "ensure the security and resilience of critical infrastructure under their control, as well as that owned and operated by other parties within their jurisdictions."[75]

Since 2005, the DoD understanding of its role and cyber threats has evolved. Initially, DoD focused on protecting its military information infrastructure. The *2005 NDS* was the first NDS that identified cyberspace as a new theater of operation. It stressed that successful military operations depended on the ability to "protect information infrastructure and data."[76] It recognized "disruptive breakthroughs," including cyber, which could fundamentally alter long-established concepts of warfare.[77] The *2005 NDS* looked at cyber through the narrow lens of vulnerabilities to information networks.[78]

The *2008 NDS* assessed that small groups  could "attack vulnerable points in cyberspace and disrupt commerce and daily life in the Unites States, causing economic damage, compromising sensitive information and materials, and interrupting critical services such as power and information networks."[79] The 2008 document included China for the first time as a

[74] US Department of Homeland Security, *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC, 2013).

[75] Ibid., 46.

[76] US Department of Defense, *2005 National Defense Strategy* (Washington, DC, March 2005), 13.

[77] Ibid., 3.

[78] Ibid., 13.

[79] *2008 National Defense Strategy*, 7.

country that was “developing technologies to disrupt our traditional advantages” in cyber warfare.[80] It further stated that while DoD should help in responding to protect lives and national assets, it was not the best “source of resources and capabilities and not the appropriate authority to shoulder these tasks.”[81]

As Presidential administrations put more emphasis on cyberspace and combating cyber threats, DoD’s role in combating cyber attacks increased. The *2010 QDR* established cyberspace as a relevant domain for the Defense Department.[82] DoD created USCYBERCOM in 2010 and recognized cyber as a domain in 2011. USCYBERCOM’s three critical missions are to defend the DoD Information Network (DoDIN), provide support to combatant commanders, and strengthen the nation’s “ability to withstand and respond to a cyber attack.”[83]

The *2011 National Military Strategy* (NMS) mentioned China as a specific threat and stated that “some states are conducting or condoning cyber intrusions that foreshadow the growing threat” in the cyber domain.[84] Unlike the *2008 NDS*, it spoke of a collaborative versus supporting relationship between Strategic Command and USCYBERCOM with US government agencies, non-government entities, industry, and international actors.[85] Unique to the *2011 NMS* is the emphasis on using a total force concept. It acknowledges the idea of ensuring there should

[80] Ibid., 22.

[81] Ibid., 7.

[82] US Department of Defense, *2010 Quadrennial Defense Review Report* (Washington, DC, February 2010), 37.

[83] US Strategic Command, *US Cyber Command Fact Sheet*, August 2013, accessed December 06, 2014, http://www.stratcom.mil/factsheets/2/Cyber_Command/.

[84] US Department of Defense, Chairman, Joint Chiefs of Staff, *The 2011 National Military Strategy of the United States of America* (Washington, DC, February 2011), 3.

[85] Ibid., 10.

be appropriate balance between active and reserve components that would enable DoD to maintain a strategic and operational depth.[86]

The 2012 strategic defense guidance located in *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* served as the national defense strategy for 2012. It identified one of the primary missions of the US armed forces as operating effectively in cyberspace and space with the "advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space."[87] It stated that "modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space."[88] It recognized the threat that both state and non-state actors possess to conduct cyber espionage and cyber attacks that result in severe effects on military operations and the homeland. Unlike the *2008 NDS*, it does not mention China as a growing risk and does not include a section concerning DoD's role as a supporting role in the interagency effort to combat cyber attacks.

The *2014 QDR* highlighted the US Defense Department's plans to invest in "new and expanded cyber capabilities and forces to enhance our ability to conduct cyberspace operations and support military operations."[89] It expanded DoD's focus to include not only deterring attacks against DoD networks and infrastructure, but also disrupting and denying adversary cyberspace

[86] Ibid., 17.

[87] US Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC, January 2012), 5.

[88] Ibid.

[89] US Department of Defense, *Quadrennial Defense Review* (Washington, DC, March 2014), 41.

operations against US interests.[90] In it, DoD further defined the relationship with DHS and emphasized the joint mission of improving critical infrastructure cyber security.[91] It outlined the strategy, which involves the creation of 133 Cyber Mission Force Teams composed of 6,000 cyber warriors.

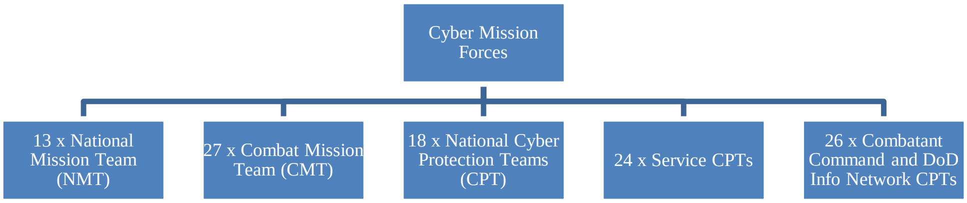
Cyber Mission Forces
13 x National Mission Team (NMT)
27 x Combat Mission Team (CMT)
18 x National Cyber Protection Teams (CPT)
24 x Service CPTs
26 x Combatant Command and DoD Info Network CPTs

Figure 4. Cyber Mission Force Construct.

*Source:* Adapted from *2014 Quadrennial Defense Review*

The creation of these forces shows DoD's commitment in meeting future challenges. One critical elements missing in the current cyber mission construct is Nation Guard cyber forces. Currently, DoD has only authorized the National Guard to create one Title 10 Cyber Protection Team (CPT) that is under control of the National Guard Bureau. It has not identified specific roles or missions for the remainder of National Guard cyber Soldiers. Army Cyber Command (ARCYBER) commander, Lieutenant General Edward Cardon stated that Guard will begin to build combat power with additional force structure coming on line in FY 2016 with the goal of eventually creating ten additional Title 32 CPTs.[92]

[90] *2014 Quadrennial Defense Review*, 15.

[91] Ibid.

[92] Edward C. Cardon, "ARMY.MIL, The Official Homepage of the United States Army,"

In October 2013, DoD made progress towards integrating the active and reserve component when the National Guard stood up the first Cyber Protection Team (CPT), the 1636th CPT.[93] Under an agreement between ARCYBER, Second Army, and the Army National Guard, the team will integrate with ARCYBER.[94] The 1636th CPT serves in a Title 10 status and will be capable of conducting a variety of missions.[95] The creation of the 1636th CPT was beneficial to integrating Guard and Active component forces, but it still does not adequately address the lack of Title 32 Guard cyber forces at the state level or the plan for building these capabilities.

In the absence of DoD guidance for existing states' Guard cyber forces, governors have increasingly called for additional National Guard involvement in cyber security issues. Governors are saddled with the difficult responsibility to protect their own state's information technology infrastructure as well as working with the private sector to protect the state's and nation's critical infrastructure. In addition, they have to be ready to respond to any disruption caused by a cyber attacks. They not only need to respond, but do so in a timely manner. One of the critical problems now is the length of time between when an attack occurs and when someone identifies it. In the

2014 Green Book: Army Cyber Command and Second Army, September 30, 2014, accessed November 29, 2014, http://www.army.mil/article/134857/.

[93] Mike Milord, "National Guard," Army Guard's First Cyber Protection Team Activated; Receives New Shoulder Sleeve Insignia, October 10, 2014, accessed November 26, 2014, http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/11413/army-guards-first-cyber-protection-team-activated-receives-new-shoulder-sleeve.aspx.

[94] Mike Milord, "ARMY.MIL, The Official Homepage of the United States Army," Army Cyber Command, Army Guard Sign Memorandum to Integrate Cyber Protection Team, June 5, 2014, accessed November 26, 2014, http://www.army.mil/article/127442/Army_Cyber_Command__Army_Guard_sign_memorandum_to_integrate_cyber_protection_team/.

[95] Ibid. 1636th CPT will be capable of conducting defensive cyberspace operations, cyber command readiness inspections, vulnerability assessments, cyber operational forces support to emulate threats, critical infrastructure assessments, theater security cooperation and Federal Emergency Management Agency support.

South Carolina attack, the discovery took almost two months.[96] This is similar to the time lag Target and Home Depot experienced when their attacks went unnoticed for one and five months respectively.

As governors looked across the threat landscape and saw the increase of attacks across multiple sectors to include state agencies and an increase in attacks against critical infrastructure, especially in the energy sector, they realized the need for effective strategies. At the same time, many of them also faced a limited cyber workforce.[97] State agencies possess the needed information security specialist to keep their networks running, but lack the personnel and resources to monitor and scan for attacks originating from medium to high-level actors. These shortages are located throughout state agencies and industrial sectors.[98] Faced with new threats and a personnel shortage, governors took notice of the growing National Guard cyber expertise that had developed through realistic training, participation in exercise scenarios with federal and state partners, and exposure to latest threat techniques and tactics. This began the process of them advocating for the integration of the Guard to into the states' cyber framework.

In support of the state governors, the National Governor's Association (NGA) published numerous articles highlighting the need for better Guard integration and the benefits of that integration. The NGA is a bipartisan organization of the nation's governors that identifies priority

[96] Marshal Heilman, *Mandiant, South Carolina Department of Revenue Public Incident Response Report*, November 20, 2012, 2, accessed December 11, 2014, http://governor.sc.gov/Documents/MANDIANT%20Public%20IR%20Report%20-%20Department%20of%20Revenue%20-%2011%2020%202012.pdf.

[97] Saporito, 1.

[98] Martic C. Libicki, David Sentry, and Julia Pollack, "Site-wide Navigation," Hackers Wanted: An Examination of the Cybersecurity Labor Market, 2014, Prologue, accessed December 11, 2014, http://www.rand.org/pubs/research_reports/RR430.html, 3.

issues and helps develop innovative solutions to problems facing state government.[99] A NGA paper in 2013, *Act and Adjust: A Call to Action for Governors,* encouraged governors to take actions to help detect and defend against cyber attacks occurring today and help deter future attacks.[100] As governors look to develop strategies to address the cybersecurity challenges they must balance the potential threat and what they are trying to protect as well as the limited cyber workforce capacity in their states. In meeting the need to establish a stable cyber workforce to respond to these issues, governors can hire new employees, train or retrain current employees, or contract out.[101]

To build the cyber workforce, governors need to design cybersecurity teams that include a mix of professionals from the private sector, state agencies, and the National Guard. They can incorporate the Guard into these teams because it possesses the needed expertise and because it has the ability to adapt its existing response and recovery measures for natural disasters to cybersecurity. The NGA recognized that the Guard is "not is a position to supplement a state's normal day-to-day cybersecurity operations," but it can assist in incident response and in a coordinate, train, advise, and assist (C/TAA) role for other state agencies.[102] The National Guard is a unique military force that can operate across state and federal responses to include State Active Duty (SAD), Full-Time National Guard Duty (Title 32), or even Active Duty (Title 10) in an incident response role.[103]

[99] "About the National Governors Association," National Governors Association, accessed December 07, 2014, http://www.nga.org/cms/about.

[100] MacLellan, 1.

[101] Saporito, 1.

[102] Ibid., 5.

[103] Annie Lively, *Understanding the Guard's Duty Status*: 1, accessed November 13, 2014, http://www.ngaus.org/sites/default/files/Guard%20Statues.pdf.

In SAD, the Governor can activate Guard personnel in response to a natural or man-made disaster or Homeland Defense mission. The Posse Comitatus Act does not apply, giving Guardsmen the ability to act in a law enforcement capacity within their home state.[104] SAD funds are allocated by state legislatures and amounts vary between states, which impacts the ability of the governor to bring Soldiers on in this status. In Title 32, the Governor, with the approval of the President or Secretary of Defense, can order a member to duty for operational Homeland Defense activities in accordance with Title 32 US Code. Through Title 10, the President can order National Guard forces to an active duty status.[105]

Governors can also leverage the Guard by incorporating them into a C/TAA role with other state partners prior to an incident. States such as California appropriated the necessary SAD funds through their legislatures and used their CND-T to conduct network vulnerability assessments of other state agencies. The assessments help detect potential vulnerabilities on these networks. The Guard is also available to provide a tiered response when an attack occurs. Utilizing the Guard in this manner ensures that local responders get the same level of support during a cyber attack that they get during other events that affect the state. By using all available state assets, governors are demonstrating that they are not just relying on federal agencies to solve their problems.

The US Congress also recognized the importance of incorporating the National Guard into the country's overall cyber efforts. With little ambiguity, industry and government experts have persistently warned Congress about the vulnerabilities and threats cyber attacks posed to the United States. In response to numerous testimonies, reports, and hearings, both the Senate and House of Representatives introduced identical versions of a bill known as the Cyber Warrior Act

[104] Ibid.

[105] Ibid.

of 2013. While Congress did not pass the bill, the bi-partisan backing for the bill highlighted the importance Congress placed on giving states resources to deal with emerging cyber threats. Senator Christopher Coons, D-Delaware, summed up the need for the resources when he said, “the Cyber Warrior Act will ensure that in the first hours and days after a devastating cyber attack, our local responders will have the same support of the National Guard for response and recovery that they do when a hurricane strikes.”[106]

The bill called for DoD to establish National Guard Cyber and Computer Network Incident Response Teams (CCNIRT). These teams would “perform duties relating to analysis and protection in support of programs to prepare for and respond to emergencies involving an attack or natural disaster impacting a computer, electronic, or cyber network.”[107] In addition, the bill stated that the Secretary of the Army and Secretary of the Air Force should ensure reserve component cyber training was equivalent to the active component training. The bill recognized that the Guard could operate in a Title 10 or Title 32 status based off the particular situation. The bill also outlined the potential role of the Guard in educating and training state and local law enforcement and government personnel.”[108]

DoD was critical of the bill and believed the act “divert[ed] limited resources from the Department’s efforts to strengthen USCYBERCOM and shift[ed] State and Department of Homeland Security financial responsibilities to the DoD.”[109] The House Armed Services

[106] "Cybersecurity Business Infrastructure Protection," Homeland Security News Wire, February 3, 2014, accessed November 11, 2014, http://www.homelandsecuritynewswire.com/dr20140203-national-guard-units-help-states-ward-off-cyberattacks.

[107] Cyber Warrior Act of 2013, H. Res. 1640, 113th Cong., 1st sess. (2013).

[108] Ibid.

[109] Ron Jensen, "Cyber Sense," *National Guard* 67, no. 6 (June 2013): 21, accessed February 13, 2015,

subcommittee on intelligence, emerging threats, and capabilities did not approve the bill due to the cost of the proposal and lack of information on the role for the Reserves. Even though the measure failed to pass, it drew attention to the governors' need for assets capable of responding to cyber attacks.

In the *2014 NDAA*, Congress tasked DoD to conduct mission analysis for cyber operations.[110] Part of this included the DoD plan for integrating the Guard and other Reserve Component units to meet total force requirements for cyber security. In section 933, Congress directed DoD to identify all Guard cyber resources, to assess the manpower needs for cyber operations forces, to evaluate the potential roles of the Guard in a concept of operations and employment, to identify the mission requirements that could be conducted by the Guard.[111] It also asked for a specific assessment if "the National Guard, when activated in a State status (either State Active Duty or in a duty status under Title 32, United States Code) [could] operate under unique and useful authorities to support domestic cyber missions and requirements of the Department or the USCYBERCOM."[112] Similar to the Cyber Warrior Act of 2013, the questions asked through Section 933 demonstrated that Congress still envisioned a greater role for the National Guard in strengthening governors' cyber security strategies.

In the response to Congress in August 2014, DoD outlined the benefits of incorporating National Guard forces into the cyber mission force construct. The DoD response is classified "For Official Use Only." It does present possible solutions for further Guard integration, but is a pre-

—

http://nationalguardmagazine.com/article/Cyber_Sense/1425297/162672/article.html.

[110] National Defense Authorization Act for Fiscal Year 2014, Public Law 113-66, 113th Cong., 1st sess (December 26, 2013), 830.

[111] Ibid., 830.

[112] Ibid.

decisional and does not provide specific authorizations or tasks for Guard for additional cyber mission forces beyond the one CPT. The DoD response is a starting point for discussions, but should not be seen as the final solution for providing critical resources to the governors.

Taken together, national strategy, DHS guidance, and DoD publications identify the most likely threats from cyber attacks as well as potential targets. State governors recognize the need to prepare to defend and respond against cyber attacks. Governors must develop plans to protect critical infrastructure based on the threat capabilities and instances of attacks already committed against states. As they take into account the threat, they also analyze the cyber expertise within the state. DHS policies and the US Congress encourage them to look at cyber capabilities within the National Guard for assistance as they develop their state strategies.

## Part 3

## National Guard Cyber Capabilities

Why should governors look to the National Guard for assistance with cyber related problems? One reason is that the Guard possesses cyber forces, which can integrate into the overall national cybersecurity defensive effort. Through the work of Army and Air National Guard Soldiers, units have worked to protect its own networks from attack. With these experiences, they have learned about different tactics cyber actors use and have gained valuable experience in identifying network vulnerabilities and fixing them prior to an attack. While DoD has not specifically designated the Guard future roles in the CMF, Guard forces have developed a cyber skill set that parallels many active component elements. In addition to the CND-Ts, Adjutant Generals created numerous ANG capabilities. Based on the threats that Guard units encountered protecting its networks and the need the states have for additional expertise, Guard leadership has expanded their cyber capabilities to help mitigate the risks they and their states encounter. This initiative by numerous Adjutant Generals enabled the Guard to grow its cyber capabilities even in the absence of direct DoD guidance and direction.

The Guard's initial involvement with cyber began with the creation of computer emergency response teams (CERTs) in the 1990s. These teams were placed on the states' Joint Force Headquarters Table of Distribution and Allowances manning documents. Many states utilized their CERTs in their overall response to Y2K concerns in 1999.[113] These teams evolved into CND-Ts, with a focus on protecting the National Guard network, GuardNet, and developing procedures to protect the networks physical and information infrastructure. [114] Even though manning of CND-Ts was limited initially to eight Soldiers, some leaders doubled or tripled the numbers, such as the Missouri National Guard which created a twenty-eight person CND-T.[115] The Soldiers on these teams completed their military education requirements and required civilian accreditations to perform their missions. These teams initially focused on defending military networks, but today have expanded in some states to include a C/TAA role for other state agencies working to protect their networks.

In 2013, The National Guard Bureau established a *Concept of Operation for Computer Network Defense Teams.* This serves as a guide for how CND-T's should operate and is based on DoD and DHS Regulations.[116] Members of the team are required to meet the same standards as

[113] John J, Monahan, "Guard Maps Plan for Y2K Emergencies," *Telegram & Gazette*, February 20, 1999, accessed September 30, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/268714473?accountid=28992.

[114] "GuardNet XXI," *Stand-To!*, July 31, 2014. accessed November 23, 2014, http://www.army.mil/standto/archive_2014-07-31/?s_cid=standto. GuardNet is a single, secure, accredited, standards-based mission command network that enables connectivity for over 2,500 training and operational facilities nationwide. It is the ARNG's portion of the Department of Defense (DOD) Information Enterprise.

[115] Caitlin Baker, "Missouri National Guard Forms Cyber Response Team | Ksdk.com," Ksdk.com, January 11, 2013, accessed November 11, 2014, http://www.ksdk.com/news/article/356592/3/Missouri-National-Guard-forms-cyber-response-team.

[116] Army National Guard, *Concept of Operations: Computer Network Defense Teams*

active component Soldiers, which are found in *DoD 8570.01-M: Information Assurance Workforce Improvement Program, Incorporating Change*. It designated the different positions on the team and the roles and responsibilities of those teams. These teams protect Guard networks, but also are available and trained to respond to a variety of cyber incidents.

Many states solely use their CND-Ts for the defense of the local military network, but Washington was one of the first states to assign the National Guard cybersecurity responsibilities that went beyond the protection of state networks. The state "recognized the potential of its National Guard as a cyberforce when it realized that many of its Soldiers, who were full-time employees and part-time Soldiers, worked for tech employers such as Google, Boeing, Verizon, and Microsoft."[117] The Washington ANG's 262nd Network Warfare Squadron conducts exercises searching for weaknesses throughout their military networks but can also conduct similar vulnerability testing of networks critical to state systems that control power, water, and emergency services.[118] This relationship benefits the National Guard by giving the Soldiers continued real world experience, training, and practice against the emerging cyber threat. It is also a cost savings measure for the state that now gets cyber support from another state agency instead of an outside organization.

In addition to providing vulnerability assessments for state agencies in Maryland, the ANG's 175th Network Warfare Squadron supports cyber security assessments by participating in

—

(2014), 9.

[117] "Cybersecurity Business Infrastructure Protection," Homeland Security News Wire, February 3, 2014, accessed November 11, 2014, http://www.homelandsecuritynewswire.com/dr20140203-national-guard-units-help-states-ward-off-cyberattacks.

[118] William Matthews, "The Next Global War," *National Guard* 65, no. 6 (June 2011): 29, accessed November 11, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/873280915?pq-origsite=summon.

penetration testing with state agencies.[119] During these exercises, cyber opposing forces act as malicious actors and attack agency networks, which help the agencies evaluate the security of their websites and portals. Security issues uncovered through the penetration test led to technical and procedural countermeasures to reduce risks.[120] The training also benefits unit members who receive valuable training and practice as a result of their participation. California's CND-T and its ANG's 261st Network Warfare Squadron also provide similar capabilities. [121]

The Virginia Date Processing Unit is another example of how the National Guard is transforming itself to meet the increased cyber threats. Originally, the unit provided data processing support to the National Guard Bureau Computer Center.[122] Today, its Soldiers participate in computer defense and network operations. Their missions vary from advising units how to harden and secure their websites to assessing state networks and even serving as emergency cyber responders.[123]

Another example of expanding roles is the Michigan National Guard's involvement with the creation of a statewide cyber range. The Michigan National Guard received funding to develop a cyber-range facility that allows public and private industry to participate in joint

[119] MacLellan, 4.

[120] Ibid.

[121] William Matthews, "Cyber Uncertainty," *National Guard* 68, no. 7 (July 2014): 25, accessed September 30, 2014, http://search.proquest.com.lumen.cgsccarl.com/docview/1552463797?accountid=28992.

[122] Scott Campbell, "Virginia Guard Data Processing Unit Conducts First Unit-level Cyber Defense Exercise," October 21, 2010, accessed November 11, 2014, http://vko.va.ngb.army.mil/virginiaguard/news/oct10/DPUexercise.html.

[123] Matthews, 28.

exercises without needing a security clearance.[124] Michigan uses the range to "train college students, technology workers, and Guardsmen to detect and prevent cyber attacks."[125] Ranges such as this serve as a good model for future partnerships and provide "valuable research and analysis of cyber vulnerabilities for state and local operators of critical infrastructure."[126] These types of initiatives are representative of the movement among governors to develop the necessary tools and resources instead of waiting for the federal government to develop solutions.

In Delaware, the ANG's 166th Network Warfare Squadron created a unique role through it work at the NSA. It focuses on defensive work to include diagnostic analysis of computer and network intrusions for the military, the national security community, and law enforcement agencies.[127] In Texas, the 273rd Information Operations Squadron performs vulnerability assessments and supports cyber exercises.[128]

The current innovations by the Guard in the cyber domain are not an isolated phenomenon in the history of the Nation Guard. The success of Guard volunteers in the Spanish-American War in 1898 and service in the Philippines created an opportunity to convert the militia units into the National Guard.[129] In 1903, Congress passed the Militia Act, which served as a new beginning for the Guard. For the first time the federal government granted funding and equipment

[124] Wood.

[125] Matthews, 24-29.

[126] Ibid.

[127] Ibid., 29.

[128] Ibid., 29.

[129] Michael D. Doubler, *Civilian in Peace, Soldier in War: The Army National Guard, 1636-2000* (Lawrence, Kansas: University Press of Kansas, 2003), 142.

in return for the Guard conforming to "federal standards for training and organization."[130] Since then the Guard has played a key role in helping defend the nation. Michael Doubler, noted military historian, traces the ARNG's involvement in homeland defense missions to include protection along the United States and Mexican border beginning in 1916, the CONUS air defense mission in the 1950s, and the Counter Drug program of the 1980s.[131] In addition to these missions, the ANG participated in the runway alert program in the 1950s. Due to the limited number of Air Force assets, the ANG provided air intercept capabilities to defend the continental United States against the Soviet air threat and represented the beginning of the Air Guard's modern homeland defense role.[132]

The CONUS air defense mission of the 1950s has multiple similarities for today's cyber environment. The ARNG served in the NIKE missile program and at the peak in 1962, 17,000 Guardsmen participated.[133] The object of the missile program was to "shoot down Soviet heavy bombers attempting to attack United States cities and industrial centers with nuclear weapons."[134] The program was the first time DoD assigned units in a state status to a full-time federal mission.[135] The benefits of using the Guard in the missile defense role are similar to the likely benefits that would result from increased missions in the cyber domain. In the NIKE program, the Guard "established itself as a readily accessible asset in the first line of defense against the

[130] Ibid., 144.

[131] Ibid., 159, 243, 342.

[132] Susan C. Rosenfeld and Charles Joseph Gross, *Air National Guard at 60: A History* (Arlington, VA: Air National Guard, 2007), 9.

[133] Michael D. Doubler and John W. Listman, *The National Guard: An Illustrated History of America's Citizen-Soldiers* (Washington, DC: Brassey's, 2003), 108.

[134] Ibid., 107.

[135] Doubler, *Civilian in Peace,* 241.

nation's most dangerous threat."[136] It also demonstrated the speed in which Guard forces could master high technology weapons. Finally, the Guard's participation resulted in manpower and dollar savings for the active Army.[137]

With a proven history of responding to a wide range of threats, it is hard to discern why DoD would not be more pro-active in utilizing the National Guard as a major partner for in the cyber mission forces construct. Guard units have completed the required training, have shown they have the capabilities to function in a variety of roles, and in some places, such as the ANG's involvement with NSA, are already working with active component forces to defend against cyber attacks. For all of its initiative and efforts, the National Guard currently has one CPT with the hope of getting an additional ten teams sometime in the future. These thirty-nine man teams will only represent seven percent of the total 6,000 DoD Cyber mission forces. While it is a start, it still leaves unanswered the question of how to integrate the existing Guard CND-Ts and other cyber forces into the national cyber force as well as how best to support states in defending their critical infrastructure.

## Part 4

## Cyber and Unified Land Operations

While the Guard possesses the capability to assist states preparing for and responding to cyber attacks, there is another reason for including Guard assets into the overall cyber mission force construct. Strengthening the role of the Guard in the cyber domain is the next logical step in adhering to established doctrine. General Keith Alexander, former USCYBERCOM commander, raised the issue when he looked at the national level strategies and saw some of the deficiencies in implementation of those strategies:

[136] Ibid., 243.

[137] Ibid.

> Despite this emphasis, however, we can argue that, while we have ample national level strategies, we have yet to translate these strategies into operational art through development of joint doctrine for cyberspace. Through the doctrine vetting process, we can develop a common understanding of what it means to conduct warfare within and through cyberspace.[138]

*ADP 3-0, Unified Land Operations (ULO),* is the Army's basic warfighting doctrine. It describes the Army's approach to generating and applying combat power in campaigns and operations.[139] "It is based on the central idea that Army units seize, retain, and exploit the initiative to gain a position of relative advantage over the enemy."[140] *ADP 3-0* describes the tenets of ULO and the operational art that commanders should use as a guide when conducting operations. National Guard integration into the mission force construct enable the Army to have better flexibility, integration, depth, and synchronization.

Employing the National Guard during a cyber attack provides flexibility for the overall response. Due to familiarity with the local communities and understanding of the state and local critical infrastructure, the Guard can quickly respond to an attack and begin defensive cyber operations. While Guard assets respond locally, a Title 10 organization could execute offensive cyber capabilities from another location. In some cases, this arrangement would allow the commander to work through Title 32 forces. Instead of deploying an entire team, he might only have to send a LNO to assist with the response. Guard forces could also leverage existing secure communication platforms within their states to insure Joint Worldwide Intelligence Communications System and NSA connectivity between the site and overall headquarters. This

[138] Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly*, no. 46 (2007): 59, accessed November 26, 2014, https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/203683705?accountid=28992.

[139] ADP 3-0, 7.

[140] Ibid., 5.

flexibility increases the options the commander has he arranges military actions in time, space, and purpose. Having forces already in the states also allows him to better control tempo.

Integrating National Guard forces in defensive cyber operations is one way to set conditions for favorable conflict resolution. As the initial responder to an incident, Title 32 cyber forces can help mitigate the effects of an attack and conduct the necessary actions to prevent further damage. Based on the type of attack, these forces can conduct reconnaissance on the threat and provide critical information to Title 10 forces that may follow on to further assist in stopping an attack by taking offensive actions against the threat. The integration of defense and offensive actions prevents the enemy from recovering by retaining the initiative. The combined actions of active component and National Guard is the best way to arrange tactical actions for "termination of the conflict on favorable terms."[141] It also allows for a response that is "rapid, unpredictable, and disorienting."[142]

Synchronization of Guard forces in this capacity provides for timely response and creates a bridge for integrating Title 10 forces into the state response to the attack. This type of synchronization provides commanders better understand of the operational environment and gives them the best opportunity for taking the initiative away from the threat. ADP 3-0 states:

> Synchronization is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time (JP 2-0). It is the ability to execute multiple, related, and mutually supporting tasks in different locations at the same time, producing greater effects than executing each task in isolation.[143]

Developing a response that synchronizes Title 10 and Guard forces creates a situation that enables commanders to build depth within their own organizations and operations in space, time, and

[141] Ibid.

[142] Ibid.

[143] Ibid.

resources.[144] Depth is essential for developing a holistic, all encompassing approach. Taking advantage of trained and certified Guard cyber warriors gives the commander of USCYBERCOM access to 54 separate CMF first responders who can gather the facts and begin work while he decides on the necessary response force. Use of Guard CMF also gives the commander the opportunity to move people from Title 32 to Title 10 quickly to respond to an escalating crisis that requires additional authorities. The Guard also possesses the ability to increase the number of Soldiers involved through the Emergency Management Assistance Compact between states.

The alternative to not utilizing National Guard would be to wait until the state requests federal assistance. This process takes time and does not provide for the rapid flexibility needed to confront a threat. While waiting for assistance, critical services would be degraded and further damage inflicted. In addition, it would take time to integrate Title 10 and local responders, due to unfamiliarity of working with one another. A trained and certified Guard cyber force on site could quickly integrate with the state and interagency response forces and would provide the best opportunity for overwhelming "the enemy through simultaneous or near-simultaneous actions."[145] All of these actions enable the governor and coordinating Title 10 forces to control tempo and regain the initiative. "By acting faster than the situation deteriorates, commanders can change the dynamics of a crisis and restore stability."[146]

## Conclusion

The current National Guard cyber capabilities should be fully integrated with DoD's overall cyber response. To accomplish this, DoD should authorize each state to move their CND-

[144] Ibid., 8.

[145] Ibid., 9.

[146] Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations* (Washington, DC: Government Printing Office, 2012), 55.

Ts from the state's TDA to unit Modification Table of Organization and Equipment and give them a federal mission trace. Affiliating the CND-Ts with the active component would give them a more specified role and bring all cyber forces under the same umbrella. Units that are currently performing cyber missions, primarily in the Air National Guard, should be aligned with active duty units and more fully integrated with their training and operations. Finally, DoD should approve the ten additional Title 32 CPTs and allow NGB to allocate them across the force. DoD should structure these teams along the lines of the Civil Support Teams and authorize full-time manning for the majority of the slots.

In addition to the reasons stated in this monograph for bringing the National Guard fully into the cyber mission force construct, there are also numerous advantages. It creates an opportunity to develop beneficial partnerships with cyber experts at state universities. The NSA and DHS have recognized many of these top university programs in the country through their Centers of Academic Excellence (CAE) program for Information Assurance and Cyber Defense.[147] Through Guard partnerships with these academic institutions, the state can increase its cybersecurity workforce. A pilot program in Mississippi placed elements of the states CND-T on campus. The team coordinates with faculty in the Computer Science program to better understand and train for threats to the state's critical infrastructure. Students also gain exposure to career opportunities and ways they could further use their skills.

Increasing the cyber capacity within the National Guard provides additional opportunities to recruit information technology experts into the total force. Many of these professionals have the necessary accreditations and training to begin working on cyber teams, but do not necessarily desire to serve in an active status. Joining the National Guard gives them an opportunity to put

[147] "National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)," National Centers of Academic Excellence, accessed December 09, 2014, https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

their skills to use in service of their country while giving them the flexibility to maintain their civilian jobs. Both organizations would benefit from the arrangement. Guard units would have highly skilled personnel who would receive most of their training through their civilian employer. Civilian companies would be able to leverage the experience their workers brought back in terms of lessons learned about current techniques and tactics by cyber actors.

Establishing a more direct link between the National Guard and active component provides a place for Soldiers who want to leave active duty, but still desire to serve in the military. Keeping them in the National Guard helps ensure their expertise is not lost while giving them the opportunity to continue to advance their skills through the civilian workforce.

A study of military history reveals numerous examples when the National Guard has been a key enabler of military operations. Throughout its history, the Guard has demonstrated its ability to integrate with the rest of the Army to help gain a position of relative advantage. To limit the National Guard in the CMF construct would be a mistake. In 1776, General Charles Cornwallis pursued General George Washington through the New Jersey countryside.[148] Through skillful maneuver, Washington managed to retreat with his Army across the Delaware River. Facing numerous obstacles, Washington sought for an opportunity to strike back against the British. The New Jersey and Pennsylvania militia created such an opportunity through harassing attacks against the Hessians at Trenton.[149] These attacks kept the Hessians in a "continuous state of alarm" and gave Washington the opening he needed to launch an attack across the Delaware

[148] David Hackett Fischer, *Washington's Crossing* (New York: Oxford University Press, 2004), 135.

[149] Ibid., 201.

River.[150] On the night of 25 December 1776, he crossed the river and captured the city of Trenton. This led to further successes at the second battle of Trenton and Princeton.

In the same way the militia attacks served as an enabling operation, the National Guard can help DoD better position itself to defend its networks as well as critical national infrastructure. Regardless of the current organization boundaries, the threat landscape has changed and DoD must change its approach if it wants to be in a place of relative advantage. Similar to the Nike missile program of the 1950s, the Guard is capable and ready to help defend the country against dangerous threats.

Governors and the Adjutant Generals are close to the front lines of future cyber attacks. They have and will continue to take steps to protect the critical infrastructure located in their state. In a complex environment, it is a mistake to not utilize a capability that is well placed and capable to aid in the defense against attacks. In the cyber domain, DoD must realize who is best placed to coordinate, prepare for, and respond to an attack. The enemy is not concerned about who is in charge or what the lines of authority are, they only hope that their attacks go unnoticed and achieve the desired results. The National Guard's integration into the larger DoD cyber forces is critical to developing an integrated web to catch these actors prior to an attack.

[150] Ibid.

# Bibliography

"About the National Governors Association." National Governors Association. Accessed December 07, 2014. http://www.nga.org/cms/about.

"Advanced Persistence Threat 1, Exposing One of China's Cyber Espionage Units." Mandiant.com. February 2013. Accessed September 12, 2014. http://intelreport.mandiant.com/.

Albright, David, Paul Brannan, and Christina Walrond. *Institute for Science and International Security Reports,* December 22, 2010. Accessed December 6, 2014. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

Anonymous. "Senators Push For National Guard Cyber Units In All States." *C4I News,* April 02, 2013. Accessed September 23, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com/docview/1326313140?accountid=28992.

Army Doctrine Publication 3-0, *Unified Land Operations*. Washington, DC: Government Printing Office, 2011.

Army Doctrine Reference Publication 3-0, *Unified Land Operations*. Washington, DC: Government Printing Office, 2012.

Army National Guard. *Concept of Operations, Computer Network Defense Teams*. 2014.

Arquilla, John, and David F. Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: Rand, 1997.

Baker, Caitlin. "Missouri National Guard Forms Cyber Response Team | Ksdk.com." Ksdk.com. January 11, 2013. Accessed November 11, 2014. http://www.ksdk.com/news/article/356592/3/Missouri-National-Guard-forms-cyber-response-team.

Bronk, Christopher, and Eneken Tikk. "The Cyber Attack on Saudi Aramco." Iiss.com. April 1, 2013. Accessed November 8, 2014. http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times*, October 11, 2012. Accessed November 09, 2014. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

Campbell, Scott. "Virginia Guard Data Processing Unit Conducts First Unit-level Cyber Defense Exercise." October 21, 2010. Accessed November 11, 2014. http://vko.va.ngb.army.mil/virginiaguard/news/oct10/DPUexercise.html.

Cardon, Edward C. "ARMY.MIL, The Official Homepage of the United States Army." 2014 Green Book: Army Cyber Command and Second Army. September 30, 2014. Accessed November 29, 2014. http://www.army.mil/article/134857/.

Chui, Michael, Markus Loffler, and Roger Roberts. "The Internet of Things." McKinsey & Company. March 2010. Accessed December 05, 2014. http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2010.

"Cyber Security Exercise, Heavy on National Guard, Completed." *US Fed News Service, Including US State News*, July 24, 2014. Accessed September 23, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com/docview/1547904646?accountid=28992.

"Cybersecurity Business Infrastructure Protection," Homeland Security News Wire. February 3, 2014. Accessed November 11, 2014. http://www.homelandsecuritynewswire.com/dr20140203-national-guard-units-help-states-ward-off-cyberat.

Doubler, Michael D., and John W. Listman. *The National Guard: An Illustrated History of America's Citizen-Soldiers*. Washington, DC: Brassey's, 2003.

Doubler, Michael D. *Civilian in Peace, Soldier in War: The Army National Guard, 1636-2000*. Lawrence, Kansas: University Press of Kansas, 2003.

Fischer, David Hackett. *Washington's Crossing*. New York: Oxford University Press, 2004.

Glazer, Emily. "J.P. Morgan's Cyber Attack: How The Bank Responded." MoneyBeat RSS. October 3, 2014. Accessed December 02, 2014. http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/.

Gorman, Siobhan, and Julian E. Barnes. "Iranian Hacking to Test NSA Nominee Michael Rogers." *Wall Street Journal*, February 18, 2014. Accessed September 01, 2014. http:/online.wsj.com/news/articles/SB10001424052702304899704579389402826681452.

Gorman, Siobhan. "NSA Director Warns of 'Dramatic' Cyberattack in Next Decade."*Wall Street Journal*, November 20, 2014. Accessed November 26, 2014. http://online.wsj.com/articles/nsa-director-warns-of-dramatic-cyberattack-in-next-decade-1416506197.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013.

"GuardNet XXI." *Stand-To!*, July 31, 2014. Accessed November 23, 2014. Http://www.army.mil/standto/archive_2014-07-31/?s_cid=standto.

Heilman, Marshal. *Mandiant South Carolina Department of Revenue Public Incident Response Report*, November 20, 2012. Accessed December 11, 2014. http://governor.sc.gov/Documents/MANDIANT%20Public%20IR%20Report%20-%20Department%20of%20Revenue%20-%2011%2020%202012.pdf.

"The Home Depot Reports Findings in Payment Data Breach Investigation." Home Depot Media Center, November 6, 2014. Accessed December 2, 2014. https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

Howard Anderson. "Utah Hack Attack: Lessons Learned." HealthcareInfoSecurity. April 13, 2012. Accessed November 08, 2014. http://www.healthcareinfosecurity.com/blogs/utah-hack-attack-lessons-learned-p-1244/op-1.

"Internet Users." Number of (2014). December 4, 2014. Accessed December 04, 2014. http://www.internetlivestats.com/internet-users/#trend.

"IRAN : World's 4th Cyber Army." *Pakistan Defence*, April 9, 2014. Accessed September 01, 2014. http://defence.pk/threads/iran-worlds-4th-cyber-army.308528/#ixzz3An0U1AkC.

"Israeli Missile Defense System 'Hacked' in Cyber Attack." August 2, 2014. Accessed September 01, 2014. http://www.almanar.com.lb/english/adetails.php?fromval=1&cid=23&frid=23&eid=163579.

Jensen, Ron. "Cyber Sense." *National Guard* 67, no. 6 (June 2013): 20-21. Accessed February 13, 2015. http://nationalguardmagazine.com/article/Cyber_Sense/1425297/162672/article.html.

Kambour, Andrew. *Enhancing the Cybersecurity of Energy Systems and Infrastructure*. Washington, DC: National Governors Association Center for Best Practices, 2014.

Keogh, Miles, and Christina Cody. *Cybersecurity for State Regulators With Sample Questions for Regulators to Ask Utilities*. National Association of Regulatory Utility Commissioners, 2013.

King, Rachel. "U.S. Defense Chief Warns of Digital 9/11." The CIO Report RSS, October 11, 2012. Accessed November 08, 2014. http://blogs.wsj.com/cio/2012/10/11/u-s-defense-chief-warns-of-digital-911/.

Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum, February 26, 2013. Accessed December 03, 2014. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Libicki, Martic C., David Sentry, and Julia Pollack. "Site-wide Navigation." Hackers Wanted: An Examination of the Cybersecurity Labor Market, 2014. Accessed December 11, 2014. http://www.rand.org/pubs/research_reports/RR430.html.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge, UK: Cambridge University Press, 2007.

Lively, Annie. *Understanding the Guard's Duty Status*. Accessed November 13, 2014. http://www.ngaus.org/sites/default/files/Guard%20Statues.pdf.

MacLellan, Thomas. *Act and Adjust: A Call to Action for Governors for Cybersecurity*. Washington, DC: National Governors Association Center for Best Practices, 2013.

Matthews, William. "Cyber Uncertainty." *National Guard* 68, no. 7 (July 2014): 24-29. Accessed September 30, 2014. http://search.proquest.com.lumen.cgsccarl.com/docview/1552463797?accountid=28992.

Matthews, William. "The Next Global War." *National Guard* 65, no. 6 (June 2011): 26-29. Accessed November 11, 2014. http://search.proquest.com.lumen.cgsccarl.com/docview/873280915?pq-origsite=summon.

Maynard, Melissa. "The National Guard Takes On Hackers." Stateline, January 28, 2014. Accessed December 06, 2014. http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/01/28/the-national-guard-takes-on-hackers.

"Michigan Leading the Effort Against Cyber Attacks." *Targeted News Service*, December 11, 2013. Accessed September 30, 2014.

https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/1466918474?accountid=28992.

Milord, Mike. "ARMY.MIL, The Official Homepage of the United States Army." Army Cyber Command, Army Guard Sign Memorandum to Integrate Cyber Protection Team, June 5, 2014. Accessed November 26, 2014. http://www.army.mil/article/127442/Army_Cyber_Command__Army_Guard_sign_memorandum_to_integrate_cyber_protection_team/.

Milord, Mike. "National Guard." Army Guard's First Cyber Protection Team Activated; Receives New Shoulder Sleeve Insignia Article View, October 10, 2014. Accessed November 26, 2014. http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/11413/army-guards-first-cyber-protection-team-activated-receives-new-shoulder-sleeve.aspx.

Minkel, JR. "The 2003 Northeast Blackout--Five Years Later." Scientific American Global RSS, August 13, 2008. Accessed November 09, 2014. http://www.scientificamerican.com/article/2003-blackout-five-years-later/.

Monahan, John J. "Guard Maps Plan for Y2K Emergencies." *Telegram & Gazette*, February 20, 1999. Accessed September 30, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/268714473?accountid=28992.

"National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)." National Centers of Academic Excellence. Accessed December 09, 2014. https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

"National Defense Authorization Includes Coons-authored Protection for National Guard Role in Cyber Missions." *Targeted News Service*, December 17, 2013. Accessed September 23, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com/docview/1468761701?accountid=28992.

"National Guard Units Help States Ward off Cyberattacks." *Homeland Security News Wire*, February 3, 2014. Accessed November 6, 2014. http://www.homelandsecuritynewswire.com/dr20140203-national-guard-units-help-states-ward-off-cyberattacks.

Pellerin, Cheryl. "United States Department of Defense." Defense.gov News Article: Cybercom Chief Details U.S. Cyber Threats, Trends, November 21, 2014. Accessed November 26, 2014. http://www.defense.gov/news/newsarticle.aspx?adbid=536685667267260418&adbpl=tw&adbpr=2596578505&cid=social_20141124_36030997&id=123696.

Poulsen, Kevin. "7-Eleven Hack From Russia Led to ATM Looting in New York | WIRED." Wired.com. December 21, 2009. Accessed December 11, 2014. http://www.wired.com/2009/12/seven-eleven/.

Prince, Brian. "Iranian Hackers Launching Cyber-Attacks on U.S. Energy Firms: May 13, 2013." Accessed September 01, 2014. http://www.eweek.com/security/iranian-hackers-launching-cyber-attacks-on-us-energy-firms-report/.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.

Ricker, Noknoi. "Maine National Guard Team Focuses on Protecting Cyber Networks." *Bangor Daily News*, July 16, 2014. Accessed September 23, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com/docview/1545554007?accountid=28992.

Riley, Michael. "How Russian Hackers Stole the Nasdaq." Bloomberg Business Week, July 17, 2014. Accessed December 02, 2014. http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

Rosenfeld, Susan, and Charles Gross. *Air National Guard at 60: A History*. Arlington, VA: Air National Guard, 2007.

Sanger, David E., and Eric Schmitt. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." *The New York Times*, July 26, 2012. Accessed November 09, 2014. http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=3&.

Sanger, David E., and Nicole Perlroth. "Cyberattacks Against U.S. Corporations Are on the Rise." *The New York Times*, May 12, 2013. Accessed September 01, 2014. http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all&module=Search&mabReward=relbias%3Ar%2C%7B%222%22%3A%22RI%3A14%22%7D.

Saporito, Laura. *The Cybersecurity Workforce: State's Needs and Opportunities*. Washington, DC: National Governors Association Center for Best Practices, 2014.

Schwartz, Mathew J. "How South Carolina Failed To Spot Hack Attack." Dark Reading, November 26, 2012. Accessed November 08, 2014. http://www.darkreading.com/attacks-and-breaches/how-south-carolina-failed-to-spot-hack-attack/d/d-id/1107515.

"Security News." PC Tools by Symantec. Accessed December 02, 2014. http://www.pctools.com/security-news/zero-day-vulnerability/.

"Significant Cyber Events." Center for Strategic and International Studies, August 7, 2014. Accessed September 01, 2014. http://csis.org/program/significant-cyber-events.

Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, UK: Oxford University Press, 2014.

"Symantec Corporation Internet Security Threat Report 2014," *Symantec Security Response Publications,* April 2014. Accessed December 1, 2014. Http://www.symantec.com/security_response/publications/threatreport.jsp.

"Testimony: National Guard Is Part of Cyber Security Solution." *US Fed News Service, Including US State News*, March 17, 2014. Accessed September 23, 2014. https://lumen.cgsccarl.com/login?url=http://search.proquest.com/docview/1507824331?accountid=28992.

"Top 9 Things You Didn't Know About America's Power Grid." Energy.gov, November 20, 2014. Accessed February 08, 2015. http://energy.gov/articles/top-9-things-you-didnt-know-about-americas-power-grid.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian,* May 16, 2007. Accessed February 3, 2015. Http%3A%2F%2Fwww.theguardian.com%2Fworld%2F2007%2Fmay%2F17%2Ftopstories3.russia.

US Congress. House. *American Energy Initiative*: *Hearing before The Subcommittee on Energy and Power*. 112th Cong., 1st sess., September 14, 2011.

_____. House. Cyber Warrior Act of 2013. H. Res. 1640, 113th Cong., 1st Sess. (2013).

_____. House. Electric Grid Vulnerability: Industry Responses Reveal Security Gaps. 113th Cong., 1st sess., 2013. H. Rept.

_____. Senate. Worldwide Threat Assessment of the US Intelligence Community. 113th Cong., 1st Sess., 2013, S. Rep, 1.

_____. Senate. Worldwide Threat Assessment of the US Intelligence Community. 113th Cong., 2nd Sess., 2014, S. Rep, 2.

US Department of Commerce. *Guide to Industrial Control (ICS) Security, (NIST Special Publication 800-82),* by Keith Stouffer and Suzanne Lightmann. May 2014.

US Department of Defense. *2005 National Defense Strategy*. Washington, DC: Government Printing Office, 2005.

_____. *2008 National Defense Strategy*. Washington, DC: Government Printing Office, 2008.

_____. *2010 Quadrennial Defense Review Report*. Washington, DC: Government Printing Office, 2010.

_____. *2014 Quadrennial Defense Review Report*. Washington, DC: Government Printing Office, 2014.

_____. *Army Directive 2012-08 (Army Total Force Policy)*. Washington, DC: Government Printing Office, 2012.

_____. Chairman, Joint Chiefs of Staff. National Military Strategy of the US. Washington, DC: Government Printing Office, 2011.

_____. *Department of Defense Directive 3025.18, Defense Support of Civil Authorities*. Washington, DC: Government Printing Office, 2010.

_____. *Department of Defense Directive 5105.77: National Guard Bureau*. Washington, DC: Government Printing Office, 2008.

_____. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Government Printing Office, 2011.

US Department of Homeland Security. Industrial Control Systems Cyber Emergency Response Team. *ICS-CERT Incident Response Summary Report for 2009 Thru 2011*. Accessed December 2, 2014. https://ics-cert.us-cert.gov/ICS-CERT-Incident-Response-Summary-2009-2011.

_____. *National Cyber Incident and Response Plan*. Washington, DC: Government Printing Office, 2010.

_____. *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: Government Printing Office, 2013.

_____. *National Strategy to Secure Cyberspace*. Washington, DC: Government Printing Office, 2003.

US President. "Fact Sheet: Presidential Decisional Directive 63, Critical Infrastructure Protection." (May 22, 1998).

_____. Presidential Decision Directive 63. “Critical Infrastructure Protection.” *Federal Register* 63, no. 150 (August 5, 1998): 41804-06.

US Strategic Command. “US Cyber Command Fact Sheet.” August 2013. Accessed December 06, 2014. http://www.stratcom.mil/factsheets/2/Cyber_Command/.

Walters, Riley. "Cyber Attacks on U.S. Companies in 2014." The Heritage Foundation. October 27, 2014. Accessed December 02, 2014. http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014#_ftn22.

Wood, Colin. "How the National Guard Is Protecting Cybersecurity." *Governing*. March 3, 2014. Accessed November 11, 2014. http://www.governing.com/topics/public-justice-safety/how-the-national-guard-Is-.html.