Strategy Research Project

Defining the DOD Role in National Cybersecurity

by

Colonel Mark R. Schonberg
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Defining the DOD Role in National Cybersecurity

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Mark R. Schonberg
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Brian H. Nussbaum
Center for Strategic Leadership and Development

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 7,531

14. ABSTRACT

Despite the almost universal acknowledgement of the cyber threats facing the United States, there exists no clear national consensus on how the country should unify cybersecurity efforts. The debate within Congress focuses around who should lead the nation's cyber efforts, but that may be the wrong discussion. The "right" discussion may be about what the nation can do quickly to secure cyberspace regardless of who is in charge of the effort. DOD, with its wealth of cyber expertise, needs to play an expanding role in addressing the nation's cybersecurity challenges. This SRP examines ways to proactively leverage DOD formations, resources, procedures, and industry partnerships along with all other U.S. government entities to dramatically improve the nation's cybersecurity posture. It argues the one federal agency within the government that is well postured to address cybersecurity is the DOD, and makes recommendations to address the country's cybersecurity concerns.

15. SUBJECT TERMS
Cyber, National Guard, Department of Homeland Security (DHS)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UU	UU	UU	UU	42	

USAWC STRATEGY RESEARCH PROJECT

Defining the DOD Role in National Cybersecurity

by

Colonel Mark R. Schonberg
United States Army

Dr. Brian H. Nussbaum
Center for Strategic Leadership and Development
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Defining the DOD Role in National Cybersecurity
Report Date:	March 2013
Page Count:	42
Word Count:	7,531
Key Terms:	Cyber, National Guard, Department of Homeland Security (DHS)
Classification:	Unclassified

Despite the almost universal acknowledgement of the cyber threats facing the United States, there exists no clear national consensus on how the country should unify cybersecurity efforts. The debate within Congress focuses around who should lead the nation's cyber efforts, but that may be the wrong discussion. The "right" discussion may be about what the nation can do quickly to secure cyberspace regardless of who is in charge of the effort. DOD, with its wealth of cyber expertise, needs to play an expanding role in addressing the nation's cybersecurity challenges. This SRP examines ways to proactively leverage DOD formations, resources, procedures, and industry partnerships along with all other U.S. government entities to dramatically improve the nation's cybersecurity posture. It argues the one federal agency within the government that is well postured to address cybersecurity is the DOD, and makes recommendations to address the country's cybersecurity concerns.

Defining the DOD Role in National Cybersecurity

> President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter.
>
> —The Comprehensive National Cybersecurity Initiative, 2010

As of June 2012, more than 2.4 billion people, or nearly a third of the world's human population, have used the Internet.[1] The estimated size of the worldwide digital economy in 2013 is $20.4 trillion, equivalent to roughly 13.8% of global sales.[2] Clearly, the world we live in today inextricably links U.S. prosperity and security to its global counterparts via the cyber domain.[3] However, even as you read this paper, attacks of unprecedented sophistication, emanating from a myriad of malicious actors target millions of computers that belong to the U.S. government, the private sector and to individual citizens. Gen Keith Alexander, the Commander of US Cyber Command (CYBERCOM) and Director of the National Security Agency (NSA), advised Congress that cyber threats to military and commercial sectors are growing, and that criminals have exploited 75 percent of our nation's computers.[4]

Despite the almost universal acknowledgement of the cyber threats facing the United States, there exist no clear national consensus on how the country should unify cybersecurity efforts. Currently, a debate rages on Capitol Hill whether a strategy led by the Department of Homeland Security (DHS), the Department of Defense (DOD), or, as many in Congress would prefer, the creation of a powerful "Cyber Czar" in the Executive Office of the President offers the best way forward. However, the debate over who should be in charge of the nation's cyber efforts maybe the wrong discussion. The "right" discussion may be what the nation can do to secure cyberspace regardless of

who is in charge of the effort. While this paper advocates changes to the status quo in regards to the leadership of the government's cyber efforts in its policy recommendations, it assumes a continuation of current policy where DHS serves as the lead cabinet agency for cybersecurity, and is responsible for protecting the federal executive branch civilian agencies and guiding the protection of the nation's critical infrastructure. This includes the "dot-gov" world, where the government maintains essential functions that provide services to the American people, as well as privately owned critical infrastructure that includes the systems and networks that support the financial services industry, the energy industry, and the defense industry.[5]

The DOD continues to manage its own internal networks and infrastructure (the "dot-mil"), while actively supporting DHS cybersecurity efforts. However, DOD, with its wealth of cyber expertise, needs to play an expanding role in addressing the nation's cybersecurity challenges. Recently, this need was illustrated when several major U.S. banks turned to the DOD, specifically the NSA, for help protecting their computer systems after a barrage of assaults that disrupted their Web sites.[6] This paper focuses on proactive leveraging of DOD formations, resources, procedures, and industry partnerships along with all other U.S. government entities to dramatically improve the nation's cybersecurity posture, and it will make the following specific recommendations for improvement.

1. Define Roles and Responsibilities; establish an Empowered Cyber lead
2. Develop Cyber Capabilities through the National Guard
3. Consolidating Cyber Operations and Government Cyber (IT) Infrastructure

4. Promulgate DOD Knowledge across the Government; Share with Private Sector
5. Safeguard and Leverage the Defense Industrial Base in order to Establish higher levels of Cybersecurity within the Private Sector
6. Ensure the Stand-Alone Survivability of the DOD Networks

A review of current policy and strategy documents designed to coordinate the government's efforts in addressing cybersecurity challenges, and the current cyber threats that shape these documents, helps frame these recommendations.

Existing National Cyber Security Policies and Strategies

An examination of the DOD role in a national cybersecurity strategy illustrates a clear need for the hard-earned and unique expertise DOD has developed being applied in support of the rest of government and the private sector. Therefore, it is essential to understand the President's, as well as other senior leaders, policy guidance and desired strategic direction. The country's cybersecurity policies and stratagems must be complimentary across the federal, state and local levels of implementation, and facilitate better cybersecurity in the private sector in order to safeguard our economic national interests.

The current National Security Strategy (NSS), published in May 2010, serves as the Obama Administration's cornerstone document for national security. It is important to note this is the first NSS to give real consideration to, let alone address, the cyber threats that face the country. The previous NSS, published by the Bush Administration in 2006, only once mentions the word cyber. The current NSS mentions the word cyber 24 times and dedicates an entire section to securing cyberspace. Clearly, the cyber

threat level, and its perceived importance to the nation, has risen dramatically within the past six years.

The NSS section on securing cyberspace perfectly illustrates the cyber dilemma facing the U.S., and for that matter the rest of the world. Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create, also produce vulnerabilities for us while simultaneously empowering those who would disrupt and destroy. They enable our military superiority, but allow intruders to continuously probe our unclassified government networks.[7] Additionally, the NSS declares the nations digital infrastructure a strategic national asset, and protecting it is a national security priority. It also addresses methods to achieve cybersecurity. It charges the country to deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by advancing two goals -- investing in people and technology, and strengthening partnerships.

In order to advance the goal of investing in people and technology, the NSS describes three key tasks:

> (1) Working across the government and with the private sector to design more secure technology that provides the ability to protect and improve the resilience of critical government and industry systems and networks.
>
> (2) Continue to invest in the cutting-edge research and development necessary for the innovation and discovery.
>
> (3) Implement a comprehensive national campaign promoting cybersecurity awareness and digital literacy; build a digital workforce for the 21st century.[8]

The second goal is strengthening partnerships. The NSS acknowledges it is necessary expand the ways for the government, the private sector, and individual citizens to work together to meet the cyber challenges. It also mandates strengthening our international partnerships on a range of issues, including the development of norms for acceptable conduct in cyberspace; laws concerning cybercrime; information assurance (including data preservation, protection, and privacy); and approaches for network defense and response to cyber attacks.[9]

Just as the NSS provides general guidance from the President on the country's overall approach to securing cyberspace, DOD produced policies and strategies direct its efforts in confronting cybersecurity challenges. The DOD has two key players within the cybersecurity arena: the National Security Agency, and U.S. Cyber Command. The 2011 National Military Strategy (NMS) directs Cyber Command to collaborate with U.S. government agencies, nongovernment entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills.[10] DOD also supports DHS efforts and homeland security functions. The NMS directs military support in response to an attack, cyber incident, or natural disaster, to rapidly provide planning, command and control, consequence management, and logistics support to the Department of Homeland Security, state and local governments, and non-governmental organizations.[11] This includes continuing to fund and train a portion of the National Guard to engage in homeland defense and defense support of civil authorities (DSCA) missions.[12] Although, it is not currently clear what role the National Guard plays in supporting requirements within the cyber domain.

Another key document covering DOD efforts in cyberspace is the 2011 DOD Strategy for Operating in Cyberspace, which examines DOD's strengths and opportunities within cyberspace and puts forth five strategic initiatives[13] to enhance cyber operations. The Strategy for Operating in Cyberspace also recognizes the U.S. Government's dependency on cyberspace. It states,

> The DOD, along with the rest of the U.S. government, depends on cyberspace to function. It is difficult to overstate this reliance; DOD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DOD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations.[14]

Additionally, the Strategy for Operating in Cyberspace emphasizes working with interagency and international partners to mitigate the risks posed to U.S. and allied cyberspace capabilities.

The other key agency involved with cybersecurity is DHS. The DHS Strategic Plan for Fiscal Years 2012-2016 lists Safeguarding and Securing Cyberspace as one of its five critical missions. DHS strategic plans and policies view today's threats to cybersecurity as requiring the engagement of the entire society to include all levels of government, law enforcement, the private sector, and members of the public in order to mitigate malicious activities while bolstering defensive capabilities.[15]

To facilitate the accomplishment of the agency's cyber mission, DHS released a mission-level strategy entitled *the Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise.* The Blue Print calls for a coordinated effort across the homeland security community to protect our nation's critical information infrastructure and promote technological advances that enable government, the private sector, and the public to be safer online.[16] The DHS long-range

cyber end-states include a cyberspace that advances economic interests and national security, and enables economic competitiveness and national defense. DHS also seeks a healthy cyber "ecosystem"[17] that facilitates performance of the other homeland security missions: the prevention of terrorism; border security; enforcement of immigration laws; and resilience to disasters. Furthermore, through partnership with the DOD, a secure cyberspace supporting the governments' execution of its critical national defense mission responsibilities.[18]

Taken together, these documents represent the over-arching U.S. policy on Cyber security. Both DHS and DOD, as well as other government agencies, possess multiple publications providing additional guidance, typically at lower (operational and tactical) levels.

Cyber Threats

Unlike the visible threat of an enemy tank or plane, which are easily defined and categorized. Cyber threats exist in a domain we cannot directly see or touch. Therefore defining and measuring these threats becomes challenging. The DOD Strategy for Operating in Cyberspace focuses on a number of central aspects of the cyber threat; these include external threat actors, insider threats, supply chain vulnerabilities, and threats to DOD's operational ability.[19] By comparison, civilian security experts identified four general categories of major cyber threats faced by the public and private sector. They are: nation-state intrusions; criminal (which extends to sophisticated organized crime); "hackivism"; and insider attacks.[20] For simplicity and evaluation, this paper groups the myriad of different cyber threats into two groups: state or quasi-state actors, and non-state actors.

State actor threats in cyberspace refer to organizations such as China's new People's Liberation Army Cybersecurity Squad[21] and its affiliated official, civilian, and semi-civilian proxies. Since the early 1990s, China has taken cyber warfare seriously, and not just in the realm of espionage. In 1999, PLA Colonels Qiao Liang and Wang Xiangsui argued that, were a showdown over Taiwan to occur, Chinese hackers could ravage American civilian infrastructure to offset U.S. military superiority.[22] Government supported hackers are even more worrisome. In China, these freelance hackers appear organized in a manner that allows the state to direct, or at least oversee and guide, their quasi-state affiliated activities. The cyber threat from countries, such as Russia, is much less government coordinated. The power dominating cyber capability in the Russian Federation is organized and controlled by criminal groups, sometimes independently and sometimes in conjunction with governmental oversight.[23] Non-state actor threats consist of three subgroups: malicious organizations, activists, and insider threats.

Perhaps the greatest daily cyber threat to the U.S., mainly the economy, comes from malicious organizations. Whether in the form of a terrorist group such as Al Qaeda, organized crime syndicates, or multi-national corporations engaged in espionage, numerous actions, such as those examined below, from these types of groups affect cyberspace daily.

The discovery of a new malware, dubbed Gauss, points to a new wave of cyber attacks sweeping the Middle East and North Africa region. The virus has been found in Windows 32bit systems, with the majority of cases being discovered in Lebanon, Israel and Palestine. Designed to capture login details for Internet banking services, Gauss

has had a particular focus on Lebanese banks although PayPal and Citibank have also been targeted.[24]

Transnational Criminal Organizations (TCOs), such as the "Brother's Circle," a multi-ethnic criminal group composed of leaders and senior members of several Eurasian criminal groups largely based in countries of the former Soviet Union but operating in Europe, the Middle East, Africa and Latin America[25], are increasingly involved in cybercrime.

Cybercrime costs consumers billions of dollars annually, threatens sensitive corporate and government computer networks, and undermines worldwide confidence in the international financial system. Some estimates indicate that online frauds perpetrated by Central European cybercrime networks have defrauded U.S. citizens or entities of approximately $1 billion in a single year.[26]

Corporate espionage also greatly impacts cybersecurity efforts. In 2011, at least five multinational oil and gas companies suffered computer network intrusions. The focus of the intrusions was oil and gas field production systems, as well as financial documents related to field exploration and bidding for new oil and gas leases.[27] This one cyber attack engaged two different targets, and illustrates the complexity often require in corporate responses. One attack can present numerous different problems each with different solutions.

Empowered by the internet and the ability to leverage hundreds of thousands, if not millions, of like-minded people in support of their cause, activist and activist organizations are thriving in the Internet age. While most activist groups simply use the internet to improve their messaging capabilities and group organization, some activist

groups are starting to use the internet as the platform for their protests. They are referred to as “hacktivists” – a conjoining of the terms “hacker” and “activist.” Hacktivism is the use of computers and computer networks as a means of protest to promote political ends.[28] As more governments and companies move their operations online, the Internet becomes an increasingly attractive place to conduct a protest. For example, hackers conducted a coordinated campaign of attacks on several Israeli Web sites during the recent Israeli-Palestinian conflict, which occurred during the November 2012 timeframe.[29]

Infiltration of the U.S. Government and America’s private sector by adversaries or disgruntled employees (the insider threat) is not a new trend. However, the level of access and ease of compromise is definitely new, as is the ability to download terabytes of proprietary or sensitive material at a keystroke. Imagine the effort, as recent as 30 years ago, to copy a company’s research and development data. It would have taken days, weeks or months to copy or photograph thousands of paper documents. The same volume of copying can be accomplished today in a matter of seconds, and stored on a thumb drive that fits on a key chain. The culprit does not need to even be physically present, cyberspace has enabled virtual pathways that allow for the exploitation of key data in an almost risk free environment. A recent survey from *E-Crime Watch*, revealed that current or former employees and contractors are the second greatest cybersecurity threat (to businesses), exceeded only by hackers.[30]

While numerous variants exist of these cyber threats, the necessity for the U.S. government to address vulnerabilities and the concerted efforts of malicious actors to exploit its networks and systems remains unchanged. Low barriers to entry for

malicious cyber activity, including the widespread availability of hacking tools and tutorials online, means that an individual or small group of determined cyber actors can potentially cause significant damage to U.S. national and economic security. [31]

Within this current cybersecurity environment - one lacking interagency unity of effort, coordination between agencies of the government and private industry, and of excessively restricted budgets - there are simple steps the DOD can implement to support the improvement of the country's overall cybersecurity posture.

Recommendations

The combination of limited fiscal resources and the real and relevant threats within cyberspace demand the development of new, and the alteration of current, policies and strategies. In fact, not only is it important to approach the cybersecurity challenge in a manner that does not require a large influx of funds, but additional resourcing may not solve the problem. A Bloomberg survey of the utility, telecommunication, financial services, and health care industries revealed that technology managers in 124 companies, each with at least 10,000 workers, said they could double spending on cybersecurity and yet their networks would remain vulnerable.[32] There are however potential ways to improve the Nation's overall cybersecurity posture, focusing on the proactive leveraging of DOD formations, resources, procedures, and industry partnerships.

Define Roles and Responsibilities; Establish an Empowered Cyber Lead

It is critically important for the U.S. Government to establish a National Cyber Coordinator (NCC) to unify, manage, and lead the efforts of the country's cyber community. The NCC would develop policies and strategies for the public and private sector in coordination with the President and Congress, as well as state and local

officials. The establishment of a NCC goes a long way toward addressing the most confusing part of the whole cyber dilemma, which revolves around the roles and responsibilities of the participants. Depending upon the interpretation of a cyber event, multiple entities could claim the lead. Was the cyber incident an attack on our government from a state sponsored cyber organization, or was it a criminal action conducted by a TCO? Did it target the private sector, or the Defense Industrial Base (DIB)? One event could easily be interpreted multiple ways. In such a vague environment, confusion and the lack of a cohesive effort amongst government organizations are all too commonly the outcome.

To address concerns over the country's efforts in securing cyberspace, the White House directed a Cyberspace Policy Review. The review found the Federal government is not organized to address this growing problem effectively now, or in the future. Responsibilities and capabilities for cybersecurity are unevenly distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way.[33]

To be fair, the Obama Administration has attempted to implement measures designed to address Cyber coordination, such as the appointment of the first White House Cybersecurity Coordinator. Additionally, in October of 2010 DOD and DHS signed a memorandum of understanding that allowed NSA to support Homeland Security cybersecurity efforts and established a personnel exchange between the agencies.[34] The lack of authority allocated to the Cybersecurity Coordinator relegates it to a position of little relevance. While a step in the right direction, the DHS/DOD

memorandum does little to address the entire government. Even today, three years after the policy review, the responsibility for a federal cyber incident response is dispersed across many federal departments and agencies because of the existing legal distinctions between national security and other federal networks. Although each player has defined areas of expertise and legal authorities, they are difficult to pull together into a single coordinated structure or response.[35]

Although it seems everyone recognizes the problem, Congress and the President have been unable to achieve a way forward. The 112th Congress failed to enact any significant cyber legislation. This may be in part because no single congressional committee or executive agency has primary responsibility for cybersecurity issues. Within the Congress there appears to be two primary schools of thought; either a DHS lead or DOD lead approach.[36] The DHS approach argues that a credible civilian government cybersecurity capability cannot originate from an intelligence organization like the NSA. The DOD proponents view the NSA and US Cyber Command as excellent capabilities, far superior to any alternative that could be utilized immediately to protect public and private networks.[37]

The DOD already has responsibility for defending its own systems, and has been forward leaning in establishing policy and making organizational changes for cybersecurity.[38] Advocates of a greater role for NSA say it is the only organization with the capability and monitoring infrastructure to protect U.S. computer networks, and that NSA's current support role to Homeland Security will not get the job done.[39] However, the drawbacks of placing DOD in charge of cybersecurity are numerous. The legal restrictions of the Posse Comitatus Act on domestic activity by military forces represent

only the most basic of issues; though their meaning and implications in the cyber realm remain far from clear. The department lacks regulatory authority and law enforcement power, and is in fact prohibited from engaging in domestic law enforcement under most circumstances.[40] It is also a drastic departure from the department's primary mission of fighting and winning the nations wars, and prompts many to ask how far is the leap from the military virtually guarding the country's critical infrastructure to physically guarding the country's critical infrastructure. Current government plans call for DOD and its subordinate services (mainly the Army and Marines) to reduce in size roughly 6% through 2017,[41] therefore giving the burden of new cybersecurity missions to the DOD would seem misplaced. Additionally, DOD networks, while arguably the most secure within the U.S. Government, are not impervious and have been penetrated numerous times.[42] So if not DHS or DOD, then who should lead the country's cyber efforts?

Establishing a unity of effort across the government and private sector is a daunting task, but the first step needed to achieve the synergy necessary to address securing cyberspace involves identifying someone to lead the effort. To answer the "who," we need only look to the aftermath of 9/11 when the U.S. faced a similar situation involving the intelligence community's failures. Faced with the need to coordinate the country's different intelligence groups spread across numerous cabinet departments, Congress and the President passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which established the Office of the Director of National Intelligence (DNI) to better unify and manage the efforts of the Intelligence Community (IC). The DNI supervises an organizational staff of 1500 personnel and oversees the 16 federal organizations that make up the IC. In doing so, he organizes and coordinates the

efforts of the IC agencies. The DNI also manages the implementation of the National Intelligence Program and serves as the principal adviser to the President and the National Security Council on intelligence issues related to national security.[43] A similar template should be applied to cybersecurity.

While many have proposed the establishment of a National Cyber Coordinator (NCC) or a Director of National Cybersecurity,[44] it is important to note most fail to examine it in a "whole of government" concept. Legislative reforms vesting legal authorities and control over governmental cyber organizations are essential to establishing an effective NCC. The creation of new Congressional committees within the House and Senate are necessary for oversight of budgets and accountability. Unlike Intelligence, which is rather narrow in its definition, cyber cuts across almost all aspects of the public and private sector. It includes portions of telecommunications and information technology sectors as part of its scope. Cyber decisions at the State and Local levels can have impacts at the National level. Therefore, building an effective NCC element may prove significantly more challenging than the creation of the DNI, but it will establish a definitive focal point for resolution (or at least directing the discussion) of cyber issues and coordinate the government's efforts.

Develop Cyber Capabilities through the National Guard

One of the most successful programs involving a coordinated Federal and State approach to managing critical threats was the formation of the Weapons of Mass Destruction Civil Support Teams (WMD-CSTs). The Guard's WMD CSTs were established in 1998 by President Clinton with support from Congress in recognition or the potential WMD threat that the U.S. faced. [45] The WMD CSTs were designed to support state and local civil authorities in WMD events, and serve as rapid response

teams. Comprised of 22 highly skilled, full-time Army and Air Guardsmen, these teams include guardsmen with specialized backgrounds in science, medicine and hazardous materials.[46]

The WMD CSTs are federally resourced, trained, and evaluated. However, they perform their missions mainly under the command and control of the State Adjutant Generals. WMD CSTs can quickly respond to a WMD incident as part of the state response. From October 2011 through March 2012, WMD CSTs engaged in 51 incident responses, 349 standby missions and 685 assist missions, in addition to their regular exercises and training. The Guard's WMD-CSTs participate in a minimum of 12 collective training exercises or regional training events per year.[47]

The recommendation for the establishment of a National Cyber Coordinator proposed utilizing the template already executed in the creation of the Director of National Intelligence. Similar to this line of thinking, DOD (with Presidential approval and in cooperation with Congress and State Governors) should establish Cyber Civil Support teams (Cyber CSTs) to address cybersecurity concerns. DOD is already required to support the National Cyber Incident Response Plan. During an incident, DOD provides Defense Support to Civil Authorities (DSCA) when requested and, in close coordination with DHS, shares threat information with the State National Guard and other State-level partners in accordance with applicable statutory authorities and established protocols.[48] The establishment of Cyber CSTs within each state would facilitate unity of effort and the rapid dissemination of information across all levels of government.

Currently, the Guard is working to develop its response capability to the Cyber threat, and is pushing to form an increasing number of special cybersecurity units.[49] What remains unclear is the exact mission and focus of these cyber organizations. Are they intelligence focused, defense focused, or network operations focused? The traditional DOD mission of fighting and winning our nation's wars does not directly enhance cybersecurity for the country.

For example, the Washington National Guard is leveraging a decade of investment in cyber security into projects that could protect state and local governments, utilities and private industry from network attacks. The aim is to bring to the digital world the kind of disaster response the National Guard already provides.[50] Unfortunately, the establishment of these uncoordinated state-sponsored units is almost a step backwards. Who equips, mans, trains and certifies this type of an organization? How might this unit be integrated into overall federal cybersecurity efforts by the DOD?

Numerous parallels already exist between the present WMD CSTs and the proposed Cyber CSTs that can address many of these questions. Both require highly technical skill sets and certifications at the individual and team level. The DOD would supervise the equipping, funding, manning, training and certification of all teams. When responding to an event, they are capable of seamlessly transitioning from the local level through to the federal level. There will always exist the option of federalizing the CSTs if necessity dictates, using the same process associated with regular National Guard units. Their dispersed locations provide the ability to respond rapidly, and gain situational awareness. While there are definitely some noticeable differences - such as

WMD events being geographically confined to certain locations while cyber incidents are less so - the similarities are worth examining.

Even within the DOD cyber community there exist little consensus on what form cyber force structure should take, and at what level it should reside: strategic, operational, or tactical. As the Air Force and Army struggle to find the right structures to embed in their active and reserve components, the Cyber CSTs could easily stand outside of the traditional structure with the intent of being State-level directed. While other Cyber formations could be activated and deployed, the Cyber CST scenario essentially maintains a constant presence within their assigned State. In fact, neither the Air Force, nor the Army cyber doctrine[51] specifically addresses roles and responsibilities for National Guard formations. The Cyber CST is one way of addressing the Guard role, but there could certainly be others.

Congressional legislation similar to that associated with the WMD CSTs would be essential in order to define relationships and structure. However, the precedence exists to rapidly execute this idea. Congress already appears to desire more Guard involvement with cyber; the fiscal year 2012 National Defense Authorization Act (NDAA) directs the study of Reserve Component personnel needed to support cybersecurity.[52]

The end-state for Cyber CSTs would consist of a full-time, federally funded National Guard unit that supports state and local civil authorities in responding to events known or suspected to involve malicious cyber activity. They would be nationally directed (DOD and the designated Service lead responsible for manning, equipping, training and certifying every team), State aligned (each state would possess at least one Cyber CST), and locally responsive. Additionally, the location of the Cyber CSTs would

promulgate federally established standards throughout State and local government, and add flexibility to the nation's overall cybersecurity posture.

Consolidating the Government's Cyber Operations and Cyber (IT) Infrastructure

Similar to the benefits derived from establishing centralized leadership for coordinating and directing the government's cyber efforts via a National Cyber Coordinator, there exist operational benefits to be gained by consolidating resources and infrastructure across the government. Specifically, the co-location of numerous operations centers, such as the United States Computer Emergency Readiness Team (US-CERT) and the NSA operations watch. The DOD has already achieved the co-location of the NSA and CYBERCOM at Fort Meade. DHS, which originally considered Fort Meade, established the US-CERT in Alexandria, Virginia. The Department of Justice (DOJ) and the Federal Bureau of Investigations (FBI), another of the governments key cyber players, distributed their cyber capabilities in the form of cyber squads spread across 56 field offices. There exist liaisons between the government's cyber players, and efforts have been made to address the gaps in authorities and information sharing, most notably the FBI led National Cyber Investigation Joint Task Force (NCIJTF). However, the process remains inefficient. A recent FBI audit on the agency's ability to address the National Security Cyber Intrusion Threat found the FBI, through the NCIJTF, was not always sharing information about cyber threats among the participating partner agencies.[53]

Co-location is not meant to imply there would be a merger of group functions; the DOJ and FBI would remained focused on law enforcement and legal matters, NSA and DOD on military objectives and intelligence, DHS on homeland security, and the other Departments, such as Treasury and Commerce, on their appropriate areas. However,

establishing a common situational awareness amongst the key cyber players facilitates cooperation and open collaboration in the execution of their missions. The ability to rapidly respond to cyber threats is vital.

To illustrate why co-location is important, let us examine a ***fictional*** cyber threat scenario.[54] The Marine Forces Cyber Command located in Quantico is alerted to an attempt to penetrate their network emanating from Japan. Unfortunately, they do not possess the ability to trace the origin of the attack. They pass their report to CYBERCOM, who immediately coordinates with the NSA. The NSA, with their advanced intelligence tools, trace the origin of the attack across multiple countries and finally deduce the attempted penetration is occurring from a coffee shop located in Carlisle, Pennsylvania. The attack appears designed to ultimately access Department of State (DOS) networks, rather that those of the Marine Corps, even though the Corps is its target. Given that the incident originated within the U.S., and the culprit may well be a U.S. citizen engaged in illegal activities, NSA is reluctant to pursue the matter any further as the lead agency. They coordinate for the issue to be turned over to the FBI for further investigation. Since the attack was designed to infiltrate the DOS network (in the "dot-gov" rather than "dot-mil" domain) via the DOD network, DHS, which is responsible for all government networks outside the DOD, becomes involved. DHS may wish to block the attack immediately, but the FBI requires the situation to develop longer in order to collect evidence, build a case, and apprehend the suspected criminal. All that coordination and the associated decisions need to happen in a matter of seconds. Technological solutions can certainly stop malicious actions when detected, but it cannot understand and potentially exploit those actions for intelligence or law

enforcement information or purposes. Human interaction is required, and by co-locating all the government's cyber operations together, we reduce some of the barriers to interagency cooperation and collaboration.

Nested within the concept of consolidated cyber operations is the concept of consolidated government Information Technology (IT) infrastructure. This relationship revolves around the premise that government IT infrastructure resides within and is part of cyber domain, and is therefore accessible to all actors that operate in cyberspace. In August 2010, Secretary of Defense Gates directed the consolidation of IT infrastructure to achieve savings in acquisition, sustainment, and manpower costs and, most importantly to this paper, to improve DOD's ability to execute its missions while defending its networks against growing cyber threats.[55] This effort resulted in a direct budget reduction of $1.7 billion for the DOD in 2012.[56] Historically, government IT investments were executed to support a hodgepodge of individual projects, programs, organizations, and facilities. This decentralized approach resulted in a patchwork of capabilities that have interoperability issues, and created cyber vulnerabilities. However, today we have the technology available to remove the current unnecessary complexity from federal cyber networks and infrastructure.

The DOD's cyber consolidation effort should serve as the template for an ambitious federal government effort. Presently, DOD spends more on IT annually than any other department or agency ($37 billion), accounting for almost half of the $78 billion government-wide IT budget in 2010.[57] Infrastructure consolidation would reduce the total amount of federal resources dedicated to maintaining the cyber infrastructure, and, if executed properly, could standardize all government assets that touch

cyberspace. Such standardization would allow for a dramatic increase in the overall federal cybersecurity posture, and the fiscal savings could potentially to be reinvested in mitigating or eliminating existing vulnerabilities. Optimally, consolidation would be implemented through the NCC concept, but could be achieved through a series of Presidential directives and legislative actions.

Promulgate DOD Knowledge across the Government; Share with Private Sector

As discussed earlier, one of the key themes within the NSS involves implementing complimentary cybersecurity policies and stratagems across the federal government, and facilitating better cybersecurity at the state and local levels, as well as within the private sector. DOD already possesses three key aspects necessary to achieve these tasks: (1) a well-structured cyber/IT professional training and certification program, (2) an information systems certification program, and (3) a robust employee cyber education program. Examination of these three capabilities will illustrate why distributing this knowledge across the government, and through private sector, offers a relatively quick and straightforward method to improve cybersecurity.

Whether the Chief Executive Officer of an aerospace engineering company or the Under Secretary for Homeland Security, most senior leaders lack the knowledge necessary to effectively manage their cybersecurity issues. They recognize the importance of cybersecurity, but do not understand cyber threats, vulnerabilities, and their possible impacts of cyber incidents. The fact that email is routed to servers beyond your organizations networks, and often beyond national borders is simply not understood. A recent National Counterintelligence Executive report cited only 5 percent of corporate chief financial officers are involved in network security matters.[58] Typically, leadership relies on members of their IT department to select qualified personnel, but

this method is purely subjective. Recognizing this dilemma, the DOD developed specific guidelines for its cyber professionals.

DOD Directive 8570 provides guidance and procedures for the training, certification, and management of all government employees who conduct cyber (in this case specific to information assurance) functions in assigned duty positions. The type of job, the level of management responsibility, and the local supervisors input all facilitate the development of minimum certification requirements. The certifications are exactly the same as the private sector. For example, a DOD network engineer is required to be Cisco engineer certified. Failure to achieve or maintain the appropriate certifications can lead to job termination. Ideally, 8570 helps non-cyber managers identify their requirements and develop the appropriate workforce. By using common IT industry standards for certification, DOD maintains synergy with the standards adopted in the private sector. Sharing these processes across the rest of the federal government will ensure a common quality within the cyber/IT workforce.

Similar to the personnel certification program, DOD also implements an information systems certification program. The DOD Information Assurance Certification and Accreditation Process (DIACAP) is designed to ensure that risk management is applied on information systems (IS). The DIACAP defines a standard set of activities, general tasks and a management structure process for the certification and accreditation of DOD information systems. Fundamentally, the DIACAP supports the transition of DOD information systems to common standards for certification and accreditation. These standards, which include guidance on managing and disseminating enterprise standards for information assurance design, implementation,

configuration, validation, operational sustainment, and reporting,[59] are easily transferable to the rest of the federal government. Additionally, the DIACAP can help facilitate private sector evaluation of the information systems and the associated risks.

DOD also possesses a robust employee education program designed to illuminate the cyber threat to the workforce. At a minimum, all DOD members are required to receive annual information assurance training. These educational products have been tailored and refined over the last two decades, and provide excellent insights to the risks associated with government information systems. Training addresses many of the techniques used by foreign intelligence services, such as social engineering and phishing; these techniques are increasingly used against non-DOD government networks and private sector entitities. A trained and aware workforce is vital to a success defense against the cyber threat. The National Counterintelligence report on foreign economic collection and industrial espionage noted companies that successfully manage the economic espionage threat realize and convey to their employees the threats to corporate data. [60] Additionally, the development of these educational products in an expensive endeavor. In 2011, the Army spent $2.6 million on required annual training just for the 40,000 Soldiers and Civilians located in Europe.[61] Sharing these training programs across the federal government could potentially decrease costs to DOD through economies of scale (thus incentivizing their participation) and will ensure a common quality and level of training.

Safeguard and Leverage the Defense Industrial Base in Order to Establish Higher Levels of Cybersecurity within the Private Sector

The Defense Industrial Base (DIB) is under cyber attack every day. The Defense Security Service reports the overall number of economic espionage and cyber intrusion

incidents submitted by cleared industry[62] in 2011 increased by nearly 65 percent over 2010.[63] The DIB is one of the eighteen critical infrastructure sectors under the National Infrastructure Protection Plan (NIPP), a DHS created program. However, DOD is assigned as the Sector Specific Agency (SSA) for the DIB. Given DOD's particular dependence on the DIB to provide equipment and ensure readiness, the need for DOD and DHS to partner with this part of the private sector against the threats they face is especially crucial.

DOD has consistently worked with the DIB to increase the protection of sensitive information. In 2007, DOD launched the Defense Industrial Base Cyber Security and Information Assurance program (DIB CS/IA). The DIB CS/IA Program includes a voluntary information sharing component under which DIB companies and the Government agree to share cyber security information out of a mutual concern for the protection of sensitive but unclassified information related to DOD programs on DIB company networks.[64] Building upon this program, DOD is working in coordination with DHS to pilot a public-private sector relationship intended to demonstrate the feasibility and benefits of voluntarily increasing the sharing of information about malicious or unauthorized cyber activity and protective cyber security measures.[65]

These initiatives, while a step in the right direction, are often awkward and slow. As illustrated earlier, the lack of centralized direction by the federal government in regards to cybersecurity complicates the process. Corporate security officers told the National Counterintelligence Executive that U.S. Government reporting procedures on economic espionage and cyber intrusions are cumbersome and redundant. Agencies such as Defense Security Service and the FBI often seek the same information, but in

different formats.[66] Coordination of this kind of reporting should not be difficult. Additionally, the volunteer nature of the program calls into question its effectiveness. The number of cyber incidents reported depends exclusively upon the DIB communities input. Companies are likely to report successful blocks against attempted breaches, but less likely to report breaches that may cast unwanted attention to poor security practices.

In order to ensure effectiveness, the federal government needs to adopt some form of regulation to ensure cybersecurity standards are implemented within the DIB. Mandated standards for the DIB ideally facilitate the spread of those standards to other parts of the private sector. The DOD, as the government's largest consumer, needs to make cybersecurity part of the overall business cost for suppliers. The DIB will almost certainly continue to be the prime target of foreign intelligence entities seeking to obtain the latest technologies. The current environment must change; voluntary compliance is no longer an acceptable option.

Ensure the Stand-Alone Survivability of the DOD Networks

One of the more difficult concepts to grasp in the cyber domain is that of shared infrastructure. The router or switch that provides internet access to your home may also be processing information from anywhere around the world. There is no doubt that shared IT infrastructure has dramatically reduced the cost of conducting business in cyberspace. The price of a local phone line in 1986 averaged $47.91.[67] By 1995, the price dropped to $43.33, and today a local phone line from AT&T costs around $30. Within the financially constrained "peace dividend" environment of the 1990s, DOD started to move away from costly stand alone IT voice and data networks to an approach centered around leasing cheaper commercial voice and data networks.

Unfortunately, today the vast majority of US critical cyber infrastructure is owned by the private sector.[68]

This reality seems to conflict with the guidance given in the NMS, which directs DOD Joint Forces to secure the '.mil' domain, and requires a resilient DOD cyberspace architecture that employs a combination of detection, deterrence, denial, and multi-layered defense.[69] Twenty-five years ago, the concept of cyber threat, or a cyber attack, was an issue of interest to really only a few researchers in academics. In this post-9/11 era, the cyber threat is serious, and poses a significant risk to U.S. economic and National security.[70]

In this new era, it is essential for the DOD to implement ways to reduce its dependence on Private IT Infrastructure. While it may be financially impossible, and to a large extent undesirable, to recreate the stand-alone voice and data networks of days past; procurement of key IT infrastructure necessary to ensure DOD can operate effectively, even in the event of a massive cyber attack, is prudent. Purchasing of existing physical infrastructure, such as fiber optic cable or data and voice switches, required to link key nodes of leadership is achievable in a fairly short amount of time. However, neither the current Department of Defense Strategy for Operating in Cyberspace, nor the Department of Defense Information Technology Enterprise Strategy Roadmap addresses the reliance on private cyber infrastructure. In order to effectively counter the risks posed by cyber threats, this paradigm must shift slightly back to the old, and more expensive, way of conducting operations.

Conclusion

In May 2009, President Obama accepted the recommendations of the first thorough review of federal efforts to defend and secure the cyber domain. Prior to 2009

Cybersecurity simply was not a focus of the federal government (at least not in a comprehensive government-wide approach). As the malicious actors developed increased capabilities and the country awakened to the real threat within cyberspace, the government's response has been slow, uncoordinated, and often ceded initiative to our opponents. However, the one element within the government that is well postured to address cybersecurity is the DOD.

In fact, DOD not only recognized the seriousness of the cyber threat well in advance of the rest of the government, it has reorganized to address the threat. Organizations such as the NSA and CYBERCOM possess an unparalleled wealth of cyber expertise, and because of this capability DOD is obligated to support all other U.S. government entities, as well as the private sector, in the quest to improve the nation's cybersecurity posture. The recommendations of this paper either follow an existing template or utilize recognized best business practices. They help address the country's cybersecurity concerns, and they fall within the authority of the government. Adoption of these recommendations certainly would improve the country's cybersecurity posture.

Costs associated with any new initiatives will meet with resistance during this time of shrinking government budgets and economic austerity, but we must look at cybersecurity as a long-term strategic investment and not a short-term cost. When compare with the catastrophic costs of not protecting our networks, such investments are actually fairly small. Perfect cybersecurity clearly is unachievable, however, the United States must strive to deter our enemies and ensure our resilience if attacked within cyberspace.

Endnotes

[1] *Internet World Stats,* Miniwatts Marketing Group, June 30, 2012, http://www.internetworldstats.com/stats.htm. (accessed February 15, 2013).

[2] Oxford Economics, *The New Digital Economy: How it will transform business,.(Oxford ,UK:* June, 2011), p.9, http://www.pwc.com/gx/en/technology/publications/assets/the-new-digital-economy.pdf (accessed February 15, 2013).

[3] The Cyber Domain definition is extremely vague within our national documents. It is defined by DOD as, "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures" (Peter Pace, *The National Military Strategy for Cyberspace Operations*, December 2006, ix). The Congressional definition is even wider, "cyberspace is the total interconnectedness of human begins through computers and telecommunication without regard to physical geography" (Steven Hildreth, *Cyberwarfare- Congressional Research Service Report for Congress*, (Washington, DC: U.S. Library of Congress, Congressional Research Services, November 15, 2000; updated June 19, 2001), 1).

[4] Gen Keith B. Alexander, "Hearing on National Defense Authorization Act for Fiscal Year 2012," Committee on Armed Services, US House of Representatives, H.A.S.C. No. 112–26, March 16, 2011, p.4

[5] Janet Napolitano, *Department of Homeland Security Strategic Plan Fiscal Years 2012-2016,* (Washington, D.C.: DHS, February 2012), 12.

[6] Ellen Nakashima. "Banks seek NSA help amid attacks on their computer systems." The Washington Post, January 11, 2013. http://articles.washingtonpost.com/2013-01-11/world/36272281_1_banks-ddos-nsa (accessed February 15, 2013).

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

[8] Ibid.

[9] Ibid., 28.

[10] M. G. Mullen, *The National Military Strategy of the United States of America,* (Washington, DC: CJCS, February 8, 2011), 10.

[11] Ibid.

[12] Ibid., 11.

[13] The five DOD Strategic Initiatives are: 1) Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential. 2) Employ new defense operating concepts to protect DoD networks and systems. 3) Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity Strategy. 4) Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity. 5) Leverage the nation's ingenuity

through an exceptional cyber workforce and rapid technological innovation. (Leon E. Panetta, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 14, 2011).

[14] Leon E. Panetta*, Department of Defense Strategy for Operating in Cyberspace (Washington, DC: U.S. Department of Defense, July 14, 2011),* 1.

[15] Ibid., 12.

[16] Ibid., 12.

[17] Cyber Ecosystem defined: The cyber ecosystem is global and includes government and private sector information infrastructure, the variety of interacting persons, processes, information and communication technologies, and the conditions that influence their cybersecurity. (Napolitano, *Department of Homeland Security Strategic Plan Fiscal Years 2012-2016,* 10).

[18] Janet Napolitano, *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise, (*Washington, D.C.: DHS, November 2011), 7.

[19] Leon E. Panetta*, Department of Defense Strategy for Operating in Cyberspace,* 3.

[20] James P. Farwell, "Industry's Vital Role in National Cyber Security," Strategic Studies Quarterly: Air University Press, (Winter 2012), 12.

[21] Beech, Hannah, "Meet China's Newest Soldiers: An Online Blue Army," Time Magazine, May 27, 2011, http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/ (accessed February 15, 2013).

[22] Erik Schechter, "Cyber Catch-up," March. 6, 2008, www.defensenews.com, http://www.defensenews.com/article/20080306/C4ISR01/803060306/Cyber-catch-up (accessed February 15, 2013).

[23] Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy - Changing the Zero-Sum Game," Strategic Studies Quarterly (Winter 2012), 100.

[24] *Cyber Terrorism: The Arab World's Invisible Threat,* KCS Briefing Paper, August 2012, http://sourcebase.wordpress.com/2012/08/17/cyber-terrorism-the-arab-worlds-invisible-threat/ (accessed February 15, 2013).

[25] Department of Treasury Office of Foreign Assets Control Specially Designated Nationals list, November 14, 2012, http://ofac-sdn-list-removal.com/ (accessed February 15, 2013).

[26] Barack Obama, *Strategy to Combat Transnational Organized Crime*. (Washington, D.C.: NSC, July 25, 2011), 7.

[27] John Markoff, "Hackers Breach Tech Systems of Oil Companies," New York Times, February 10, 2011, http://www.nytimes.com/2011/02/10/business/global/10hack.html?_r=0 (accessed February 15, 2013).

[28] *Examples of e-Crimes: Hacktivism*, e-Crime Wales, 2011, http://www.ecrimewales.com/server.php?show=ConWebDoc.1607 (accessed February 15, 2013).

[29] Nicole Perlrot, "Anonymous Steps Up Attacks on Israeli Sites," New York Times, November 16, 2012, http://bits.blogs.nytimes.com/2012/11/16/anonymous-steps-up-attacks-on-israeli-sites/ (accessed February 15, 2013).

[30] Matt Bishop and Deborah A. Frincke, "Combating the Insider Cyber Threat," IEEE Security & Privacy, January/February 2008, 61. www.cert.org/archive/pdf/combatthreat0408.pdf (accessed February 15, 2013).

[31] Leon E. Panetta*, Department of Defense Strategy for Operating in Cyberspace,* 11.

[32] James P. Farwell, "Industry's Vital Role in National Cyber Security," 14.

[33] Barack Obama, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* (Washington, D.C.: White House, May 2009), i.

[34] Janet Napolitano and Robert Gates, "Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," Washington,D.C., October 13, 2010, www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed 23 Jan 2013).

[35] Barack Obama, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* 23.

[36] James P. Farwell, "Industry's Vital Role in National Cyber Security," 17.

[37] James P. Farwell, "Industry's Vital Role in National Cyber Security," 23.

[38] Kevin P. Newmeyer, "Who Should Lead U.S. Cybersecurity Efforts?" Prism 3, No.2. (Washington, D.C.: NDU Press, March 2012), 121.

[39] Siobhan Gorman, "NSA Chief Seeks Bigger Cybersecurity Role," The Wall Street Journal, February 27, 2012, http://online.wsj.com/article/SB10001424052970203833004577247710881763168.html (accessed January 29, 2013).

[40] Kevin P. Newmeyer, "Who Should Lead U.S. Cybersecurity Efforts?," 121.

[41] Thom Shanker and Christopher Drew, "Pentagon Seeks Biggest Military Cuts Since Before 9/11," The New York Times, January 6, 2011, http://www.nytimes.com/2011/01/07/us/07military.html?_r=0 (accessed February 15, 2013).

[42] This observation is derived from my personal experience within DOD IT services for over the past 20 years. The DOD operation "Buckshot Yankee" is perhaps the greatest illustration of this kind of event. For more information visit: http://articles.washingtonpost.com/2011-12-08/world/35288364_1_agentbtz-malware-government-networks (accessed February 15, 2013).

[43] Intelligence.gov. http://www.intelligence.gov/about-the-intelligence-community/structure/ (accessed January 29, 2013).

[44] The idea of a National Cyber Coordinator or Director is not unique to this paper; several other writers have proposed the idea. The most in depth look I found during my research was provided by Kevin Newmeyer in his article "Who Should Lead U.S. Cybersecurity Efforts?" referenced within this paper (see endnote 38) and available online at: http://www.ndu.edu/press/us-cybersecurity-efforts.html (accessed February 15, 2013).

[45] Liza Porteus Viana, "Guard's WMD Civil Support Teams Can Respond Faster Than Other Federal Assets," Homeland Security Today, March 14, 2012, http://www.hstoday.us/briefings/correspondents-watch/single-article/guards-wmd-civil-support-teams-can-respond-faster-than-other-federal-assets/af2160975c8dc3d4ab7f17f0942bdcdc.html (accessed February 15, 2013).

[46] Ibid.

[47] Ibid.

[48] Janet Napolitano, *National Cyber Incident Response Plan, Interim Version*. (Washington, D.C.: DHS, September 7, 2010), C-2.

[49] Homeland Security News Wire, "National Guardsmen, the new front line in cybersecurity," December 19, 2011, http://www.homelandsecuritynewswire.com/dr20111219-national-guardsmen-the-new-front-line-in-cybersecurity (accessed February 15, 2013).

[50] Adam Ashton, "WA National Guard focusing on cyber security," The News Tribune, October7, 2012, http://www.thenewstribune.com/2012/10/07/v-printerfriendly/2323245/guard-focusing-on-cyber-security.html (accessed February 15, 2013).

[51] The specific doctrine examined was USAF Doctrine Document (AFDD) 3-12 on *Cyberspace Operations*, July 15, 2010, and Army Cyberspace White Paper (Draft) (v0.1), *Cyber – An Element of Combat Power with Strategic to Tactical Consequence 2012-2030*, August 19, 2012.

[52] *National Defense Authorization Act for Fiscal Year 2012*, House Resolution1540, 112th Congress, first Session, (January 5, 2011), located under Title X-General Provisions, Sub-title 1 Miscellaneous Authorities and Limitations, Section 1076-Study on Recruitment, Retention, and Development of Cyberspace Experts, subparagraph (b)(2)(D) States: An exploration of the various recruiting, training, and affiliation mechanisms, such as the reserve components, including the individual ready reserves, the civilian expeditionary workforce, corporate and university partnerships, the Reserve Officers' Training Corps, and civilian auxiliaries to address challenges to recruitment, retention, and training. http://www.opencongress.org/bill/112-h1540/text (accessed February 15, 2013).

[53] Robert S. Mueller, III, *Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat: Audit Report 11-2,* (Washington, DC: U.S. Department of Justice, September 2011), iv.

[54] This is a fictional scenario for illustrative purposes only.

[55] Teri M. Takai, *Department of Defense (DOD) Information Technology (IT) Enterprise Strategy Roadmap* (Washington, DC: U.S. Department of Defense, September 6, 2011), v.

[56] Ibid.

[57] Department of Defense, *National Defense Budget Estimates for FY 2010,* Accessed February 15, 2013, from: http://comptroller.defense.gov/defbudget/fy2010/Green_Book_Final.pdf Source information from the *Department of Defense (DOD) Information Technology (IT) Enterprise Strategy Roadmap* p.8.

[58] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace- Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-11,* (Washington, D.C: ONCIX, September 6, 2011), A-2.

[59] *Department of Defense INSTRUCTION NUMBER 8510.01*, November 28, 2007, ASD(NII)/DoD CIO, DOD Information Assurance Certification and Accreditation Process (DIACAP), 3.

[60] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace- Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-11,* A-2.

[61] While assigned as the Chief of Staff for 5th Signal Command in Europe, I supervised the funding for the Army in Europe Information Technology Training (AE-ITT) program. FY 2011 funding consisted of $2.1 million, but was later revised to $2.6 million.

[62] Cleared Industry refers to the part of the DIB that has access to U.S. Government classified and unclassified networks.

[63] Stanley L. Sims, *Targeting U.S. Technologies - A Trend Analysis of Reporting from the Defense Industry 2012,* (Washington, D.C: Defense Security Service (DSS), 2012), 64.

[64] Department of Defense, *FACT SHEET: Defense Industrial Base (DIB) Cybersecurity Activities,* May 11, 2012, http://www.defense.gov/news/d20120511dib.pdf (accessed February 15, 2013).

[65] Paul Stockton, "Ten Years After 9/11: Challenges for the Decade to Come," Homeland Security Affairs, Volume 7, The 9/11 Essays, September, 2011, 4.

[66] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace- Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-11,* A-3.

[67] Tracy Waldon and James Lande, *The Industry Analysis Division's of Rates Price Indices and Household Expenditures for Telephone Service*, Industry Analysis Division, Common Carrier Bureau, Federal Communications Commission. (Washington, D.C., March 1997), 17.

[68] Richard Weitz, “Global Insights: The DHS’ Cybersecurity Logjam,” World Politics Review, 10 April 2012, http://www.worldpoliticsreview.com/articles/11827/global-insights-the-dhs-cybersecurity-logjam (accessed February 15, 2013).

[69] M. G. Mullen, *The National Military Strategy of the United States of America,* 19.

[70] U.S. Congress, House of Representatives, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the Committee on Homeland Security, *Examining the Cyber Threat to Critical Infrastructure and the American Economy*, 112th Congress, First session, March 16, 2011, 1. http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf (accessed February 15, 2013).

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu