DE GRUYTER DOI 10.1515/jhsem-2012-0001 — Homeland Security & Emergency Management 2013; 10(1): 1–28

Austen D. Givens* and Nathan E. Busch

Integrating Federal Approaches to Post-Cyber Incident Mitigation

Abstract: This article argues that the federal government lacks a cohesive approach to post-cyber incident mitigation – that is, the closing of vulnerabilities that become apparent during and after a cyber incident. To begin addressing this gap in cybersecurity capabilities, greater legal, cultural, and technological integration among the Department of Defense, Department of Homeland Security, and US Intelligence Community would be helpful in achieving a more unified strategy in post-cyber incident mitigation.

Keywords: cybersecurity; defense; homeland security; mitigation; public policy.

***Corresponding author: Austen D. Givens,** King's College London, London, UK,
e-mail: austen.givens@kcl.ac.uk
Nathan E. Busch: Christopher Newport University, Newport News, VA, USA

1 Introduction

The federal government has a cybersecurity problem. In late May 2013 *The Washington Post* reported that Chinese hackers had stolen several advanced US weapons systems designs from private defense firms and US government agencies (Nakashima 2013b). These stolen designs included plans for the US missile defense system in Asia, which was built to shoot down nuclear missiles aimed at the United States and its allies, as well the US Navy's widely-used F/A-18 fighter jet (*Ibid.*). Senior US government officials claimed that these thefts were part of a huge ongoing Chinese government cyber espionage campaign (*Ibid.*; DOD 2013: pp. 51–53; Nakashima 2013a; Sanger 2013).

The thefts were not exactly surprising. In 2012 former Director of National Intelligence (DNI) Mike McConnell, former Secretary of Homeland Security Michael Chertoff, and former Deputy Secretary of Defense William Lynn characterized the Chinese cyber threat bluntly in a *Wall Street Journal* opinion column, noting that "[t]he Chinese are the world's most active and persistent practitioners of cyber espionage today" (McConnell et al. 2012). Further underscoring the scope of Chinese cyber espionage, a 2013 Department of Defense (DOD) report to Congress indicated that in 2012, numerous US government and private sector computer networks were targeted for intrusions for the purpose of data exfiltration,

"some of which appear to be attributable directly to the Chinese government and military" (DOD 2013: p. 36).

Cyber threats such as these are particularly insidious because the interconnectedness of federal computer networks means that a vulnerability in one federal agency's network can create vulnerabilities in other agencies' networks. Both DOD and DHS work on cybersecurity initiatives, and these close ties mean that hackers can exploit an electronic vulnerability in one agency's network to gain access to another agency's network (Guinchard 2011: pp. 83–84). For example, in 2010, email messages began spreading across the Internet with the subject lines "Here You Have" and "Just for You" (Mills 2010). These messages, which came to be known as the VBMania virus, rapidly propagated themselves across computer networks (Kaplan 2010). Some versions of the message contained links that supposedly pointed toward documents; others provided an apparent link to pornographic online videos. When clicked on, both links actually silently downloaded software that hijacked the user's Microsoft Outlook email application, which would then send the virus to the user's contacts (*Ibid.*). The virus would also simultaneously "scan" users' web browsers, looking for saved passwords to covertly steal and export. When affecting multiple computer users, this flurry of activity flooded computer networks, shutting down organizations' servers (*Ibid.*). Press reports indicated that both NASA and US Immigration and Customs Enforcement computer networks may have been temporarily crippled by the virus (Kaplan 2010; Mills 2010).[1]

The potential for damage in one federal agency's computer network to spill over into other federal agency computer networks suggests that a consistent federal approach to cybersecurity is needed. Integrated solutions to cybersecurity vulnerabilities that view federal information systems in a holistic way would appear to be effective in countering these threats (Chittister and Haimes 2011; McGraw 2013: pp. 117–118). But federal approaches to cybersecurity are problematically divided (Westby 2007; Chabinsky 2010).

Basic legal and semantic challenges abound in cybersecurity, including difficulties in crafting and passing laws related to cybersecurity (Flowers et al. 2013: pp. 7–12). This is partly because there is a continuing tension between the need for government visibility into cyber activities, and an equally pressing requirement to safeguard civil liberties and constitutional rights against unreasonable searches (McCullagh 2012). Moreover, terms like cyber war, cyberterrorism, cyberespionage, and cyber crime are fluid and imprecise. This makes defining governmental roles in cybersecurity challenging. For example, when is a cyber incident

1 Although unnamed sources claimed that US Immigration and Customs Enforcement networks were affected by the virus, the agency officially denied that its networks had been impacted.

considered a cyber attack, requiring DOD involvement? And what is the threshold of severity that compels DOD to become involved? The answers to these questions are unclear.

There is also basic disagreement about locating overarching federal cybersecurity authority within the Department of Homeland Security (DHS), DOD, or the White House (Westby 2007; CSIS 2008; White and Coldebella 2010; Newmeyer 2012). Conflicting directives and regulations complicate this issue. As the lead federal agency for incident management, DHS is charged with coordinating the federal response to a cyber attack that impacts the United States (The White House 2003). DOD, on the other hand, retains authority for warfighting. As in traditional conflicts, DOD is responsible for defending against and responding to cyberattacks launched by nation-state or non-state actors (DOD 2009). Thus a foreign electronic attack on US systems would theoretically be met by at least two distinct responses. While DOD would retaliate against the attack itself, the specific domestic impacts of the attack – incident management, in other words – would be addressed by DHS (Sharp 2010). As a joint DOD/DHS memorandum of agreement (MOA) in 2010 outlined, the overall coordination of the federal response would rest with the Secretary of Homeland Security (DHS and DOD 2010).[2] This organizational division of responsibilities is historically consistent with that used for traditional threats – foreign militaries, natural disasters, and so on (The White House 2003; DOD 2009). But in the dynamic domain of cyberspace, these different departmental roles prove cumbersome.

Recognition of this issue is not new. In 2009 President Obama specifically highlighted the trouble with un-integrated federal approaches to cybersecurity:

> No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should – with each other or with the private sector (The White House 2009b).

Nearly 4 years later, we have not made significant progress in constructing a cohesive, unified federal cybersecurity policy (GAO 2011a,b). This lack of integration spans the whole of federal cybersecurity, which includes functions like cyber preparedness, incident response and recovery, offensive and defensive cyber warfare, public-private sector coordination, and citizen education on cyber threats (Dipert 2010; Harknett et al. 2010; Hollis 2010; Nojeim 2010; White and Coldebella 2010; Cyber Incidents 2011; Dunlap 2011; Etzioni 2011; Fischer 2011;

2 Perhaps anticipating the need for excellent interagency cooperation, this memorandum addresses fundamental principles of communication, for cybersecurity between DOD and DHS.

Guinchard 2011; NIST 2011; Newmeyer 2012). Examining this policy challenge, therefore, has wide-ranging implications for cybersecurity measures across the federal government.

This article focuses on problematic divisions of responsibility in a specific area of cybersecurity – DOD, DHS, the White House, the FBI, and the CIA's approaches to post-cyber incident mitigation – to illustrate this broader set of problems. We define a "cyber incident" as any electronic event with destructive effects upon both information systems and US national security. This would exclude acts like pinging and port scanning, for example, but would include events like introduction of malware or data theft (CSIS 2013; FEMA 2013; CPNI n.d.; Deloitte n.d.). A "post-cyber incident" would therefore include the actions that these federal agencies would take to respond to attacks, and to "prevent attacks, reduce vulnerabilities, and fix systems" after attacks have taken place (DHS 2010).

The article begins by arguing that the current approaches to post-cyber incident mitigation employed by DHS, DOD, the White House, the FBI, and the CIA are problematically divided. It then makes the case that further legal, cultural, and technological integration among these federal organizations would help achieve a more unified federal approach to post-cyber incident mitigation.[3] Finally, we conclude with a few summary observations and policy recommendations.

2 Current Federal Approaches to Post-Cyber Incident Mitigation

Within the federal government post-cyber incident mitigation responsibilities are primarily divided among DOD, DHS, and the White House. Member agencies of the federal intelligence community (IC) also have significant roles in cybersecurity. To an extent this division of responsibilities makes sense, as each of these governmental entities has a distinct cybersecurity mission in the context of the federal government as a whole. But cybersecurity issues cut across the federal government and do not limit themselves neatly to one federal agency or one department. Given that cybersecurity issues affect multiple areas of the federal government, it is logical to integrate federal approaches to post-cyber incident

3 We acknowledge that there are certain details about federal cybersecurity activities that remain classified, and therefore may exist outside the public domain. This article is based entirely on unclassified, open source material.

mitigation. Yet this has not happened. Instead DHS, DOD, and the White House have each carved out their own approach to post-cyber incident management. The Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI), too, have not synchronized their approaches to post-cyber incident mitigation with the rest of the federal government.

In the following discussion of DHS, DOD, the White House, and the IC's approaches to cybersecurity, it becomes clear that much important work remains before federal approaches to post-cyber incident mitigation are adequately integrated. And if left un-integrated, these current federal approaches to post-cyber incident mitigation create the possibility for electronic vulnerabilities to remain exposed, increasing risks to government computer networks.

2.1 DHS' Current Approach to Post-Cyber Incident Mitigation

First released in September 2010 by DHS, the National Cyber Incident Response Plan (NCIRP) remains in draft form (DHS 2010). It broadly addresses mitigation, that is, "ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident" (*Ibid*., M-1). For example, the plan identifies DHS' National Cybersecurity and Communications Integration Center (NCCIC) as the facility where federal partners assemble to "develop and share…mitigation recommendations using established communication channels" (*Ibid*., 24). This suggests that DHS can only *recommend* to other agencies that they take certain steps to close cyber vulnerabilities. But there is no authority or inducement to *compel* other agencies to take action to mitigate threats. Without the prospect of incentives or penalties, it is unreasonable to assume that other federal agencies will simply comply with DHS' cybersecurity recommendations (Schneider and Ingram 1990).

Within the NCCIC, DHS houses the US Computer Emergency Readiness Team (US-CERT). CERT is the operational arm of the NCCIC, and responds to cyber incidents nationwide (US-CERT n.d.). US-CERT actively coordinates with other federal agencies, as well as critical infrastructure operators, business owners, and academic institutions (*Ibid*.). In theory, US-CERT's activities help to facilitate more effective cyber incident response across the federal government. But like the NCCIC as a whole, US-CERT cannot compel other federal agencies to implement specific mitigation measures after a cyber incident occurs. It can only encourage implementation of post-cyber incident mitigation measures.

This illustrates a divided interagency approach to post-cyber incident mitigation. The decision to implement post-cyber incident mitigation recommendations rests with agency heads and is executed through authority delegated

to government departments' Chief Information Officers (CIOs). In other words, the decision to require a software security patch is up to a given agency's CIO, not DHS. This fractured approach to cyber incident mitigation is understandable, because there is good reason for agencies to maintain control over their own IT infrastructure. However, the examples discussed above underscore both the scope of current cyber threats and the degree to which malware can infect multiple government computer networks. Therefore, a disjointed approach to post-cyber incident mitigation seems short-sighted. More integrated strategies for mitigation that transcend agencies prove more effective, because they more accurately reflect the dynamic nature of electronic threats. Unfortunately, in its Strategy for Operating in Cyberspace, DOD further reinforces a fractured approach to post-cyber incident mitigation.

2.2 DOD's Current Approach to Post-Cyber Incident Mitigation

The 2011 DOD Strategy for Operating in Cyberspace underlines the mis-alignment of mitigation responsibilities between DHS and DOD (GAO 2011c).[4] The document discusses the need for internal DOD threat mitigation in multiple ways, including guarding against insider threats and protecting the technology supply chain with private sector partners (DOD 2011: p. 7, 9). But in discussing DOD's partnerships with other agencies on cybersecurity initiatives, the Strategy notes that DOD will support DHS in "leading interagency efforts to identify and mitigate cyber vulnerabilities in the nation's critical infrastructure" (DOD 2011: p. 8). However, as demonstrated earlier, DHS' leadership role in cyber mitigation is one of centralized coordination. It has no authority to sew up gaps in cybersecurity across the executive branch. Like other executive branch agencies, the best that DHS can do is *recommend* steps to mitigate threats. DOD's deference to DHS' mitigation leadership here is therefore problematic.[5]

Although the strategy describes a clear concern for threat mitigation within DOD, it ultimately punts the interagency approach on post-cyber incident mitigation to DHS. But DHS cannot require other agencies to mitigate

4 This GAO reports underlines the need for more clearly defined cybersecurity requirements across DOD.

5 The two primary DOD entities involved in cybersecurity operations are US Cyber Command (USCYBERCOM) and the National Security Agency (NSA). The Director of the NSA is dual-hatted as commander of USCYBERCOM. The two organizations work closely together, but there are clear dividing lines between their areas of responsibility and those of DHS.

the risk of cyber threats. Agencies may implement recommended mitigation measures, or not. As the lead federal departments in cybersecurity, DOD and DHS' un-integrated approach to post-cyber incident mitigation poses risks for both their own computer networks, as well as those of other executive branch agencies. It is reasonable to assume that clear direction from the Executive Office of the President (EOP) would help address this issue. But this has not yet occurred.

2.3 The White House's Current Approach to Post-Cyber Incident Mitigation

Shortly after being sworn into office in 2009, President Barack Obama ordered a re-appraisal of federal cybersecurity policy (Harknett and Stever 2009; Sanger and Markoff 2009; The White House 2009a). The result of this 60-day effort was the Cyberspace Policy Review, which began to adjust cybersecurity policies from the George W. Bush administration (The White House 2009a). The Review was comprehensive in scope – a strategy document. Although the Review discussed the need for mitigation in multiple respects, it was silent on what agencies or individuals should steer mitigation efforts (The White House 2009a: p. i, v, 17, 31, C-10). Following the Review, White House updates to the Bush administration's Comprehensive National Cybersecurity Initiative (CNCI) began to take shape.

The EOP's decision to publish an unclassified version of the CNCI provides a helpful view into the administration's thinking about post-cyber incident mitigation responsibilities (Nakashima 2010a; The White House 2010). The CNCI first outlines twelve points related to broader cybersecurity policy, including deploying intrusion detection sensors across government networks, as well as developing deterrence strategies and programs (The White House 2010: p. 2, 5). In this sense, it is more tactically oriented and detailed than the Cyberspace Policy Review. Broader thematic discussion of mitigation also appears in the CNCI. However, the CNCI specifically mentions mitigation exactly twice: once in the context of counterintelligence, and again in protecting the global supply chain (*Ibid.*, 4–5). With few exceptions, such as the description of the prominent role played by the US-Computer Emergency Readiness Team (US-CERT), there is a conspicuous lack of specific responsibility for post-cyber incident mitigation in the CNCI.

This shows that the EOP's view of federal post-cyber incident mitigation is even murkier than that of DOD and DHS. It raises serious doubts about the feasibility of implementing mitigation measures in a uniform way across the federal

Table 1 Federal Cybersecurity Authorities Examined in this Article.[6]

Organization	Primary Organizational Cybersecurity Mission	Cybersecurity Guidance Document	Cybersecurity Document Purpose
Department of Defense	Treat cyberspace as a domain for military dominance	*DOD Strategy for Operating in Cyberspace*	Presents a strategic vision of how DOD approaches cybersecurity internally and in partnerships at all levels
Department of Homeland Security	Work with public, private and international entities to secure cyberspace and US cyber assets	*National Cyber Incident Response Plan*	Creates a strategic framework for organizational preparedness for, response to, and recovery from cyber incidents
Executive Office of the President	Centrally coordinate cybersecurity policymaking process	*Comprehensive National Cybersecurity Initiative*	Guidance to establish a front line of cyber defense; defend against full spectrum of threats; and strengthen future cybersecurity environment

government, at least as currently outlined. DOD and DHS take a narrow approach to the issue – meaning they exercise direct control over their own IT infrastructure, and little else. By contrast, through the Cyberspace Policy Review and CNCI, the EOP essentially describes mitigation as a good thing without identifying concrete steps for instituting mitigation procedures. Table 1 above provides a brief summary of these entities and the cybersecurity authorities examined in this analysis.

DHS and DOD have important roles and responsibilities in post-cyber incident mitigation. But their respective roles and responsibilities are not as integrated as they could be. And the EOP's virtual silence (thus far) on how to integrate DOD and DHS' approaches to post-cyber incident mitigation does not help the situation. Absent policy changes, the cybersecurity disconnect between DHS and DOD will likely continue for the foreseeable future.

6 Open source cybersecurity strategy documents for the CIA or FBI do not appear to be available.

2.4 The CIA and FBI's Current Approaches to Post-Cyber Incident Mitigation

DOD and DHS are member agencies of the IC. They must balance their roles as the leading federal agencies in cybersecurity and their roles as part of the IC. This can cause difficulties in their interactions with the CIA and FBI, which also have roles in cybersecurity, and which are also member agencies of the IC. To further complicate matters, it is also unclear what the role of the rest of federal IC is in addressing cyber threats. While DHS and DOD tend to dominate discussions of federal cybersecurity policy, both the FBI and the CIA have been collecting intelligence on cyber threats. Yet DHS and DOD also retain their own intelligence functions – DHS has its own office of Intelligence and Analysis, and DOD houses multiple intelligence agencies, including the National Security Agency (NSA). To date, it is unclear how DOD and DHS will coordinate their actions in cybersecurity with other IC member agencies, especially the FBI and CIA.

The lack of clarity in how the IC member agencies will coordinate with each other and with related federal organizations can lead to confusion in post-cyber incident mitigation. In a February 2013 speech, FBI Director Robert Mueller underscored this problem:

> What is the allocation of responsibilities among DHS, NSA, and the FBI? I do know there has been some confusion as to the roles of these three agencies... While the answer depends in part on the scope and the nature of the intrusion, the FBI often will be the first responder because of our nationwide coverage. But the investigative team, at a minimum, should include the expertise of both DHS and NSA... Our agencies operate under separate authorities and have different roles to play. Yet we also understand that we must work together on every substantial intrusion and share information among the three of us (Mueller 2013).

Although Mueller emphasized that the FBI must collaborate with other federal agencies in cybersecurity, he also points out that there has been confusion about the roles of different federal agencies in cybersecurity.

This confusion can create challenges in post-cyber incident mitigation. Divided and unclear responsibilities mean that there is greater potential for post-cyber incident mitigation measures to remain unimplemented. Without clear direction, it is not reasonable to assume that the FBI – or any agency – will implement mitigation measures after a cyber incident. Doing so would take away needed time and resources from other pressing agency priorities.

The CIA faces similar challenges in cybersecurity. Former CIA director Michael Hayden, who stepped down in 2009, now says that a substantial amount of information about cyber incidents is "horribly over-classified," inhibiting

learning about electronic vulnerabilities, and ultimately making post-cyber incident mitigation more difficult (Kaiser 2011). In October 2011 Congressional testimony, Hayden extended this thinking further:

> We need to recalibrate what is truly secret. Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion and created by a common body of knowledge (Hayden 2011: p. 7).

Hayden's suggestions make sense. For an individual to view classified material about cyber incidents, she must have a federally-issued security clearance. But without a security clearance, she cannot view this classified material. This means that classified information about cyber incidents is walled off from anyone without a security clearance – including private sector experts and academic researchers. But government officials could turn to these very experts so as to create new post-cyber incident mitigation measures – *if* these experts had access to detailed information about these now-classified cyber incidents.

It is critical to keep some information classified – especially information about intelligence sources or methods. Yet over-classifying information about cyber incidents ultimately harms government by limiting outside experts' ability to diagnose and treat the root causes of cyber incidents. Continuing to over-classify information about cyber incidents will leave cyber vulnerabilities open longer, for it blocks a team of skilled physicians (outside experts and academic researchers) from a sick patient (federal computer networks).

Howard Schmidt, the former Coordinator for Cybersecurity for the Obama administration, reinforced Hayden's observations about cybersecurity information being over-classified in a recent interview. He noted that "[i]n one US case in 2011, it took 102 days from when an attack was reported [for government] to share the information with the private sector, which is unconscionable" (Ashford 2013). In this comment, Schmidt reinforces Hayden's concern about the over-classification of certain cybersecurity information. To integrate federal approaches to cybersecurity more fully, IC member agencies will need to coordinate closely to make more information about cybersecurity threats available to private sector partners in a timely fashion (Busch and Givens 2012, 2013; Givens and Busch 2013a,b).

2.5 Why Greater Federal Integration has not Occurred

Problematically divided federal approaches to cybersecurity persist. But there are several reasons why these divisions continue. First, within the federal

government, there is a clear and deliberate separation between domestic and international responsibilities. Government officials often use the acronyms CONUS (Continental United States) and OCONUS (Outside the Continental United States) as shorthand for this distinction. Historically DOD is an OCONUS-focused agency. While DOD has countless facilities and bases inside the United States, its basic mission of protecting the United States really occurs OCONUS – whether at overseas military installations or in theaters of war like Iraq or Afghanistan. The CIA is similar. It collects foreign intelligence about foreign targets.

But DHS and the FBI are different than DOD and the CIA. DHS and the FBI focus on CONUS. DHS is charged with protecting the United States, but that protecting occurs overwhelmingly inside US borders – not overseas. The FBI is a federal law enforcement agency. Like DHS, the vast majority of its operations take place inside CONUS. The reasons for this division between CONUS and OCONUS responsibilities in DOD, the CIA, DHS, and the FBI are deeply rooted in history, law, and organizational cultures. It is not easy for policymakers to begin merging such deeply rooted historical, legal, and cultural factors. Moreover, there is a natural human tendency to resist change. And organizations like DOD, the CIA, DHS, and the FBI are made up of dedicated professionals who also naturally resist change. Collectively these factors make bridging the divide between OCONUS and CONUS in cybersecurity a challenge.

Second, for the federal government as a whole, cybersecurity is fairly new territory. Until recently agencies like the US Air Force worked on cybersecurity initiatives, but they worked in relative isolation from the rest of the federal government. But now federal agencies like the CIA and FBI that did not previously work on cybersecurity are working on cybersecurity. And federal agencies like the FBI and DOD that did not work together previously on cybersecurity now have to work with one another on cybersecurity. It takes time for the "newness" of these changes to sink into organizations and take root. Agency leaders need to be patient, too, in order to learn about one another's new capabilities and responsibilities in cybersecurity. The dust will eventually settle as these federal agencies assume new independent roles in cybersecurity, and learn to coordinate their roles with those of other agencies. But until the dust settles, post-cyber incident mitigation measures will not be as integrated as they could be.

Third, cybersecurity is a particularly new area of operations for the CIA and FBI. By contrast, the US Air Force, which is part of DOD, has been involved with cybersecurity operations since at least 1997 (Federal Laboratory Consortium for Technology Transfer 2013). DHS was formed in 2002 (Homeland Security Act 2002). Its Office of Cybersecurity and Communications came into being in 2006 (DHS n.d.). Therefore, DHS' participation in cybersecurity spans a significant percentage of the agency's existence to date. But historically the CIA is an agency

concerned with two key priorities: collecting and analyzing foreign intelligence about state and non-state actors, and conducting covert action. At first glance collecting and analyzing information about cybersecurity threats does not fit neatly into either of those categories.

Similarly, while the FBI has long investigated violations of federal law, jurisdictional boundaries between government and private sector operations blur easily in the electronic world. This means that, for the FBI, getting involved in cybersecurity investigations means learning to distinguish jurisdictional boundaries that are a far cry from those seen in more conventional criminal investigations. For both the CIA and FBI it is likely challenging to make sense of their own capabilities and responsibilities in cybersecurity, in part because cybersecurity itself is such a new subject for them. And until the CIA and FBI are able to make good sense of their capabilities and responsibilities in cybersecurity, this will limit their ability to integrate their approaches to post-cyber incident mitigation with DHS and DOD.

Fourth, inter-organizational tensions die hard. Despite the heavy post-9/11 emphasis on unity of effort in government, turf battles among agencies continue. Cybersecurity policy blends hierarchical military organizations and flatter, more collaborative civilian agencies. These organizational differences create the potential for sharp disagreements over policy and procedures among agency heads, contributing to inter-organizational tensions. Moreover, integrating federal approaches to cybersecurity means that DOD, DHS, the CIA, and the FBI now share complementary missions. With these missions in mind, these agencies' leaders must lobby Congress each year for budget money to deal with cybersecurity threats. Yet the need for Congressional funding can set these agencies at odds with one another. Agency leaders must independently show members of Congress that their organizations are overtaxed in managing cybersecurity threats, and make a strong case to Congress for additional funding for their respective organizations. If DOD, DHS, the CIA, and the FBI are each doing this simultaneously, there is potential for "winners" and "losers" to emerge – the "winners" getting the lion's share of Congressional funding for cybersecurity, while the "losers" get less funding for cybersecurity. This split between funding "winners" and "losers" can fuel inter-organizational resentment, making integration of cybersecurity operations even more difficult than before.

Recent reporting that China's People's Liberation Army (PLA) continues to hack into US public and private sector information systems demonstrates the urgency of integrating federal approaches to cybersecurity (Mandiant 2013). PLA theft of public and private sector information is a crime, and falls into the FBI's domain of responsibility. Simultaneously, PLA operations against US government systems fall into DOD's domain. The CIA, too, plays a part in this, for it collects

intelligence on cyber threats from overseas. DHS has the leading role in managing the domestic consequences of any cyber incidents stemming from PLA penetration of US information systems. To mitigate the risk of future hacking by the PLA, it will be important for DOD, DHS, the CIA, and the FBI to integrate their collective knowledge of PLA capabilities and methods, and apply that collective knowledge to developing robust mitigation measures.

3 Recommendations for Improving Integration for Federal Post-Cyber Incident Mitigation

Given the challenges that we have seen in federal responses to cybersecurity threats, there are important steps that need to be taken to better integrate federal approaches to cybersecurity. Doing so will require time, effort, resources, and patience. As a first step toward better integration of federal approaches to cybersecurity, below we offer a set of policy recommendations to improve federal approaches to post-cyber incident mitigation. These recommendations cannot solve every problem related to cybersecurity. But they do suggest a viable way forward in better integrating federal cybersecurity activities.

3.1 Legal Integration for DOD and DHS

Laws governing DOD and DHS have sometimes overlapping, conflicting, and confusing responsibilities in cybersecurity. To better align DOD and DHS roles in cybersecurity, policymakers will need to identify and work through the legal challenges facing DOD and DHS to improve cybersecurity coordination. Underscoring the magnitude of this issue, former DNI Dennis Blair once noted that "The precedents and the laws on the books are just hopelessly inadequate for the complexity of the global information network" (quoted in Nakashima 2010b). Given these problems, it may be necessary to consider updates to laws circumscribing DOD and DHS' roles in cybersecurity. Two provisions deserve special attention: the Posse Comitatus Act of 1879, and the Homeland Security Act of 2002.

The Posse Comitatus Act of 1879 (18 U.S.C. § 1835) prohibits use of military assets in domestic law enforcement functions except in extremely limited circumstances, such as armed rebellion (Toomer 2002: pp. 29–30; Fischer 2011: p. 10). There is debate over whether the Posse Comitatus Act restricts military

cooperation in managing cyber incidents with domestic impacts.[7] Presumably, this prohibition would extend to assisting with post-cyber incident mitigation, particularly in criminal investigations of malicious cyber incidents. It may be beneficial for policymakers to revisit the Posse Comitatus Act to accommodate the complexity of investigating cyber incidents affecting US assets. DOD may have valuable information to share with law enforcement officials about a cyber incident's underlying causes. These same data could help to close electronic vulnerabilities, preventing future incidents. But with a legal wall separating DOD from law enforcement authorities, this possibility diminishes. A careful, tightly defined expansion of DOD's authorities in domestic post-cyber incident mitigation would therefore be prudent. This change would permit DOD to aid domestic law enforcement agencies in cyber incident investigations and analyses, with a view to preventing future, similar incidents. A foundational law affecting DHS – the Homeland Security Act of 2002 – could also be modified to expand DHS' participatory role in cyber conflicts.

DHS receives its authority to manage response to domestic incidents from the Homeland Security Act (HSA) of 2002 and Homeland Security Presidential Directive 5 (Homeland Security Act 2002; The White House 2003). The HSA could be revised in a narrow way to permit select DHS personnel to participate in offensive and defensive cyber operations alongside DOD personnel. DHS' involvement under this arrangement might range from a significantly enhanced role, such as direct active engagement in offensive and defensive actions, to more limited involvement via consultations in command centers. In a legal sense, this shift would place DHS on a similar footing as the US armed forces in cybersecurity (Armed Forces 2012).

There would be multiple advantages to this arrangement. At present, both DHS and DOD have divergent missions. They use different vocabularies in describing cyber threats and think about cybersecurity in fundamentally distinct ways – i.e., the former primarily concerned with domestic civilian and government systems, and the latter with US armed forces' and DOD-centric networks. Each department also uses different computer systems to manage information. By permitting limited DHS engagement in cyber conflict, there would be an increase in efficiency in cybersecurity operations. Knowledge transfer between DOD and DHS would become more fluid due to increased familiarity with systems and terminology. This, in turn, would promote more effective responses. The information

7 Toomer provides an excellent discussion of the armed forces' supporting role in the War on Drugs and managing the 1992 Los Angeles riots. Fischer draws an analogy between these real-worlds events and those occurring in the cyber arena.

and learning from these responses would then smoothly translate into post-cyber incident mitigation measures. Having DOD and DHS personnel working shoulder-to-shoulder in cyber conflict means that mitigation measures can be implemented using complete, well-understood information (Nakashima 2010b).[8] There is less chance for misunderstanding what occurred, how to respond to it, and how to prevent it from happening again. For both DOD and DHS, then, collaboratively engaging in cyber conflicts would provide greater governmental unity and coordination in post-cyber incident mitigation.

There is clear precedent for this evolution in thinking about government departments' roles in conflict. Consider the federalization of National Guard (NG) assets to conduct military operations overseas (Lowenberg n.d.). NG resources belong to the states and NG units report to state Governors. The NG is historically proficient in managing disasters domestically. Yet it quickly adopts non-traditional roles when federalized and deployed to the battlefield. This seems a helpful analog in understanding the need to afford DHS greater offensive and defensive capabilities in cyberspace (Buchalter 2007). Having active duty armed forces and NG personnel working together in combat helps foster a stronger response. Similarly, DHS, whose primary emphasis is the United States and its territories, could also take on a limited role in cyber conflicts, enhancing response and post-cyber incident mitigation measures.

A second example further underscores the feasibility of cyber combat capabilities being shared by DOD and DHS. The conflicts in Afghanistan and Iraq benefitted from an expanded CIA role in "preparing the battlefield." In advance of US armed forces personnel arriving in each country, CIA officers helped establish intelligence networks and select targets for military action (Shaughnessy 2011; Chesney 2012). This was all done with a view toward aiding DOD, blurring the line between the intelligence community and defense activities (Best 2011). As outlined above, there is a similar blurring now between DOD and DHS in cybersecurity policy. It is sensible to re-examine existing laws governing each department to adapt to this evolving need.

This proposal is also directly reminiscent of the information sharing "wall" between law enforcement and intelligence agencies prior to the 9/11 attacks (Grewe 2004). At one time, legal barriers between the CIA and FBI made sense, particularly as protection against domestic collection of intelligence on US citizens. But 9/11 forced that understanding to evolve. The "wall" needed to come down to permit the two agencies to work together more closely, while retaining

8 There has been vigorous debate about whether DOD involvement in offensive cyber operations should legally be considered covert action.

their distinct organizational identities and maintaining respect for citizens' civil liberties (Doyle 2002; U.S. Cities 2003).[9]

Given current knowledge of cybersecurity demands and ambiguities, lowering legal barriers between DOD and DHS makes sense. The implementation of the USA PATRIOT Act, which accelerated the lowering of the "wall" between intelligence and law enforcement agencies, provides an essential model for this increased coordination in cybersecurity (Department of Justice 2004). The Act first required a great deal of legal analysis and re-calibration to effectively boost information sharing between intelligence and law enforcement agencies. Similarly, improving cybersecurity information sharing between DOD and DHS will require policymakers to catalogue and sort through the legal parameters for increased coordination. This is particularly important in the context of criminal investigations and prosecutions, which must be conducted with important constitutional safeguards in place. If intelligence and law enforcement agencies fail to adhere to these constitutional safeguards, then evidence from criminal investigations may not be admissible in court.[10]

These proposals for greater legal integration between DOD and DHS may also present challenges given DOD and DHS' different missions. There may be areas of cybersecurity in which greater coordination between DOD and DHS proves impossible. However, a great deal can be accomplished in areas where DOD and DHS missions overlap, as well as within the broader framework of federal cybersecurity policy. These steps toward deeper legal integration could have the secondary effect of bridging differences between DOD and DHS' organizational cultures.

3.2 Cultural Integration for DOD and DHS

DOD and DHS are culturally distinct. The former is a largely uniformed department; the latter is primarily civilian. DOD has long looked outside the United States to address defense issues, rather than concentrating on what is occurring inside the continental United States. DHS was created to focus on the domestic front, rather than overseas. DOD dates to the National Security Act of 1947, while DHS celebrates its tenth anniversary this year. Yet both departments must actively cooperate to advance their respective missions in cybersecurity. DOD's

9 While beyond the scope of this article, the lowering of the information sharing "wall" remains controversial. The USA PATRIOT Act, a landmark law that helped to advance this idea, remains a particular point of contention among civil libertarians and privacy advocates.

10 The authors thank an anonymous reviewer for this suggestion.

cultural orientation toward warfighting, and DHS' focus on domestic incidents, would change with more integrated cybersecurity operations.

Historically, DOD's role in domestic post-incident mitigation has been limited. For instance, one recalls the US Army Corps of Engineers' responsibilities in response to Hurricane Katrina in 2005 – building temporary sandbag levees, and later helping rebuild permanent flood prevention infrastructure (U.S. Army Corps of Engineers 2011). What might an expansion of this role in post-cyber incident mitigation realm look like, and how might that alter DOD culture? First, there would be a need to educate DOD personnel on the importance of collaborating with officials at all levels of government on cybersecurity initiatives. This is a far cry from DOD's current focus on its own departmental-level cybersecurity needs. It would also likely mean a moving away from the notion of limited DOD involvement with civilian IT infrastructure. This means an expectation of increasing DOD engagement with civilian authorities in areas related to cyber incidents. Joint DHS-DOD teams, for example, might consult with private firms on ways to ensure their organizations are not unnecessarily vulnerable to electronic intrusions. This would be a shift for post-cyber incident mitigation activities; in the past, these sorts of visits would typically be from the Federal Bureau of Investigation (FBI), DHS, or both agencies. DOD involvement with civilian organizations in this way is more consistent with the true demands of cybersecurity, which call for integrated solutions.

For its part, DHS personnel would need to adopt a more global perspective. Rather than narrowly focusing on domestic concerns, the tightly linked world of international politics and domestic security would loom increasingly large in the DHS organizational conscience. DHS would likely expand its own international ties with foreign governments to collaboratively address post-cyber incident mitigation (The White House 2011).[11] There is also reason to expect closer collaboration among DOD, DHS, and business leaders in the United States, rooted in domestic cybersecurity concerns. Increased potential for "militarization" of DHS cybersecurity offices is also a possibility. This would be a natural byproduct of cultural cross-pollination of military and civilian entities. There is potential, then, for a mutually beneficial cultural transformation in both DOD and DHS due to increased cooperation on post-cyber incident mitigation initiatives. It is also logical to more closely link DOD and DHS' technologies to achieve post-cyber incident mitigation goals.

11 The Strategy underlines the importance of international partnerships in the development of cyberspace, which suggests that an expanded global role for DHS role would be consistent with the EOP's thinking.

3.3 Technological Integration for DOD and DHS

Greater legal and cultural integration will affect the technology used by DOD and DHS. That may mean that DOD needs to be granted greater access to domestic information systems. For example, DOD could have more access to private sector Supervisory Control and Data Acquisition (SCADA) systems controlling the operation of bridges and dams, and more access to data centers that deal with components of US critical infrastructure.

DOD's present responsibilities as part of USCYBERCOM include securing domestic electrical power and manufacturing facilities for military operations (Alexander 2010). This expansion to other facets of critical infrastructure would therefore be a natural extension of DOD's current role.

In a similar way, DHS could be given greater access to DOD networks and systems both inside and outside the United States, and could strengthen ties with firms that support DOD IT infrastructure overseas. For both DOD and DHS, this will likely require new tools that need to be installed, deployed, and maintained over time. But first it will require both agencies to navigate a challenging set of public expectations.

The prospect of government access to private sector computer networks has been a point of great concern for many years. This concern was underscored by recent revelations from Edward Snowden, a former National Security Agency (NSA) contractor, that the NSA has been collecting telephone call metadata from Verizon and data about customers of some of the most well-known IT firms, including Google, Facebook, and Microsoft (Groll 2013). According to the NSA, this data was collected to gather intelligence for counterterrorism purposes (*Ibid*.). Unlike the NSA surveillance, our proposal here deals with monitoring the general health of computer networks used in critical infrastructure like banks, bridges, airports, and hospitals to protect against cyber attacks. It is not related to the Snowden case or collecting intelligence about anyone's individual Internet activity.

Government routinely monitors industrial processes like manufacturing for a number of reasons, such as worker safety, environmental contamination, zoning laws, and building permits (CSIS 2011). The state's purpose here is multi-faceted, but centers around two ideas: it is appropriate for government to take measures to ensure the safety of its citizens, and this same function can prove a source of revenue for the state through taxes and fees. Government also regulates private activity when it carries consequences for the general welfare. This is why driving drunk in one's own car on public roads is prohibited.

Attacks on computer networks that regulate critical infrastructure can and do carry consequences for human life (CSIS 2011). Some government monitoring of these computer networks makes sense because of these networks' importance for

national security. For example, a sudden drop or spike in network activity could be indicative of a larger cyber attack taking place. Having this kind of warning would be valuable for DOD and DHS, because it would permit them to take quick action to stop the attack. It would also save time for the firm whose network is being attacked, since the firm would not have to alert DOD and DHS, as DOD and DHS would already know about the attack. So it is not a question of whether it is appropriate for government to monitor the health of critical infrastructure computer networks – it is appropriate. Rather, the question is one of depth: how much monitoring is appropriate, and what type of monitoring is appropriate?[12]

It is reasonable for DOD and DHS to monitor the general health of critical infrastructure computer networks using new technology. Whether monitoring software is installed on these networks (what might be termed a high government intrusion activity), or firms voluntarily generate and send reports to DOD and DHS (which could be labeled a low government intrusion activity), enhancing DOD and DHS' access to networks that manage critical infrastructure stands to benefit the totality of cybersecurity. At the same time, it would be essential for policymakers and administrators to create safeguards to protect against potential abuses of these technologies. In particular, any monitoring of private sector computer networks would need to be undertaken with the full knowledge and consent of the firms themselves, as well as their customers.

3.4 Integration for the US Intelligence Community

As the recommended changes above between DOD and DHS occur, there will also be a need for further integration of cybersecurity operations within the IC as a whole, particularly with the CIA and FBI. Because the CIA is the lead federal agency for foreign intelligence collection, it will necessarily be a valuable source of information on global cyber threats. As the premier federal law enforcement agency, the FBI is in an excellent position to use CIA intelligence to conduct investigations and prosecute cyber criminals. The CIA and FBI can apply lessons learned from the 9/11 attacks to facilitate better integration of their cybersecurity operations, providing a blueprint for improving IC-wide cybersecurity integration.

In the wake of the 9/11 attacks, federal officials recognize that the historical "wall" between intelligence agencies and law enforcement agencies could

12 We are careful here to distinguish between monitoring and regulation. The former (which we favor) involves passive collection and analysis of information. The latter involves actively controlling individual or organizational access to Internet resources, with or without legal justification.

unnecessarily encumber investigations of suspected terrorists (Department of Justice 2004). Information sharing between intelligence agencies and law enforcement agencies can be valuable in counterterrorism, because it can make investigations and prosecutions easier. In part, the USA PATRIOT Act served to lower the "wall" between intelligence agencies and law enforcement agencies (*Ibid*.). Section 504 of the PATRIOT Act specifically allows for this kind of information sharing between law enforcement and intelligence agencies in terrorism cases, other cases where there is potential for "grave hostile acts" (though not necessarily terrorism), and when there is covert intelligence collection being conducted by a foreign power against the United States (USA PATRIOT Act 2001).

It may be possible for the IC to apply Section 504 of the USA PATRIOT Act to cybersecurity cases as well as terrorism cases. For example, a company attacked by hackers might call in the FBI to conduct forensic analysis on the attack. With the company's permission, the FBI might then pass forensic information about the attack on to the CIA. The CIA, in turn, could use this information to adjust its own overseas intelligence collection requirements. After collecting new intelligence overseas, the CIA could pass what it has learned on to the FBI, which could use that new information to better identify and prosecute those responsible for the attack. This kind of information sharing between the CIA and FBI is very much in the original spirit of the Act. This CIA-FBI information sharing could also be a valuable model for the other member agencies of the IC, and could help to better protect public and private information systems. And achieving this level of operational integration within the IC requires focused, sustained leadership from the Office of the Director of National Intelligence (ODNI), which oversees the IC.

3.5 Finding A Quarterback

The federal government needs a "quarterback" for cybersecurity. This problem is similar to those encountered by the federal government prior to the 9/11 attacks. The 9/11 Commission noted in its final report that, in the lead-up to the attacks, it appeared that no one was in charge of government-wide counterterrorism efforts:

> In our hearings we regularly asked witnesses: Who is the quarterback? The other players are in their positions, doing their jobs. But who is calling the play that assigns roles to help them execute as a team? Since 9/11, those issues have not been resolved (National Commission on Terrorist Attacks Upon the United States 2004: p. 400).

The analysis above shows that no one federal entity is leading cybersecurity efforts. The President, as leader of the federal executive branch, theoretically acts as the "quarterback" for federal cybersecurity efforts, pushing executive branch agencies to better integrate their cybersecurity operations. In practice, however, the President delegates this responsibility to the White House Coordinator for Cybersecurity, or "cyber czar." But at the time of this writing, there has been no formal "cyber czar" since Howard Schmidt left the position in May 2012 (The White House 2013). At least one report suggests that Schmidt left partly out of frustration – his position had great responsibility, but little actual authority or influence upon federal cybersecurity policy (Tuutti 2012). Absent changes in the Coordinator's job description, it is reasonable to expect Schmidt's successor to encounter similar frustrations.

But post-9/11 intelligence reforms offer a model for creating a federal cybersecurity quarterback with the authority needed to integrate federal cybersecurity efforts more effectively. In 2004, Congress created the ODNI position in order to institute a "quarterback" for the IC's seventeen member agencies (ODNI n.d.; Seventeen Agencies and Organizations United Under One Goal n.d.). The ODNI was given the authority to oversee the budgets, strategy, and agenda of the IC as a whole. In this way, the federal government helped ensure that IC member agencies were working in concert, sharing information, and better meeting the intelligence needs of policymakers.

A new office outside the White House – the Office of the National Coordinator for Cybersecurity (ONCC) – could play an ODNI-like role in synchronizing federal cybersecurity policy, including post-cyber incident mitigation activities. Like the ODNI, it would be important for Congress to provide this position with budgetary and legal authority to steer federal cybersecurity initiatives. It is only through these authorities that the ONCC would be able to shape federal cybersecurity priorities.

The National Coordinator for Cybersecurity – the specific person who would head the ONCC – would likely also be a Presidential appointee subject to Senate confirmation. Because the ONCC would be located organizationally and physically outside the White House, this position could avoid being politicized in a way that would not be possible if it were located in the White House. And over time, the ONCC could begin to implement a clear, measurable federal cybersecurity agenda, divide cybersecurity responsibilities among different agencies, and help government organizations to work together more effectively. Once the ONCC is in place, the White House Coordinator of Cybersecurity position could be scrapped, because it would no longer be necessary. Although cybersecurity intelligence operations would still need to be coordinated with the ODNI, this office could go a long way toward integrating current federal approaches to cybersecurity.

4 Conclusions

In September 2012 Congressional testimony, FBI Director Robert Mueller observed that "cyber security may well become our highest priority in the years to come" (Mueller 2012). Five months later the White House released a new presidential decision directive (PDD) about resilience and critical infrastructure protection. This PDD made protecting critical infrastructure from cyber threats and protecting critical infrastructure from physical threats co-equal federal priorities (The White House 2013). In a March 2013 worldwide threat assessment, Director of National Intelligence (DNI) James Clapper underscored the growing importance of cyber threats before turning to more familiar topics like terrorist groups and nuclear proliferation (Clapper 2013). The FBI, DHS, and US Air Force are aggressively hiring thousands of new cybersecurity specialists (Federal Bureau of Investigation 2012; Johnson 2012; Slabodkin 2013). Given the prominence that cyber threats have taken within the federal government, it is all the more important to address challenges to post-cyber incident mitigation.

For this enormous growth to be effective, there is an urgent need to integrate and streamline the federal approach to cybersecurity. As we have argued, however, the current approach to post-cyber incident mitigation remains problematically divided. To address the requirements of post-cyber incident mitigation, greater legal, cultural, and technological integration among DOD, DHS, the White House, and the IC is necessary to enhance current capabilities.

Some might claim that the 2010 DHS-DOD MOA on cybersecurity already points in this direction. Others could highlight joint DOD-DHS planning, training, exercising, and day-to-day operations – all of which show that both agencies are taking steps toward integrating their cybersecurity activities (DHS and DOD 2010). While acknowledging the benefits of these steps, a cohesive approach to cybersecurity now requires far more integration than we see in the status quo. This article's recommendations represent a next step in this evolutionary process.

However, a great deal would still need to be done. In addition to the federal level, future research is also needed in this area related to the role of state and local governments in cybersecurity. Appropriate funding levels for local and state cybersecurity initiatives, and the degree to which these initiatives interface with federal programs, remain unclear. Additional surveys of DOD, DHS, CIA, and FBI officials' own views about their roles in cyber conflict and post-incident mitigation would also help clarify understanding of how these agencies see their responsibilities in federal cybersecurity policy. Finally, there is a need for greater access to data on cyber incidents. It is publically known that US government computer systems are attacked thousands of times per day (Lynn 2010). Making more information about these attacks publically available for analysis would be

helpful to scholars in determining new ways to understand and respond to cybersecurity threats.

The expanding US dependence on IT means that cybersecurity policy will remain a topic of significant interest for the years ahead. It is now helpful to question whether certain historical barriers in the federal government remain useful for post-cyber incident mitigation. Cyber threats recognize no organizational boundaries. In countering them, perhaps the United States should not, either.

References

Alexander, Keith (2010) "U.S. Cybersecurity Policy and the Role of USCYBERCOM." Transcript of Remarks at the Center for Strategic and International Studies Cybersecurity Policy Debate Series. Retrieved May 1, 2012, from csis.org: http://csis.org/files/attachments/100603csis-alexander.pdf

Armed Forces (2012) Title 10, United States Code.

Ashford, Warwick (2013) Former US Cyber Czar Howard Schmidt tells Business not to Wait for Government. Retrieved March 22, 2013, from computerweekly.com: http://www.computerweekly.com/news/2240177283/Former-US-cyber-czar-Howard-Schmidt-tells-business-not-to-wait-for-government.

Best, Richard A. (2011) *Covert Action: Legislative Background and Possible Policy Questions*. Washington, DC: Congressional Research Service.

Buchalter, Alice R. (2007) *Military Support to Civil Authorities: The Role of the Department of Defense in Homeland Defense*. Washington, DC: Federal Research Division, Library of Congress.

Busch, Nathan E. and Austen D. Givens (2012) "Public-Private Partnerships in Homeland Security: Opportunities and Challenges," Homeland Security Affairs, 8(1):1–24.

Busch, Nathan E. and Austen D. Givens (2013) "Achieving Resilience in Disaster Management: The Role of Public-Private Partnerships," Journal of Strategic Security, 6(2):1–19.

Center for the Protection of National Infrastructure (n.d.) Cyber Incident Response (CIR) Service. Retrieved June 4, 2013, from http://www.cpni.gov.uk/about/Who-we-work-with/cir/.

Center for Strategic and International Studies (2008) *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidence*. Washington, DC.

Center for Strategic and International Studies (2011) *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC.

Center for Strategic and International Studies (2013) *Significant Cyber Incidents Since 2006*. Washington, DC. Retrieved June 4, 2013, from http://csis.org/files/publication/130514_Significant_Cyber_Incidents_Since_2006_0.pdf.

Chabinsky, Steven R. (2010) "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line," Journal of National Security Law & Policy, 4:27–39.

Chesney, Robert M. (2012) "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," Journal of National Security Law & Policy, 5:539–629.

Chittister, Clyde G. and Yacov Y. Haimes (2011) "The Role of Modeling in the Resilience of Cyberinfrastructure Systems and Preparedness for Cyber Intrusions," Journal of Homeland Security and Emergency Management, 8(1):1–19.

Clapper, James R. (2013) Worldwide Threat Assessment to the Senate Select Committee on Intelligence. Retrieved March 22, 2013, from intelligence.gov: http://www.dni.gov/files/documents/Intelligence%20Reports/WWTA%20Remarks%20as%20delivered%2012%20Mar%202013.pdf.

"Cyber Incidents Hit 90% of U.S. Firms" (2011) The Information Management Journal, 8.

Deloitte (n.d.) Your Cyber Attack Mitigation Strategy? 'Offline' is not the Only Option. Retrieved June 3, 2013, from http://www.deloitte.com/assets/Dcom-Iceland/Local%20Assets/Documents/24607A%20Cyber%20attack.pdf.

Department of Defense (2009) Memorandum to the Secretaries of the Military Departments from Robert Gates, Secretary of Defense, Subject: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations. Retrieved April 13, 2012, from http://info.publicintelligence.net/OSD05914.pdf.

Department of Defense (2011) *Department of Defense Strategy for Operating in Cyberspace*.

Department of Defense (2013) Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. Retrieved June 4, 2013, from http://www.defense.gov/pubs/2013_china_report_final.pdf.

Department of Homeland Security and Department of Defense (2010) Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity. Retrieved April 13, 2012, from dhs.gov: http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

Department of Homeland Security (n.d.) Office of Cybersecurity and Communications. Retrieved March 22, 2013, from dhs.gov: http://www.dhs.gov/office-cybersecurity-and-communications.

Department of Homeland Security (2010) *National Cyber Incident Response Plan* [Interim Version].

Department of Justice (2004) Report From The Field: The USA PATRIOT Act At Work. Retrieved March 22, 2013, from http://www.justice.gov/olp/pdf/patriot_report_from_the_field0704.pdf.

Dipert, Randall R. (2010) "The Ethics of Cyberwarfare," Journal of Military Ethics, 9(4):394–410.

Doyle, Charles (2002) The USA Patriot Act: A Sketch. Retrieved May 7, 2012, from http://www.fas.org/irp/crs/RS21203.pdf.

Dunlap, Charles J. (2011) "Perspectives for Cyber Strategists on Law for Cyberwar," Strategic Studies Quarterly, 5(1):81–99.

Etzioni, Amitai (2011) "Cybersecurity in the Private Sector," Issues in Science and Technology, 28(1):58–62.

Federal Bureau of Investigation (2012) National Cyber Security Awareness Month 2012: Are You the Weakest Link? Retrieved March 22, 2013, from fbi.gov: http://www.fbi.gov/news/news_blog/national-cyber-security-awareness-month-2012.

Federal Emergency Management Agency (2013) Cyber Attack. Retrieved June 4, 2013, from http://www.ready.gov/cyber-attack.

Federal Laboratory Consortium for Technology Transfer (2013) Spotlight On: Air Force Research Laboratory-Rome Research. Retrieved March 22, 2013, from Site: http://www.flcnortheast.org/200607_03.html.

Fischer, Eric A. (2011) *Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions*. Washington, DC: Congressional Research Service.

Flowers, Angelyn, Sherali Zeadally and Acklyn Murray (2013) "Cybersecurity and US Legislative Efforts to address Cybercrime," Journal of Homeland Security and Emergency Management, 10(1):1–27.

Givens, Austen D. and Nathan E. Busch (2013a) "Information Sharing and Public-Private Partnerships: The Impact on Homeland Security," Homeland Security Review 7(2), forthcoming.

Givens, Austen D. and Nathan E. Busch (2013b) "Realizing the Promise of Public-Private Partnerships in US Critical Infrastructure Protection," International Journal of Critical Infrastructure Protection, 6(1):39–50.

Grewe, Barbara A. (2004) Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations. Commission on Terrorist Attacks Upon the United States Staff Monograph. Retrieved May 7, 2012, from: http://www.fas.org/irp/eprint/wall.pdf.

Groll, Elias (2013) NSA Swears Its Spy Programs Are No Big Deal in PRISM Spin War, Round Two. Retrieved July 17, 2013, from foreignpolicy.com: http://blog.foreignpolicy.com/posts/2013/06/17/prism_spin_war_round_two_nsa_swears_its_intel_programs_are_no_big_deal.

Guinchard, Audrey (2011) "Between Hype and Understatement: Reassessing Cyber Risks As Security Strategy," Journal of Strategic Security, 4(2):75–96.

Harknett, Richard J. and James A. Stever (2009) "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen," Journal of Homeland Security and Emergency Management, 6(1):1–14.

Harknett, Richard J., John P. Callaghan and Rudi Kauffman (2010) "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," Journal of Homeland Security and Emergency Management, 7(1):1–24.

Hayden, Michael (2011) *The Cyber Threat*. Statement for the Record, House Permanent Select Committee on Intelligence. Retrieved March 22, 2013, from http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingHayden.pdf.

Hollis, David M. (2010) "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," Joint Forces Quarterly, 58(3):48–53.

Homeland Security Act (2002) Pub. L. No. 107-296, 116 STAT. 2135.

Johnson, Nicole (2012) DHS to Hire 600 Cyber Professionals. Retrieved March 22, 2013, from federaltimes.com: http://blogs.federaltimes.com/federal-times-blog/2012/10/31/dhs-to-hire-600-cyber-professionals/

Kaiser, Tiffany (2011) Former CIA/NSA Head: Cyber Security Threats 'Horribly Overclassified.' Retrieved March 22, 2013, from dailytech.com: http://www.dailytech.com/Former+CIANSA+Head+Cyber+Security+Threats+Horribly+OverClassified/article22953.htm.

Kaplan, Jeremy A. (2010) Beware of Link: E-Mail Virus Plays Havoc with Internet. Retrieved May 16, 2012, from foxnews.com: http://www.foxnews.com/scitech/2010/09/09/beware-link-e-mail-virus-plays-havoc-internet/.

Lowenberg, Timothy J. (n.d.) The Role of the National Guard in Homeland Defense and Homeland Security. National Guard Association of the United States. Retrieved May 7, 2012, from: http://www.ngaus.org/ngaus/files/ccLibraryFiles/Filename/000000000457/primer%20fin.pdf.

Lynn, William J. (2010) "Defending a New Domain," Foreign Affairs, 89(5):97–108.

Mandiant (2013) APT1: Exposing One of China's Cyber Espionage Units. Retrieved March 22, 2013, from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

McConnell, Michael, Michael Chertoff and William Lynn (2012) "China's Cyber Thievery Is National Policy – And Must Be Challenged," *The Wall Street Journal*, Retrieved June 4, 2013 from ABI/INFORM Complete.

McCullagh, Declan (2012) Opposition Grows to CISPA 'Big Brother' Cybersecurity Bill. cnet.com. Retrieved May 16, 2012, from http://news.cnet.com/8301-31921_3-57419540-281/opposition-grows-to-cispa-big-brother-cybersecurity-bill/.

McGraw, Gary (2013) "Cyber War Is Inevitable (Unless We Build Security In)," Journal of Strategic Studies, 36(1):109–119.

Mills, Elinor (2010) 'Here You Have' Virus Spreading Through the Internet. CBSNews.com. Retrieved May 16, 2012, from: http://www.cbsnews.com/8301-501465_162-20016098-501465.html?tag=contentMain;contentBody.

Mueller, Robert (2012) Statement before the Senate Committee on Homeland Security and Governmental Affairs. Retrieved March 22, 2013, from fbi.gov: http://www.fbi.gov/news/testimony/homeland-threats-and-agency-responses.

Mueller, Robert (2013) Remarks at RSA Cyber Security Conference. Retrieved March 22, 2013, from fbi.gov: http://www.fbi.gov/news/speeches/working-together-to-defeat-cyber-threats.

Nakashima, Ellen (2010a) "White House Declassifies Outline of Cybersecurity Program," *The Washington Post*. Retrieved May 17, 2012, from: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030202113.html.

Nakashima, Ellen (2010b) "Pentagon is Debating Cyber-Attacks," *The Washington Post*. Retrieved May 15, 2012, from http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507464.html.

Nakashima, Ellen (2013a) "U.S. said to be Target of Massive Cyber-Espionage Campaign," *The Washington Post*. Retrieved June 4, 2013 from http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html.

Nakashima, Ellen (2013b) "Confidential Reports Lists Weapons System Designs Compromised by Chinese Cyberspies." *The Washington Post*. Retrieved June 4, 2013, from http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

National Commission on Terrorist Attacks Upon the United States (2004) The 9/11 Commission Report. Retrieved March 22, 2013, from http://www.9-11commission.gov/report/911Report.pdf.

National Institute of Standards and Technology (2011) *National Initiative for Cybersecurity Education Strategic Plan: Building a Digital Nation* [DRAFT].

Newmeyer, Kevin P. (2012) "Who Should Lead U.S. Cybersecurity Efforts?" Prism, 3(2): 115–126.

Nojeim, Greg T. (2010) "Cybersecurity and Freedom on the Internet," Journal of National Security Law & Policy, 4:119–137.

Office of the Director of National Intelligence (n.d.) Intelligence Reform and Terrorism Prevention Act of 2004. Retrieved March 22, 2013, from dni.gov: http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-irtpa.

Sanger, David E. (2013) "U.S. Blames China's Military Directly for Cyberattacks," *The New York Times*. Retrieved June 4, 2013, from http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all&_r=0;.

Sanger, David E. and John Markoff (2009) "Obama Outlines Coordinated Cyber-Security Plan," *The New York Times*. Retrieved May 17, 2012, from: http://www.nytimes.com/2009/05/30/us/politics/30cyber.html.

Schneider, Anne and Helen Ingram (1990) "Behavioral Assumptions of Policy Tools," The Journal of Politics, 52(2):510–529.

Seventeen Agencies and Organizations United Under One Goal (n.d.) intelligence.gov Retrieved March 22, 2013, from intelligence.gov: http://www.intelligence.gov/about-the-intelligence-community/.

Sharp, Walter G. (2010) "The Past, Present, and Future of Cybersecurity," Journal of National Security Law & Policy, 4:13–26.

Shaughnessy, Larry (2011) 10 Years of War: Missiles and Horses. Retrieved May 17, 2012, from cnn.com: http://security.blogs.cnn.com/2011/10/03/war-in-afghanistan-started-with-cruise-missiles-stealth-bombers-and-horses/.

Slabodkin, Greg (2013) Air Force Plans to Hire 1,000 Cyber Warriors Starting in Fiscal 2014. Retrieved March 22, 2013, from fiercegovernmentit.com: http://www.fiercegovernmentit.com/story/air-force-Plans-Hire-1000-Cyber-Warriors-Starting-Fiscal-2014/2013-01-23.

Toomer, Jeffrey K. (2002) A Strategic View of Homeland Security: Relooking the Posse Comitatus Act and DOD's Role in Homeland Security. Retrieved April 21, 2012, from dtic.mil: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA403866.

Tuutti, Camille (2012) What Cyber Czar's Departure Means for White House Cyber Priorities. Retrieved March 24, 2013, from fcw.com: http://fcw.com/articles/2012/05/22/howard-schmidt-impact-cyber-priorities.aspx.

The White House (2003) Homeland Security Presidential Directive 5: Management of Domestic Incidents. Retrieved April 13, 2012, from http://www.fas.org/irp/offdocs/nspd/hspd-5.html.

The White House (2009a) Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Retrieved July 18, 2013, from http://www.whitehouse.gov/documents/cyberspace_policy_review_final.pdf.

The White House (2009b) Remarks By The President On Securing Our Nation's Cyber Infrastructure. Retrieved May 1, 2012, from http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

The White House (2010) *Comprehensive National Cybersecurity Initiative.*

The White House (2011) International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Retrieved July 18, 2013, from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

The White House (2013) Presidential Policy Directive – Critical Infrastructure Security and Resilience. Retrieved March 22, 2013, from http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

United States Computer Emergency Readiness Team (n.d.) About Us. Retrieved June 4, 2013, from https://www.us-cert.gov/about-us/.

Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 STAT. 272 (2001).

U.S. Army Corps of Engineers (2011) Hurricane and Storm Damage Risk Reduction: Background Information. Retrieved May 17, 2012, from http://www.mvn.usace.army.mil/hps2/hps_background.asp.

"U.S. Cities, States Fight PATRIOT Act" (2003) *The Information Management Journal*, 12.

U.S. Government Accountability Office (2011a) *Cybersecurity: Continued Attention Needed to Protect Our Nation's Cyber Infrastructure.* Statement of Gregory C. Wilshusen Before the

Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, U.S. House of Representatives.

U.S. Government Accountability Office (2011b) *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities.* Report No. GAO-11-75.

U.S. Government Accountability Office (2011c) *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities.* Report No. GAO-11-421.

Westby, Jody R. (2007) *Homeland Security v. Homeland Defense: Gaps Galore*. Paper for St. Mary's University School of Law, Center for Terrorism Law.

White, Brian M. and Gus P. Coldebella (2010) "Foundational Questions Regarding the Federal Role in Cybersecurity," Journal of National Security Law & Policy, 4:233–245.