AIR WAR COLLEGE

AIR UNIVERSITY

A NATIONAL SOLUTION:

RETHINKING THE EMPLOYMENT OF AIR NATIONAL GUARD TITLE 32 STATUS CITIZEN-AIRMEN TO DEFEND THE NATION'S CYBERSPACE INFRASTRUCURE

by

Maurice M. McKinney, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Jill Singleton, USAF

14 February 2013

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Maurice M. McKinney is a U.S. Air Force Cyberspace officer assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from Roosevelt University in 1994 with a Bachelor of General Studies degree in Computer Science, Northwestern University in 1999 with a Masters of Information Technology, Air University in 2006 with a Masters in Military Operational Art and Science, and University of Maryland University College in 2011 with a Doctor of Management.

Lt Col McKinney has served on numerous active duty assignments to include volunteering for U.S. Air Forces Central (USAFCENT) special assignments in both Operation Iraq Freedom (OIF) and Operation Enduring Freedom (OEF). He is also a graduate of the AF's Air Command and Staff College (ACSC) residence program where he received the 2006 Armed Forces Communications and Electronics Association (AFCEA) research honor award. He has previously published papers on Transformational Satellite (TSAT) communications and China's global telecommunications expansion.

Abstract

This research contributes to the national discussion regarding the employment of Air National Guard Title 32 status citizen-airmen to conduct cyberspace operations. The author argues that the Air National Guard's role in defending the nation against cyber-attacks is unclear and that policy makers must enact legislation that authorize and fund the employment of ANG members in a Title 32 state, versus federal, status to conduct cyberspace operations. This paper offers viable solutions for clarifying the Air National Guard's role in defending the nation against cyber-attacks.

Using an evidence-based research approach that includes systematic reviews of national and military cyberspace policy, Title 10 and Title 32 authorities, case studies, and military doctrine, the author recommends that president and Congress enact Title 32 legislation that authorizes and funds the employment of Air National Guard members in a Title 32 state, versus federal, status to conduct cyberspace operations.

The author also recommends creating a National Guard Cybersecurity Program and adding it to the National Guard Capabilities for Domestic Operations program. The author presents a National Guard Cybersecurity Program conceptual model that illustrates one approach for institutionalizing and organizing Air National Guard cyber forces to support federal and state cyberspace operations.

Additionally, the paper recommends the creation of two Air National Guard cybersecurity programs that strategically place Title 32 status cyber professionals at the Department of Homeland Security, National Security Agency, Federal Bureau of Investigation, United States Cyber Command, Office of the White House Cybersecurity Coordinator, and 54 States, Territories, and District of Columbia.

Introduction

> *A cyber 9/11 could happen imminently. We shouldn't wait until there is a 9/11 in the cyber world. There are things we can and should be doing right now that, if not prevent[sic], would mitigate the extent of damage.*
>
> -Janet Napolitano
> Speech at the Wilson Center, Washington, DC, 24 January 2013

In this quote, an Obama administration official, once again, sounds the proverbial alarm that a cyber-attack against the U.S. is imminent and may have devastating effect on the nation's critical infrastructure. [1] If this alarm were sounded following the U.S. Forest Service warning of wildfires that threatened loss of life or damage to the nation's critical infrastructure, the Air National Guard's (ANG) Modular Airborne Fire Fighting System (MAFFS) air crews would be called to help suppress the fires. [2] Yet, when the Department of Homeland Security (DHS), the federal department "responsible for overseeing the protection of the .gov domain and for providing assistance and expertise to private sector owners and operators" explicitly states a 9/11-type cyber-attack could happen imminently, the ANG has no authority to prepare for or respond to cyber-attacks against the nation's critical infrastructures. [3]

The ANG plays an important supportive role in domestic operations (DOMOPS). For example, the ANG's 109th Airlift Wing provides airlift support to the National Science Foundation's (NSF) United States Antarctic Program (USAP). In this partnership the ANG provides air crews and facilities and the NSF funds and manages the program.

The ANG also supports DoD's Air Sovereignty Alert (ASA) operations program. The ASA operations program was initiated following the 9/11 attacks and is a component of Operation Noble Eagle.[4] The ASA operations are conducted by 18 ANG units. At all 18 ASA sites both ANG and active-duty personnel are "dual-tasked" to conduct Operation Enduring

Freedom (OEF) missions and ASA operations.[5] ASA operations consist of ground operations that take place before fighter aircraft take off. However, once the fighter aircraft takes off, an ANG pilot automatically converts from state Title 32 status to federal Title 10 status.

Unfortunately, as of February 2013, there is no legislation, written or pending, that authorizes and funds the integration and employment of ANG cyberspace forces, in a Title 32 status, to prepare for or respond to cyber-attacks against the homeland. Therefore, the ANG has no authority to prepare for or respond to cyber-attacks against the nation's critical infrastructures. Furthermore, the ANG's role in defending the nation against cyber-attacks is not considered a DOMOPS program. It is not written in any Air Force or Joint doctrine; nor is it codified in Title 32 authority. Consequently, the ANG's role in defending the nation against cyber-attacks is unclear.

The paper's argument is that the ANG's role in defending the nation against cyber-attacks is unclear and that policy makers must enact legislation that authorize and fund the employment of ANG members in a Title 32 state, versus federal, status to conduct cyberspace operations. This paper proposes solutions that policy makers should consider in authorizing and funding the use of ANG personnel, in a Title 32 state status, to conduct cyberspace operations.

Research Relevance

This research comes at a time of increased interest and concern about cybersecurity. First, the President of the United States (POTUS) has declared that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation" and protecting the "digital infrastructure" is a national security priority.[6] Second, the House Committee on Armed Services (hereafter referred to as the "House Committee") wants to know how National Guard computer network defense (CND) units will be

affected when activated in a Title 32 or State Active Duty (SAD) status."[7] The House Committee added language in the Fiscal Year (FY) 2013 *National Defense Authorization Act* (NDAA) that directs the Secretary of Defense (SECDEF) to brief the House Committee on a "…description of what activities these units may be expected to perform when activated in a title 32 [*sic*] or State Active Duty-status, and the policies and authorities that are in place to govern those activities."[8] The briefing is due by 2 July 2013.[9]

Third, the DHS needs additional cybersecurity professionals to supplement their cyberspace homeland defense mission.[10] Fourth, the DoD is looking at ways to increase U.S. Cyber Command's (USCYBERCOM) cyberspace resources.[11] Fifth, the Air Force (AF) wants stronger integration of Title 32, USC, National Guard, Title 10, USC, Armed Forces, and Title 50, USC, War and National Defense, roles and responsibilities.[12]

Finally, the National Governors Association (NGA) perceives that "…cybersecurity is the weakest link in their efforts to protect critical infrastructure assets in their individual states"[13] and are taking steps to "…examine the role state policy can and should play in ensuring adequate cybersecurity…."[14] For all the reasons listed above, it is important to rethink the employment of ANG Title 32 status citizen-airmen to defend the nation's cyberspace infrastructure.

This paper uses the terms *cyberspace* and *cyberspace operations* as defined in Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. It defines *cyberspace* as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers; and *cyberspace operations* is defined as the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace.[15]

Authorities

Title 32 and State Active Duty

The U.S. Constitution authorizes the National Guard (NG) to serve based on Title 32 authorities. The NG maintains a "dual status" to support federal and state missions.[16] In their dual status, ANG personnel have the ability to organize, train, and equip for homeland defense support and wartime combat operations.

When ANG members perform duty under Title 32 they are under the command of their respective state governor. As shown in Table 1, ANG members may perform duty in an array of service types, duty types, training categories, and Title 10 and Title 32 authorities. Airmen who are on Inactive Duty for Training (IDT) are funded by the federal government and usually perform training one weekend a month and 15 days per year. Airmen in IDT status are prohibited from performing duty other than training and regulations limit their annual training days.

Table 1: Duty Relationships

Service Type	Type Duty	Training Category	Title
Inactive Duty	IDT	AFTP TPPA UTA PT	32 32 32 32
AD or FTNGD	ADOT	ADOS AGR MPA STAT TOUR	10/32 10/32 10 10
	ADT	IADT FST AT ST	10/32 10/32 10/32 10/32

Adapted from Air National Guard Instruction 36-2001, *Management and Training Operational Support within the Air National Guard*, 19 October 2009.

Airmen who perform Active Duty for Training (ADT) or Active Duty for Other Than Training (ADOT) can be placed on Title 32 or Title 10 orders. Airmen in ADT status may perform

Annual Training (AT) or Formal School Training (FST). Airmen in ADOT status can support active or reserve component missions. State governors may also activate ANG personnel to Full-Time National Guard Duty (FTNGD) status for homeland defense missions under the authority of Title 32, subsection 502(f). This authority provides the Governor with the ability to maintain command and control of the Airmen, and the federal government provides the pay and allowances. When activated under Title 32, NG members are exemption from the Posse Comitatus Act (PCA). This exemption allows NG members to support federal, state, and local law enforcement agencies while under control of the state governor.

State governors my activate ANG personnel to a SAD status for state emergencies or homeland defense missions. Airmen activated in SAD status become state employees and are governed by state statue and paid using state funds. Similar to the Title 32 status, SAD status is exempt from the PCA.

Posse Comitatus Act

The PCA prohibits direct law enforcement assistance, including interdiction of vehicle, vessel, aircraft, or other similar activity; a search or a seizure; an arrest, apprehension, stop and frisk, or similar activity; and use of military personnel to surveillance or pursuit individuals.[17] The PCA applies to active duty military personnel in the Army and Air Force and National Guard personnel in specific Title 10 status.

Title 10

Title 10 authorizes and regulates active-duty military forces. The Army, Navy, Air Force and Marines serve based on Title 10. ANG members in Title 10 12301(d), 12302, and 12304 statuses are subject to the Posse Comitatus Act.

National and Military Cyberspace Policy and Initiatives

The cyber threat is one of the most serious economic and national security challenges we face as a nation.

-President Barack Obama
Remarks on securing U.S. cyber infrastructure
29 May 2009

This is a quote from President Obama's press briefing on 29 May 2009 announcing the release of the C*yberspace Policy Review*; the Obama administration's first attempt at developing a comprehensive national cyber strategy. It recommended 24 near-term and mid-term actions to ensure a coordinated response to significant cyber incidents.[18] Following the *Cyberspace Policy Review* release, a multitude of national and military cyberspace policies were published.

In December 2009, the White House created the Cybersecurity Office within the National Security Staff and named a Special Assistant to the President and Cybersecurity Coordinator (hereafter referred to as the "White House Cybersecurity Coordinator"). In May 2010, The White House released the *National Security Strategy* (NSS) that listed cybersecurity threats as "…one of the most serious national security, public safety, and economic challenges the U.S. faces as a nation."[19] It also solidified the nation's commitment to protecting and defending the homeland from cyber threats.

In May 2011, the Obama administration released the *International Strategy for Cyberspace*, describing its plans for engaging with the international community regarding cyber issues.[20] The common theme among the national cyber policies was to strengthen the nation's ability to defend against cyber-attacks. However, none of the national cyberspace policy documents mentioned integrating the NG into national cyberspace strategy.

Department of Defense (DoD) Cyberspace Policy

The DoD's cyberspace policies focus on defending military cyberspace infrastructure. On 23 June 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish USCYBERCOM. By 1 October 2010, USCYBERCOM achieved full operating capability, which included taking operational control (OPCON) of some Army, Air Force, Navy and Marine cyber organizations.

USCYBERCOM's mission is to plan, coordinate, integrate, synchronize, and direct activities to operate and defend the DoD information networks.[21] The ANG cyber forces are presented to USCYBERCOM as part of 24th Air Force (AFCYBER) reserve cyber forces. Unfortunately, two years and five months after USCYBERCOM's full operating capability was announced, the debate continues about how to integrate ANG cyber forces, in a Title 32 status, into AFCYBER and USCYBERCOM's missions.

The 2011 *Department of Defense Strategy for Operating in Cyberspace* provided five strategic initiatives for combating cyber threats and cyber adversarial activity. One initiative includes partnering with other U.S. government departments and agencies to "…enable a whole-of-government cybersecurity strategy."[22] This initiative formalized DoD's commitment to work with civil authorities, interagency partners, and private sector entities to collectively meet the nation's growing cyberspace threats.

In September 2010, Secretary of Defense Gates and Secretary of Homeland Security Napolitano signed a Memorandum of Agreement (MOA) regarding Cybersecurity.[23] The MOA promotes joint operational planning, improving public and private cybersecurity threat information sharing, and assists in de-confliction and synchronization of cybersecurity efforts.

This includes mutual support for cyber security capabilities development and synchronization of current operational cybersecurity mission activities.

Department of Homeland Security (DHS) Cyberspace Policy

The DHS published its own strategic cyberspace policies. The 2010 *Quadrennial Homeland Security Review* included safeguarding and securing cyberspace as a mission objective. The safeguarding and securing cyberspace objective outlines the department's intentions to prevent cyber adversaries from exploiting or attacking the nation's information infrastructure.[24] The DHS 2011 *Blueprint for a Secure Cyber Future* is a plan of action for securing the homeland from cyber threats—specifically, protecting critical information infrastructure and strengthening the cyber ecosystem and using "outcome-based metrics" to justify homeland security investments.[25]

The DHS understands that its cyber workforce needs to grow to provide adequate protection of the nation's cyber infrastructure. On 6 June 2012, Secretary of Homeland Security Napolitano announced the formation of a Task Force on CyberSkills. The group was given a two-part mandate: "first, to identify the best ways DHS can foster the development of a national security workforce capable of meeting current and future cybersecurity challenges; and second, to outline how DHS can improve its capability to recruit and retain sophisticated cybersecurity talent."[26] The Task Force on CyberSkills delivered 11 recommendations. Surprisingly, not one recommendation included integrating NG cyber forces to support DHS's cyber missions.

Air Force and ANG Cyberspace Policy

There are two primary documents that outline the AF's cyberspace vision and strategy: *Cyber Vision 2025* and Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations.* The AF's *Cyber Vision 2025* describes the AF plan to develop and employ its cyber forces over

the next 12 years. It recognizes that the National Guard has an important cyber role and recommends stronger integration of Title 10, 32, and 50 roles and responsibilities.[27] Air Force Directive Document (AFDD) 3-12 codifies the AF's approach to cyberspace operations and outlines the command, control, and organization of its cyberspace forces.[28]

The ANG has approximately 8,500 cyberspace professionals.[29] They are organized, trained, and equipped to support AFCYBER and Air Force Intelligence, Surveillance, and Reconnaissance's (AFISRA) cyberspace missions. As shown in figure 1, the ANG cyber force structure is currently aligned with AFCYBER and AFISRA organizations.[30] While this organizational construct aligns neatly with supporting Title 10 military cyberspace operations, it falls short of identifying how ANG cyber forces, in a Title 32 status, could support other key federal and state organizations in meeting their homeland cybersecurity missions.

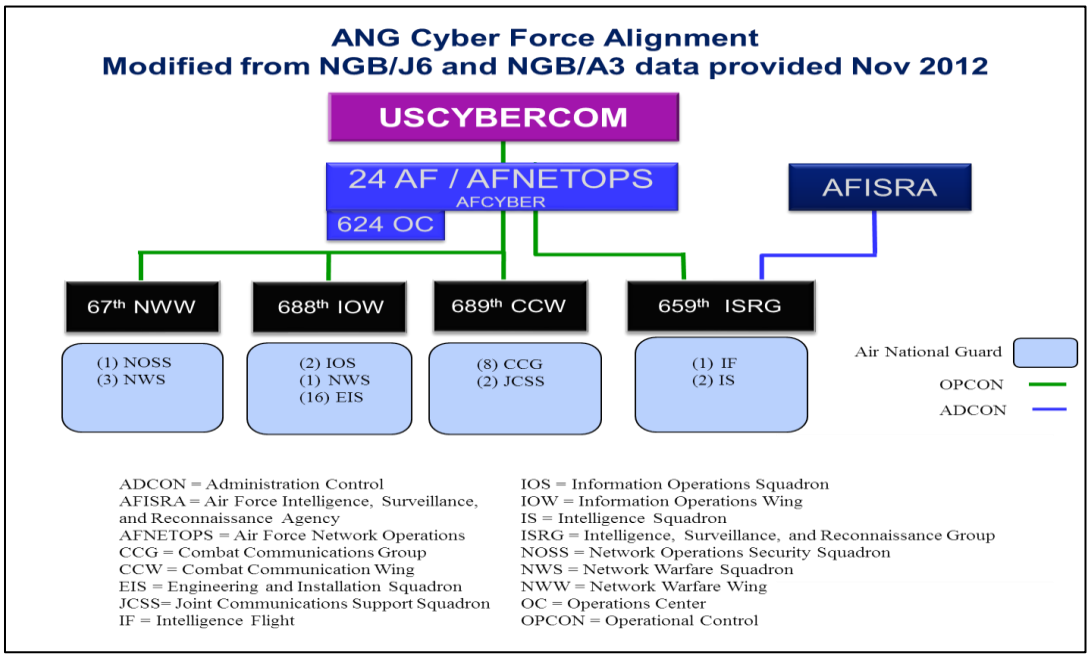

Figure 1. ANG Cyber Force Alignment. Adapted from COL David L. Collins, "National Guard Cyber Force Presentation," National Guard Bureau, 8 November 2012

For example, it does not show how ANG cyber forces, in a Title 32 status, could support the DHS's National Cybersecurity and Communications Integration Center (NCCIC) in its cyber

mission of safeguarding and securing cyberspace;[31] nor does it clearly show how ANG cyber forces, in a Title 32 status, could provide support to the FBI's National Cyber Investigative Joint Task Force (NCIJTF) mission. Furthermore, it fails to illustrate how ANG cyber forces, in a Title 32 status, could support the White House Cybersecurity Coordinator, and it does not show how ANG cyberspace forces, in a Title 32 status, could provide support to NSA's Central Security Service (CSS) Threat Operations Center (NTOC).

Analysis

Research confirms that national and military cyberspace policy and initiatives focus on employing Title 10 active-duty cyber forces to conduct military cyberspace operations, but lack solutions for integrating Title 32 National Guard cyber forces to support cyberspace operations. The evidence also shows that existing Title 32 authority and Air National Guard Instructions (ANGI) authorize the automatic conversion from Title 32 to Title 10 if a specific Title 10 response is required.

Based on the evidence findings, this paper suggests that three National Guard cyber programs be created: National Guard Cybersecurity Program (NGCSP), ANG Cyber Sovereignty Alert Program (ANG-CSAP), and ANG Cybersecurity Teams (ANG-CST). Creating the proposed programs requires modifying existing authorities, finding new funding streams, and effectively utilizing cyberspace personnel. The following sections discuss some of the advantages, limitations, and restrictions of implementing the three programs.

Advantages

Creating the three National Guard cyber programs offers several advantages. First, the three programs would institutionalize the employment of ANG Title 32 status citizen-airmen to defend the nation's cyberspace infrastructure. In particular, the programs would provide

dedicated cyber personnel to prepare for and respond to cyber threats and cyber-attacks against the nation. Additionally, the programs would also allow clear tracking of ANG Title 32 status citizen-airmen cyber skills, cyber warfare equipment, and cyber personnel readiness. The programs would also authorize programmed funding, training and equipment refresh cycles.

Second, Title 32 allows the Secretary of Defense (SECDEF) to provide funds to a Governor to employ National Guard units or members to conduct homeland defense activities the SECDEF determines are necessary and appropriate.[32] The SECDEF could use this authority to fund the three programs. Additionally, the ANG could request funds from DHS to support domestic cyberspace operations. The Washington National Guard (WNG), in fact, has received some grant funding from DHS—albeit small, the gesture demonstrates DHS willingness to support the development of state and local cyber response plans.[33]

Third, while in a Title 32 status, ANG personnel assigned to the three programs maintain Posse Comitatus Act (PCA) exemption.[34] This exemption allows NG members to support federal, state, and local law enforcement agencies while under control of the governor. However, once an ANG member converts to Title 10, they are no longer exempt from PCA.

Fourth, the three programs do not interfere with a governor's authority to activate ANG personnel to a SAD status for state emergencies or homeland defense missions. In fact, the three programs support the National Governors Association's (NGA) efforts to protect critical infrastructure assets in their individual states. [35]

Limitations and Restrictions

There are several limitations for implementing the three programs. First, there are limited funds to employ ANG Title 32 cyber forces to defend the nation's cyberspace infrastructure. For the foreseeable future, the defense budget will continue to decrease and all

services must decide which programs they will fund. The ANG is no exception. The ANG must decide if growing cyberspace personnel is one their top priorities. If so, the ANG must decide how much funding to allocate toward growing cyberspace personnel at the expense of other programs.

Second, the three programs may require ANG cyber force structure tradeoffs. Currently, a majority of ANG cyber forces are assigned to legacy cyber missions in Combat Communications Squadrons (CBCS) and Engineering and Installation Squadrons (EIS). If the ANG decides to expand its emerging cyberspace forces into network warfare squadrons (NWS) and information operations squadrons (IOS), the initial manning should come from retraining CBCS and EIS cyber personnel. Of course, this decision rests with Air Force and ANG senior leaders.

Third, the "1095 restriction" limits time a NG member can stay on Military Personnel Appropriation (MPA) man-day orders before being counted against strength authorizations. [36] The 1095 restriction applies to National Guard and Air Force Reserve members that reach 1,095 days in a 1,460-day period. This law applies to National Guard members called to active-duty under Title 10 section 12301(d) and FTNGD under Title 10 section 502. [37]

Recommendations

Enact Title 32 Legislation

A national solution to integrate and employ NG cyber forces requires the President and Congress to enact Title 32 legislation that authorizes and funds three programs. The three programs should be authorized and funded for two reasons. The first reason is to establish a legal foundation for integrating and employing National Guard cyber forces, in a Title 32 status, to support federal and state cyberspace missions. The second reason is to prevent Title 32 and

Title 10 authority obstacles in the event a National Guard cyberspace operator, in a Title 32 status, needs to defend critical cyberspace infrastructure against a cyber-attack.

Create a National Guard Cybersecurity Program (NGSCP)

Similar to the National Guard Counterdrug Program (NGCD), the NGCSP should be a domestic operations (DOMOPS) program this is authorized and funded by the President and Congress.[38] The DoD and DHS should provide funds on an annual basis to governors of states that participate in the NGSCP. The NGCSP operations would be conducted using Title 32 authority under command and control of the state governors. As shown in figure 2, the NGSCP would provide management and oversight of the ANG CSAP and ANG-CST programs. The NGCSP leadership would be responsible for developing relationships and strategically placing ANG-CST cyberspace operators.

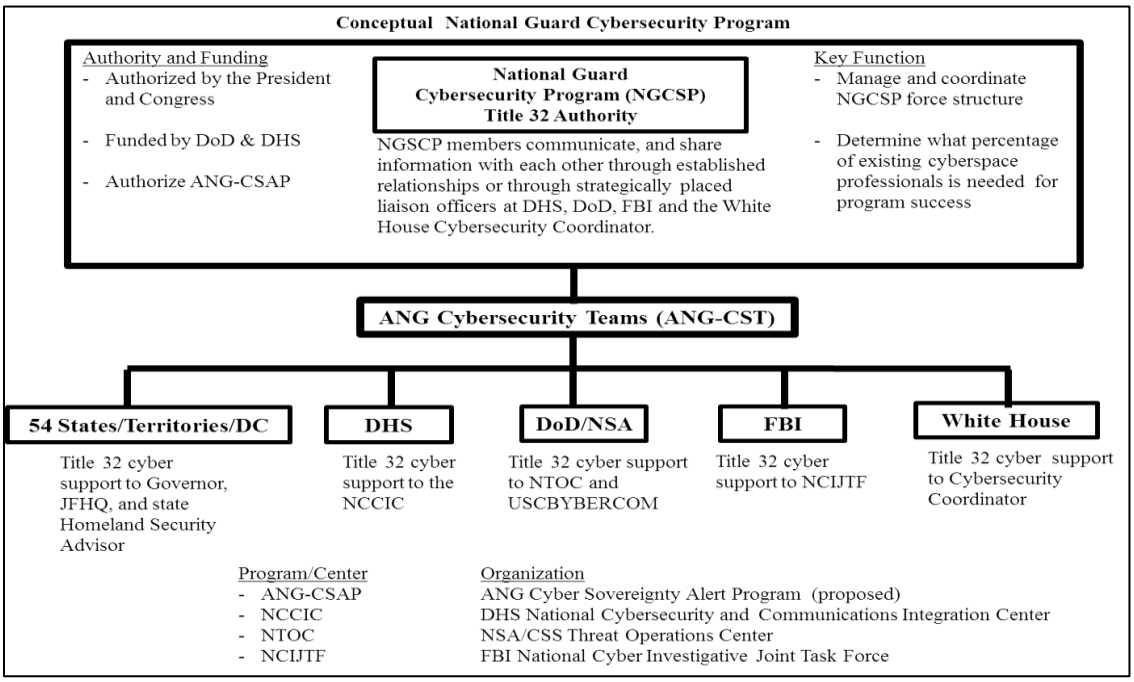

Figure 2. Conceptual National Guard Cybersecurity Program

As illustrated in Figure 2, ANG-CST members, in a Title 32 status, would be strategically placed within the 54 States, Territories and District of Columbia, DHS's National Cybersecurity

and Communications Integration Center (NCCIC), USCYBERCOM, NSA/CSS Threat Operations Center (NTOC), FBI's NCIJTF, and the Office of the White House Cybersecurity Coordinator.

Create an ANG Cyber Sovereignty Alert Program (ANG-CSAP)

Recognizing that cyberspace systems cross many borders and the reality that cyber-attacks happen in milliseconds, the ANG-CST members would need authority to defend against a cyber-attack. The ANG-CSAP program would allow ANG cyberspace operators to instantaneously convert from state Title 32 status to federal Title 10 status to conduct military cyberspace operations. The notion that ANG cyberspace operators can automatically convert from Title 32 and Title 10 is codified in ANG Instruction 10-203, *Air National Guard (ANG) Alert Resource Management*.

ANG Instruction 10-203 states that "ANG aircrew and ground support personnel can perform non-contingency alert duty in Title 32 FTNGD-OS, Title 32 Active Guard/Reserve (AGR) and Title 10. Provisions will be made to ensure members automatically convert to Title 10, if a specific Title 10 trigger is included in higher headquarters guidance. In accordance with 10 U.S.C., 12301(d), members…must sign a Title 10 consent statement prior to performing alert duty."[39] Naysayers might ask why would ANG cyber personnel need to automatically convert from Title 32 to Title 10. The following fictitious scenario may provide some insight on how and why the NGCSP, ANG-CSAP, and ANG-CST programs could achieve desired cyberspace operations effects.

Fictitious Scenario of Cyber Attack

Let's assume that policy makers enacted Title 32 legislation that authorized and funded the three proposed programs: NGCSP, ANG-CSAP, and ANG-CST. In accordance with the new

legislation, the chief of the National Guard Bureau (CNGB) decided that each state could assign a percentage of their cyber personnel to the NGCSP. The Maryland ANG decides to assign 20 percent of their cyberspace personnel to the NGCSP. The Title 32 legislation also authorized NGCSP members to be activated to Full-time National Guard-Operation Support (FTNGD-OS) status for homeland defense missions under the authority of Title 32, subsection 502(f) and assigned to ANG-CST.

Based on the tri-lateral memorandum of agreement (one of this paper's recommendation) between DOD, DHS and NGB, the Maryland ANG sends an ANG-CST member to the NTOC (also located in Maryland). Per the tri-lateral MOA, the ANG-CST member, in a Title 32 status, has performed cyberspace duties inside the NTOC at least one weekend per month. Also, per the tri-lateral memorandum of agreement (MOA), the ANG-CST member has a top secret clearance and credentials to access NTOC's classified system.

The NSA has credible intelligence that a cyber-attack is imminent against the nation's critical infrastructure. The NSA, USCYBERCOM and DHS have determined that additional cyber resources are needed to defend against the cyber-attack. Per the tri-lateral MOA, the NTOC leadership sends a request to the Maryland ANG for cyberspace operations support. The Maryland ANG sends the ANG-CST member that's familiar with NTOC's cyberspace mission and operations.

The ANG-CST team member is tasked to monitor classified systems to determine if threats and vulnerabilities are present in military networks. While monitoring the classified systems, she notices what appears to be the initial phase of a cyber-attack against one of the nation's critical infrastructures. Within seconds, she determines that the cyber-attack source is coming from computers in China, Iran, and Russia. Since she is part of the NGCSP, her orders allow automatic conversion from Title 32 to Title 10. Within seconds, she stops the cyber-attack and prevents the

cyber adversary from installing remote access software and computer viruses on critical cyber infrastructure systems.

This fictitious scenario demonstrated how ANG cyber forces could support a federal agency in achieving desired cyberspace effects. Similar support could apply to other federal and state departments and agencies such as USCYBERCOM, DHS's NCCIC, FBI's NCIJTF and State's crisis action centers.

Title 32 Support to 54 States, Territories and the District of Columbia

The NGB should collaborate with the National Governors Association to discuss the possibility of conducting state specific critical cyberspace infrastructure assessments. At least one State CIO has taken advantage of the ANG's cyberspace expertise and conducted a cyberspace assessment of their state's cyber infrastructure. The WNG approach to supporting domestic cyberspace operations is an exemplar for developing state-centric ANG-CST. The WNG's approach to domestic cyberspace operations is an exemplar because they did not wait for federal policy makers to enact legislation on how to best protect Washington State's critical infrastructures.

In the absence of federal legislation, the WNG worked with the governor, the state's homeland security advisor, and numerous state agencies to create and fund aspects of their state's cyberspace response plan. For example, the WNG developed a Concept of Operations (CONOPS) for Domestic Cyberspace Response (DCR) that provides cyberspace response options for the Governor of Washington State and the State Homeland Security Advisor.[40] They also used a DHS Homeland Security (HLS) grant to develop a state-wide cyber critical infrastructure response plan. [41] While this approach has limitations such as programmed funding, it does provide an exemplar for other states to follow if they are interested in creating a state centric cyberspace response program.

Create a Memorandum of Agreement (MOA) with DHS and USCYBERCOM

The CNGB, secretary of defense, and secretary of homeland security should consider a tri-lateral cybersecurity MOA that integrates the ANG cyberspace forces into USCYBERCOM's and DHS's cyber missions. The DHS's NCCIC "…serves as a centralized location for federal, state, local, tribal, and territorial governments to share and coordinate cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions." [42] ANG-CST personnel in a Title 32 status could support DHS's NCCIC in analyzing cyber threats and vulnerabilities and coordinate findings with other federal, state, and local departments and agencies. Additionally, ANG-CST personnel could assist in rapidly responding to cyber incidents and support recovery efforts.

The NTOC personnel collaborate with DHS and other military organizations such as the Defense Information Systems Agency (DISA) to provide situational awareness of an adversary's attempt to attack or exploit military networks. ANG-CST members could coordinate with military and intelligence agencies for all-source threat analysis. ANG-CST personnel could monitor classified systems to determine if threats and vulnerabilities are present in military networks and assist in developing mitigation strategies. They could also assist in facilitating security incident reporting to the appropriate authorities and disseminating threat advisories. Furthermore, ANG-CST personnel, in a Title 32 status, could support USCYBERCOM with cyber defense analytics, cyber forensics, cyber management team support, cyber indications and warnings, and participate in joint operational planning teams.[43]

Create a Memorandum of Agreement (MOA) with FBI

The FBI's NCIJTF is focal point for all government agencies to coordinate, integrate, and share information related to domestic cyber threat investigations.[44] While the FBI's NCIJTF

coordinates national-level cyber efforts, the FBI's Cyber Task Forces (FBI CTF) coordinates local-level cyber efforts. In particular, the FBI's CTF operates in 56 field offices and "synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions."[45]

The ANG-CST personnel, in a Title 32 status, could support the FBI's cyber law enforcement efforts in several ways. They could assist FBI CTF teams in reviewing all-source data and identifying intelligence gaps. They could assist in the development of a common operating picture of hostile cyber intrusion-related activity that aid cyber investigations. Furthermore, ANG-CST personnel could support the FBI CTF in identifying new methods and signatures of attack.

Provide Title 32 Support to the White House Cybersecurity Coordinator

The White House Cybersecurity Coordinator leads the interagency development of national cybersecurity strategy and policy.[46] ANG-CST personnel, in a Title 32 status, could assist the Cybersecurity Coordinator in reviewing national cybersecurity strategy and policy to ensure that National Guard cyberspace resources and capabilities are considered in future national cyberspace strategy and policy development. ANG-CST personnel assigned to this duty should have policy and plans expertise to identify how National Guard cyber resources could support other federal and state departments and agencies cyberspace strategy. This individual could also provide the NGB Office of the Legislation Liaison (NBG/LL) with proactive reporting of proposed national cybersecurity strategy and policy initiatives that may have implications for the National Guard.

Areas of Further Research

This paper focused on solutions for employing ANG cyber forces to conduct cyberspace operations. Further research is warranted on how the Army National Guard (ARNG) could be integrated into a National Guard Cybersecurity Program. This paper does not advocate growing the existing ANG cyber force. It does advocate growing emerging cyberspace missions and reducing legacy cyberspace missions. Consequently, manpower and mission impact analysis studies are warranted. The author is not a lawyer. Therefore, a legal opinion on the proposed solutions and recommendations warrants further research.

Conclusion

This paper offers viable solutions for clarifying the ANG's role in defending the nation against cyber-attacks. In particular, the paper recommends that the president and Congress enact Title 32 legislation that authorizes and funds the integration and employment of ANG members in a Title 32 state, versus federal, status to conduct cyberspace operations. The legislation establishes a legal basis that allows Title 32 status cyber forces to defend the nation's cyberspace infrastructure. It also recommends the creation of a National Guard Cybersecurity Program (NGCSP) as cyberspace domestic operations (DOMOPS) program. The NGCSP conceptual model illustrates one approach for institutionalizing and organizing ANG cyber forces to support cyberspace operations.

Additionally, the paper recommends the creation of two Air National Guard cybersecurity programs that strategically place Title 32 citizen-airmen cyber professionals within the Department of Homeland Security, National Security Agency, Federal Bureau of Investigation, United States Cyber Command, Office of the White House Cybersecurity Coordinator, and each state's Joint Forces Headquarters. By adopting this paper's

recommendations, the Chief of the National Guard Bureau and the Director of the Air National Guard will take a major step to ensuring that ANG cyber forces are ready, reliable, and relevant to defend the nation's critical infrastructures.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Deborah Charles, "U.S. homeland chief: cyber 9/11 could happen imminently" http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124 (accessed 24 January 2013); Secretary of Defense Panetta also warned of a cyber-attack against the United States. Secretary of Defense Leon Panetta, "A cyber attack perpetrated by nation states are [sic] violent extremists groups could be as destructive as the terrorist attack on 9/11." http://www.defense.gov/speeches/speech.aspx?speechid=1728 (accessed 24 January 2013).
2. National Guard Regulation, "National Guard Domestic Operations: Emergency Employment of Army and Other Resources," 13 June 2008, 8, http://www.ngbpdc.ngb.army.mil/pubs/10/ANGI10_8101.pdf (accessed 1 November 2012).
3. Department of Homeland Security, "Ensuring Security and Resilience in the Cyber Ecosystem," http://www.dhs.gov/secure-cyber-networks (accessed 13 December 2012).
4. United States Government Accountability Office, *Homeland Defense: Continued Actions Needed to Improve Management of Air Sovereignty Alert Operations*, January 2012, 1, http://www.gao.gov/products/GAO-12-311 (accessed 3 January 2013).
5. Ibid., 2.
6. National Security Strategy, May 2010, 27, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 4 November 2012).
7. National Guard Bureau Office of the Legislative Liaison, "*FY2013 National Defense Authorization Act: Analysis of H.R. 4310, The National Defense Authorization Act for Fiscal Year 2013,"* 12, http://www.ng.mil/ll/analysisdocs/FY2013/NGB-LL%20Analysis%20-%20FY13%20NDAA.pdf (accessed 25 January 2013).
8. Ibid., 13.
9. Ibid.
10. Department of Homeland Security, "Cyber Skills Task Force Report," Fall 2012, 24, https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf (accessed 13 January 2013).
11. Cheryl Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies" 8 November 2012,http://www.defense.gov/news/newsarticle.aspx?id=118479 (accessed 8 December 2012).
12. U.S. Air Force, *Air Force, Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025*, AF/ST TR 12-01, 15, 15 July 2012.
13. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 11. http://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (accessed 1 November 2012).
14. National Governors Association, "Governors O'Malley and Snyder to Lead NGA Resource Center on Cybersecurity," 2 October 2012, http://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html (accessed 30 December 2012).

15. Department of Defense, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, as amended through 31 January 2011, http://ra.defense.gov/documents/rtm/jp1_02.pdf (accessed 30 Oct 2012).

16. National Guard Regulation, "National Guard Domestic Operations: Emergency Employment of Army and Other Resources," 13 June 2008, 3, http://www.ngbpdc.ngb.army.mil/pubs/10/ANGI10_8101.pdf (accessed 1 November 2012).

17. Department of Defense, *Department of Defense Directive 5525.5: DoD Cooperation with Law Enforcement Officials*, (Washington, DC: Department of Defense, 20 December 1989), 14, http://www.fas.org/irp/doddir/dod/d5525_5.pdf (accessed 17 October 2012).

18. President of the United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 37-38, http://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (accessed 1 November 2012).

19. President of the United States, *National Security Strategy*, 27, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 2 November 2012).

20. Executive Office of the President, "*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*," May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 17 November 2012).

21. Department of Defense, "U.S. Cyber Command," Washington, DC, Department of Defense, http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 22 November 2012).

22. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, 8, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf (accessed 2 February 2013).

23. Secretary of Defense to Secretary of Homeland Security, Memorandum of Agreement, 13 October 2010. http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed 20 November 2012)

24. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, February 2010, vii, http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (accessed 17 December 2012).

25. Department of Homeland Security, *Blueprint for a Secure Cyber Future*, November 2011, 11. http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (accessed 8 December 2012).

26. Department of Homeland Security, *Homeland Security Advisory Council: CyberSkills Task Force Report*, Fall 2012, 2, https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf (accessed 22 November 2012).

27. U.S. Air Force, *Air Force, Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025*, 15, 15 July 2012.

28. U.S. Air Force, Air Force Doctrine Document 3-12, *Cyberspace Operations*, 15 July 2010, incorporating change 1, 30 November 2011), v, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf (accessed 15 November 2011).

29. COL David L. Collins," National Guard Cyber Force Presentation," National Guard Bureau, 8 November 2012.

30. Ibid.

31. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, 29, February 2010.

32. Title 32, US Code, sec. 902 (1956).

33. Washington National Guard, "Washington State Domestic Cyber Integrated Project". The Department of Homeland Security gave the State of Washington a $80,000.00 homeland security grant for domestic cyber planning.

40. Posse Comitatus Act, Title 18, USC, sec. 1385.

35. National Governors Association, "Governors O'Malley and Snyder to Lead NGA Resource Center on Cybersecurity," 2 October 2012, http://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html (accessed 30 December 2012).

36. Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Public Law 108–375, 108th Cong. (28 October 2004), sec. 416, http://www.dod.gov/dodgc/olc/docs/PL108-375.pdf

37. Ibid.

38. National Guard Bureau, *National Guard Domestic Operations: Emergency Employment of Army and Other Resources*, 13 June 2008, 7, http://www.ngbpdc.ngb.army.mil/pubs/10/ANGI10_8101.pdf (accessed 1 November 2012).

39. Air National Guard Instruction 10-203, *Air National Guard (ANG) Alert Resource Management*, 2, http://www.e-publishing.af.mil/shared/media/epubs/angi10-203.pdf (accessed 6 January 2013).

40. Lt Col Gent Welsh, LTC Thomas Muehleisen, and Major Tobey Ream, *Washington National Guard Concept of Operations for Domestic Cyberspace Response*, 12 July 2012, 5.

41. Ibid.

42. Department of Homeland Security, "About the National Cybersecurity and Communications Integration Center," http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (accessed 22 January 2013).

43. Lt Col Lee T. Furches, *Air National Guard Cyber Warfare Mission Options*, 18 July 2012. Cyber defense analytics, cyber forensics, cyber management team support, cyber indications and warnings, and participate in joint operational planning teams are listed in Lt Col Furches presentation as USCYBERCOM desired capabilities.

44. Federal Bureau of Investigation, *National Cyber Investigative Task Force*, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (accessed 6 January 2013).

45. Federal Bureau of Investigation, *Cyber Task Forces Building Alliances to Improve the Nation's Cybersecurity*, http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1 (accessed 29 March 2013).

46. White House, "White House Profile," http://www.whitehouse.gov/blog/author/Michael%20Daniel (accessed 12 January 2013).

Glossary

AD	Active Duty
ADOS	Active Duty for Operational Support
ADOT	Active Duty for Other Than Training
ADT	Active Duty for Training
AFTP	Additional Flying Training Period
AGR	Active Guard/Reserve
ANG	Air National Guard
AT	Annual Training
FST	Formal School Training
FTNGD	Full-time National Guard
FTNGD-OS	Full-time National Guard-Operation Support
IDT	Inactive Duty for Training
IADT	Initial Active Duty for Training
MPA	Military Personnel Appropriations
PT	Proficiency Training
STAT TOUR	Statutory Tour
TP	Training Period
TPPA	Training Period for Preparation of Assemblies
USC	United States Code
UTA	Unit Training Assembly

Bibliography

Air Force Doctrine Document (AFDD) 3-12,*Cyberspace Operations.* Maxwell AFB, AL: LeMay Center for Doctrine Development and Education. 15 July 2010, incorporating change 1, 30 November 2011. http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf (accessed 15 November 2012).

Air National Guard Instruction (ANGI) 10-203, *Air National Guard (ANG) Alert Resource Management.* Andrews AFB, MD: Air National Guard (Air National Guard Publication), 22 February 2012. http://www.e-publishing.af.mil/shared/media/epubs/angi10-203.pdf (accessed 6 January 2013).

Charles. Deborah. "U.S. homeland chief: cyber 9/11 could happen imminently." Reuters, 24 January 2013. http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124 (accessed 24 January 2013).

Collins, COL David L. Collins. "National Guard Cyber Force Presentation." Washington, DC: National Guard Bureau. 8 November 2012.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* Washington, DC: Department of Defense, July 2011. http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf (accessed 2 February 2013).

Department of Defense. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.* Washington, DC: Joint Chiefs of Staff, 8 November 2010, as amended through 31 January 2011. http://ra.defense.gov/documents/rtm/jp1_02.pdf (accessed 23 January 2013).

Department of Defense. "U.S. Cyber Command," Washington, DC: Department of Defense. http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 22 November 2012).

Department of Homeland Security. *About the National Cybersecurity and Communications Integration Center.* Washington, DC: Department of Homeland Security. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (accessed 22 January 2013).

Department of Homeland Security. *Blueprint for a Secure Cyber Future.* Washington, DC: Department of Homeland Security, November 2011. http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (accessed 8 December 2012).

Department of Homeland Security. *CyberSkills Task Force Report*. Washington, DC: Department of Homeland Security (Homeland Security Advisory Council), Fall 2012. https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf (accessed 13 January 2013).

Department of Homeland Security. *Ensuring Security and Resilience in the Cyber Ecosystem.* Washington, DC: Department of Homeland Security. http://www.dhs.gov/secure-cyber-networks (accessed 13 December 2012).

Department of Homeland Security. *Homeland Security Advisory Council: CyberSkills Task Force Report.* Washington, DC: Department of Homeland Security, Fall 2012. https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf (accessed 22 November 2012).

Department of Homeland Security. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland,* Washington, DC: Department of Homeland

Security, February 2010. http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (accessed 17 December 2012).
Executive Office of the President of the United States. *National Security Strategy.* Washington, DC: Executive Office of the President of the United States, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 2 November 2012).
Executive Office of the White House. *White House Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*."Washington, DC: Executive of the President of the United States, May 2009. http://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (accessed 1 November 2012).
Executive Office of the White House. "White House Profile." Washington, DC: Executive Office of the White House. http://www.whitehouse.gov/blog/author/Michael%20Daniel (accessed 12 January 2013).
Federal Bureau of Investigation. *National Cyber Investigative Task Force*, Washington, DC: Federal Bureau of Investigation. http://www.fbi.gov/about-us/investigate/cyber/ncijtf (accessed 6 January 2013).
Furches, Lt Col Lee T. "Air National Guard Cyber Warfare Mission Options." Paper presented to National Guard Bureau. Andrews Air Force Base, MD: Air National Guard, 18 July 2012.
National Guard Bureau. *National Guard Domestic Operations: Emergency Employment of Army and Other Resources*." Washington, DC: National Guard Bureau, 13 June 2008. http://www.ngbpdc.ngb.army.mil/pubs/10/ANGI10_8101.pdf (accessed 1 November 2012).
National Guard Bureau Office of the Legislative Liaison. *FY2013 National Defense Authorization Act: Analysis of H.R. 4310, The National Defense Authorization Act for Fiscal Year 2013.* Washington, DC: National Guard Bureau, January 2013. http://www.ng.mil/ll/analysisdocs/FY2013/NGB-LL%20Analysis%20-%20FY13%20NDAA.pdf (Accessed 25 January 2013).
National Governors Association. "Governors O'Malley and Snyder to Lead NGA Resource Center on Cybersecurity," 2 October 2012. NGA.com. http://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html (accessed 30 December 2012).
Obama, Barack, H. President of the United States. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, DC: President of the United States, May 2009. http://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (accessed 1 November 2012).
Panetta, Leon. Secretary of Defense. "A cyber attack perpetrated by nation states are violent extremists groups could be as destructive as the terrorist attack on 9/11." 11 October 2012. http://www.defense.gov/speeches/speech.aspx?speechid=1728 (accessed 24 January 2013).
Posse Comitatus Act. Title 18. USC. sec. 1385.
Ronald W. Reagan. National Defense Authorization Act for Fiscal Year 2005. Public Law 108–375. 108th Cong. (28 October 2004), sec. 416. http://www.dod.gov/dodgc/olc/docs/PL108-375.pdf.
Secretary of Defense. To Secretary of Homeland Defense. Memorandum of Agreement, 13 October 2010. http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed 20 November 2012)

Title 10. US Code. secs. 12301(d)-12304.
Title 32. US Code. sec. 902.
Washington National Guard. W*ashington State Domestic Cyber Integrated Project.* Camp Murray, WA: Washington National Guard, n.d.
Welsh, Lt Col Gent, LTC Thomas Muehleisen, and Major Tobey Ream. *Washington National Guard Concept of Operations for Domestic Cyberspace Response. C*amp Murray, WA: Washington National Guard, 12 July 2012.
US Air Force. *Air Force, Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025.* AF/ST TR 12-01. Washington, DC: US Air Force. 15 July 2012.
United States Government Accountability Office. *Homeland Defense: Continued Actions Needed to Improve Management of Air Sovereignty Alert Operations*. GAO-12-311. Washington, DC: Government Accountability Office, January 2012.