AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

MOVING LEFT OF BOOM: LEVERAGING TITLE 32 NATIONAL GUARDSMEN TO SHARE CYBER THREAT INTELLIGENCE WITH STATE AUTHORITIES

by

Kevin L. Archer, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor(s): Dr. Dennis Duffin

Maxwell Air Force Base, Alabama

June 2016

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 or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

ACKNOWLEDGEMENTS

I wish to convey my sincere gratitude to my wife and son. Though I am the one who made the commitment, you both have sacrificed just as much. It is your support that made this possible.

ABSTRACT

As the government looks for ways to prevent cyber attacks against critical infrastructure, information and intelligence sharing between federal and state governments becomes paramount. This research answers the question, "How can the National Guard (NG) legally aid in the prevention of cyber attacks by providing cyber threat intelligence to state governments?" The problem/solution framework is used to examine existing laws, regulations and authorities as well as various strategies and plans. The research concludes the lack of legal clarity and intelligence oversight concerns may deter intelligence sharing by the National Guard. It also concludes with the proper approval; the NG can be leveraged to share intelligence and help alleviate the high demand for skilled analysts. By drafting a single approval request from the National Guard Bureau to the Secretary of Defense, establishing "left and right" boundaries using a model similar to the NG Counterdrug Program, states could use Title 32 National Guardsmen to share cyber threat intelligence with state governments to attempt to mitigate cyber attacks on critical infrastructure.

Introduction

In December 2015, three regional power companies in Ukraine lost power impacting more than 225,000 people.[1] A subsequent investigation revealed the unscheduled power outage was caused by a synchronized and coordinated cyber attack, likely occurring after the attackers were on the company's networks for some time.[2]

This type of crippling cyber attack against critical infrastructure concerned the Council of Governors when they, along with the Department of Homeland Security (DHS) and the Department of Defense (DoD), crafted the Joint Action Plan for State-Federal Unity of Effort on Cybersecurity. While the Council of Governors recognized DHS has the lead role in the federal government for working with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems, they also expressly wanted to pursue the use of the National Guard's capabilities and authorities.[3] Figuring out how to use the existing cyber expertise in the National Guard may have been due to limited DHS cyber experts in the field. DHS Secretary Jeh Johnson testified before Congress in 2016 that DHS is not where it needs to be on hiring cyber talent because it cannot match private sector pay or the appeal of the intelligence agencies.[4]

The DoD, for its part, recognized effective cybersecurity will require close collaboration with state and local governments and it, "must further develop adequate warning intelligence of adversary intentions and capabilities for conducting destructive and disruptive cyberattacks [*sic*] against DoD and the United States."[5]

This research report culminates with an answer to the question, "How can the National Guard legally aid in the prevention of cyber attacks by providing cyber threat intelligence to state governments?" The primary problem is how to overcome intelligence "stovepipes", comply

with intelligence oversight laws, and share the intelligence with state governments to enable them better to protect their critical infrastructure and prevent catastrophic cyber attacks before they occur. The report focuses less on the intelligence itself. Instead, it examines existing laws, regulations and authorities as well as various strategies and plans.

The author makes the argument Title 32 National Guardsmen should be utilized to share cyber threat intelligence with state governments to attempt to mitigate cyber attacks on critical infrastructure. "From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States."[6] The DoD assumes a sophisticated state actor could target critical infrastructure either as a part of a conflict or to affect public safety.[7] The state perspective is cybersecurity is the weakest link in their efforts to protect critical infrastructure.[8] Pundits may argue that the DoD sharing intelligence with state authorities violates US laws and regulations. However, the National Guard operating under US Code Title 32 could be the conduit to facilitate this collaboration.

This report is written utilizing the problem/solution framework to provide a recommendation on how the National Guard should be leveraged to share cyber threat intelligence between federal and state governments. A solid foundation of information on authorities, executive orders, directives, and regulations provides an overall understanding of what is permissible. Also, the author examines current cyber strategies and plans to ascertain the current vision of the leadership pertinent to preventing cyber attacks. The author accomplishes the examination by highlighting applicable points from the DoD Cyber Strategy as well as the Council of Governors' Joint Action Plan. The aforementioned laws and regulations, juxtaposed with leadership vision, build a perceived barrier that makes sharing intelligence a daunting task. This research documents the author's recommendations to offer a viable "workaround" that complies with existing laws and regulations, and attempts to get "Left of Boom."

Background

To understand what the military's limitations are on sharing intelligence and collaborating with state and local authorities, this research will examine several terms, authorities, executive orders, DoD directives and regulations that in many cases prohibit this type of activities.

Left of Boom

The term "Left of Boom" was coined in the early 2000's by the US military and describes its efforts to combat improvised explosive devices in Iraq and Afghanistan.[9] However in this context "boom" refers to a cyber attack. To move "left of boom' in cyberspace means to "further develop adequate warning intelligence of adversary intentions and capabilities for conducting destructive and disruptive cyberattacks [*sic*] against DoD [Department of Defense] and the United States."[10] By moving "left" of the cyber attack (boom), the chance to change the conditions that facilitate the attack greatly increase, as does the probability of preventing the attack before it occurs.

Authorities

Title 10 US Code - Armed Forces is the legal basis for the armed forces in the United States Code and organized into sections for each service and an overall general provisions section. The general provisions section is further subdivided into Organization; Personnel; Training and Education; Service, Supply, and Procurement roles of the Army, Air Force, Navy, Marines and the Reserve Components.[11] The federalization of the National Guard into a Title 10 status occurs for purposes of augmenting an active-duty component. National Guard federalization can occur voluntarily or involuntarily when ordered by the President of the United States or in certain cases the Secretary of Defense.[12] The federalized National Guard is subject to the same laws and regulations as active-duty forces and is under the control of the President.

Title 18 US Code § 1385 - Use of Army and Air Force as posse comitatus, otherwise known as the Posse Comitatus Act (PCA) was originally enacted in 1878 to prohibit federal forces from performing police actions in the southern states after the civil war.[13] Today, after changes in the law and subsequent DoD Directives, "the PCA generally prohibits US military personnel from direct participation in law enforcement activities. Some of those law enforcement activities would include interdicting vehicles, vessels, and aircraft; conducting surveillance, searches, pursuit, and seizures; or making arrests on behalf of civilian law enforcement authorities. Prohibiting direct military involvement in law enforcement is in keeping with long-standing US law and policy limiting the military's role in domestic affairs."[14] While active-duty Title 10 forces (including federalized National Guard forces) are prohibited from direct involvement in law enforcement activities, key exceptions to the PCA include the Coast Guard and the non-federalized National Guard in Title 32 or State Active Duty (SAD).

Title 32 US Code - National Guard, along with the US Constitution, provides the legal basis for the National Guard and its roles and responsibilities. Like Title 10, Title 32 is divided into similar sections: Organization; Personnel; Training; Service, Supply and Procurement; and Homeland Defense Activities.[15] When not in a Title 10 status, the primary role of the National Guard is to train for the purpose of augmenting Title 10 forces (as required). Thus, the National Guard in this role is considered to be in a "training" status or a Title 32 status.

Within Title 32, members are considered to be either drill status or "full-time" guardsmen. Drill status guardsmen (DSG) train for their federal Title 10 mission, one weekend per month in training periods called Regularly Scheduled Drills (RSD) and 15 days per year, called Annual Training (AT).[16] There are several permissible situations to accomplish additional training throughout the year, but these are the minimum requirements for an annual period.

There are two types of "full-time" guardsmen. The first is an Active Guard & Reserve (AGR); these members "are on voluntary active duty providing full-time support to National Guard, Reserve, and Active Component organizations for the purpose of organizing, administering, recruiting, instructing, or training the Reserve Components."[17] AGRs can be either in a Title 32 or a Title 10 status.

The second type of "full-time" guardsmen is a Title 32 military technician (also referred to as dual-status technicians). A military technician is a federal civilian employee through the week, however during RSDs or AT military technicians convert to military members the same as drill status guardsmen. Similar to an AGR, the role of a military technician is to organize, administer, instruct, or train the National Guard, as well as perform the maintenance and repair of supplies issued to the National Guard or the armed forces.[18] Unlike most federal civilian employees, though, to be employed as a military technician they must also meet additional requirements. Military technicians must: be a member of the National Guard, hold the military grade specified by the Secretary concerned for that position, and while performing duties as a military technician, wear the appropriate uniform and rank.[19]

Title 32 drill status and "full-time" Guardsmen are under state control and commanded by the governor, but are federally funded for the purpose of training for their federal Title 10 mission. Making matters even more complicated, military technicians and drill status guardsmen, while both federally funded, are paid from separate appropriations. This is an important point because using appropriated federal funds for a purpose other than what was intended could result in a financial law purpose violation.[20]

State Active-Duty (SAD) is when the governor activates the National Guard for a state authorizing the National Guard to support civil authorities during a natural disaster. For instance, Ohio Revised Code allows the governor to order the organized militia (State National

Guard Units) to aid civil authorities to: execute state laws, suppress insurrection, act in the event of a natural disaster, and promote the health, safety, and welfare of the citizens of the state.[21] It is important to note that guardsmen in a SAD status are paid by the State and operate under State laws. Thus, they are not considered to be functioning in a DoD capacity.[22] Regarding pay and allowances, many states match basic pay with the same rank and grade as federal armed forces, but SAD pay and allowances can vary depending on state law.[23] Finally, when performing in a SAD status, guardsmen do not earn points towards their federal retirement.

Executive Orders, Regulations, and Directives

Executive Order (EO) 12333, United States Intelligence Activities was issued by President Ronald Reagan, on 4 December 1981. It defined the members of the Intelligence Community to include the intelligence and counterintelligence elements of the Army and the Air Force. It established the guidelines for foreign and domestic intelligence activities. Intelligence activities, as defined by EO 12333, are "all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order."[24] EO 12333 specified that the Intelligence Community can "collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents."[25] It also prohibits physical surveillance of a United States person in the United States by elements of the Intelligence Community unless there is prior approval of the Attorney General after consultation with the Director of National Intelligence.[26]

Executive Order 13636, Improving Critical Infrastructure Cybersecurity was issued by President Barack Obama on February 12, 2013. It states "the cyber threat to critical

infrastructure continues to grow and represents one of the most serious national security challenges."[27] EO 13636 asserts in order to protect critical infrastructure, cyber threat information should be shared with US private sector. It also called for the establishment of an expanded Enhanced Cybersecurity Services (ECS) program for the critical infrastructure sector. This program currently conducted by DHS offers three types of ECS. The three types include domain name service sinkholing (blocks access to malicious domain names), email filtering (blocks malicious email based on certain criteria), and netflow analysis (uses passive detection to identify threats).[28] While EO 13636 mentions sharing unclassified as well as classified information, it caveats the procedures for sharing the information must "protect intelligence and law enforcement sources, methods, operations, and investigations."[29] Finally, EO 13636 specifically points out privacy and civil liberties protection concerns. It states any activity under this order must incorporate privacy and civil liberties protections and "shall be implemented consistent with applicable law and subject to the availability of appropriations."[30]

Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience was issued in conjunction with EO 12636 on 12 February 2013 by President Barack Obama. Much like EO 12636, PPD 21 focuses on strengthening the security of critical infrastructure. The main differences between the two documents are that PPD 21 replaced Homeland Security Presidential Directive-7 and stated the security and resilience of critical infrastructure is a "shared responsibility among the federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure."[31] The policy further states the federal government will work with SLTT entities to proactively takes steps manage risk and seek to "reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure."[32]

PPD 21 directed Federal roles and responsibilities to partner with critical infrastructure owners and operators as well as SLTT entities. PPD 21 assigned DHS the responsibility of coordinating the overall federal effort of protecting the nation's critical infrastructure. Among other responsibilities, DHS is tasked to evaluate national capabilities, opportunities, and challenges as well as analyze threats and vulnerabilities of critical infrastructure.[33] The Department of Justice (DOJ), namely the Federal Bureau of Investigation (FBI), was assigned the responsibility of leading counterterrorism and counterintelligence investigations and related law enforcement activities. "DOJ shall investigate, disrupt, prosecute, and otherwise reduce foreign intelligence, terrorist, and other threats to, and actual or attempted attacks on, or sabotage of, the Nation's critical infrastructure."[34] The FBI is also tasked with leading the National Cyber Investigative Joint Task Force (NCIJTF). NCIJTF serves as a focal point for "coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community (IC), DoD and other agencies as appropriate."[35] The IC was tasked to provide and coordinate on intelligence assessments regarding threats to critical infrastructure in accordance with applicable laws.

PPD 21 outlined three strategic imperatives:

1. Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience;

2. Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government;

3. Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure.[36]

The first imperative called for the creation of two national critical infrastructure centers under the direction of DHS. The National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) were a result of PPD

21 and focused on the physical and cyber defense aspects (respectively) of critical infrastructure.[37] Although the third imperative called for an integration and analysis function, it was not to replicate the function of the IC or involve intelligence collection activities. Finally, PPD 21 designated the 16 sectors associated with critical infrastructure.[38]

DoD 5240.1-R, Activities of DOD Intelligence Components that Affect United States Persons was signed by Attorney General William Smith, and Secretary of Defense Caspar Weinberger in 1982. It implemented EO 12333 and is still applicable to all DoD intelligence components today. DoD 5240.1-R consists of 15 procedures for the purpose of enabling DoD intelligence components to carry out authorized functions while concurrently protecting the constitutional rights and privacy of US persons. Procedure 1 defines applicability and scope and is labeled "General Provisions". Procedures 2 through 4 provide the authority for DoD intelligence components to collect, retain, and disseminate information concerning US persons.[39] Procedures 5 through 10 refer to techniques used to collect information for foreign intelligence and counterintelligence.[40] Procedures 11 through 15 refer to "other aspects of DoD intelligence activities, including the oversight of such activities."[41] Procedures 1 through 10 require the approval of the Attorney General and procedures 11 through 15 provide further guidance to DoD intelligence components in implementing EO 12333.[42]

Many of these Procedures are outside the scope of this research. However, the examination of Procedures 2, 3, 4, and 12 provide the greatest insight into the rules governing DoD intelligence component cooperation with law enforcement agencies.

Procedure 2 refers to collecting information about US persons. Procedure 2 states information is "collected only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties."[43] The allowed types of collected information about a US person include information obtained with consent, publicly available

information, and foreign intelligence. It is important to note that these types of information about a US person may only be collected by a DoD intelligence component "if it is necessary to the conduct of a function assigned the collecting component."[44]

Procedure 3 governs the retention of US persons information. Information about a US person may be retained if it was collected lawfully according to rules outlined in Procedure 2. "Information about United States persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained under these procedures."[45]

Procedure 4 "governs the kinds of information about United States persons that may be disseminated, without their consent, outside the DoD intelligence component that collected and retained the information."[46] Disseminating information collected and retained under Procedures 2 and 3 is only permissible if the recipient has a reasonable need to receive the information.[47] Also, the recipient must have a need for the information in the course of performing official duties.[48]

Procedure 12 outlines the provisions for DoD intelligence components to assist law enforcement authorities. It incorporates limitations specified in EO 12333 and other limitations as prescribed in DoD Directive 5525.5. In 2013, DoD Directive 5525.5 was canceled and incorporated into DoD Instruction 3025.21, *Defense Support to Civilian Law Enforcement Agencies*.[49] Procedure 12 states cooperation between DoD intelligence components and law enforcement authorities is authorized for the following purposes:

1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;
2. Protecting DoD employees, information, property, and facilities;
3. Preventing, detecting or investigating other violations of law.[50]

The cooperation is contingent upon approval of an authorized official, provided the "General Counsel of the providing DoD component concurs in such use."[51]

DoDD 5105.77, National Guard Bureau (NGB) was reissued by Secretary of Defense Ash Carter on 30 October 2015. The directive updates the previous directive published on 31 May 2008. It specifically updates the "the organization and management, responsibilities and functions, relationships, authorities, and administration of the Chief, NGB, and the NGB,"[52] as prescribed by section 10503 of Title 10 U.S. Code. DoDD 5105.77 also restates sections 10501 and 10502 of Title 10 U.S. Code, that NGB is a joint activity of DoD and that the Chief, NGB (CNGB), is responsible for the organization and operations of NGB.[53]

DoDD 5105.77 states the NGB consists of the Office of CNGB; the National Guard Joint Staff; the Office of the Director, Army National Guard, and the Office of the Director, Air National Guard.[54] It authorizes the Directors of the Army National Guard and the Air National Guard to directly coordinate with the Army Staff and the Air Staff respectively.[55] The directive stipulates NGB is the main communication channel between the Departments of the Army and the Air Force and the states on matters that pertain to the non-federalized National Guard. NGB is also the main communication channel between the states and the Secretary of Defense, the CJCS and DoD Components on matters that pertain to the National Guard.[56] It lists twelve separate responsibilities of CNGB. Among those responsibilities are that the Chief, NGB, "is a principal advisor to the Secretary of Defense, through the CJCS, on matters involving non-federalized National Guard forces, and on other matters as determined by the Secretary of Defense."[57] In addition, CNGB, as a member of the Joint Chiefs of Staff (JCS), "has the specific responsibility of addressing matters involving non-federalized National Guard forces in support of homeland defense and civil support missions."[58]

Lastly, Enclosure 2 of DoDD 5105.77 delegates "authority to exercise, within assigned responsibilities and functional areas, all authority of the Secretary of Defense derived from statute, E.O., regulation, and interagency agreement, except where specifically limited by statute, E.O., or the Secretary of the Army, or the Secretary of the Air Force."[59] Enclosure 2 lists several specific authorities delegated to CNGB for the administration and operation of the National Guard Bureau. One of the listed authorities allows CNGB to establish and maintain regulations, instructions, and reference documents for the functions assigned to NGB.[60]

DoDI 3025.21 Defense Support of Civilian Law Enforcement Agencies was published and signed by Under Secretary of Defense for Policy, James N. Miller on 27 February 2013. It incorporates and replaces DoD Directive 5525.5 (referenced in DoD 5240.1-R). This Instruction sets policy regarding the use of DoD to support federal, state, tribal and local civilian law enforcement agencies.[61] While this directive focuses mainly on the Title 10 armed forces (DoDI 3025.21 specifically states it is not applicable to the National Guard in a Title 32 or SAD status[62]), it does assign responsibilities for the "use of Reserve Component personnel in support of civilian law enforcement agencies, in coordination with the Secretaries of the Military Departments and the Assistant Secretary of Defense for Reserve Affairs (ASD(RA)), and with the Chief, National Guard Bureau (NGB), as appropriate. This will include guidance for use by approving authorities in evaluating the effect on military preparedness of requests for civilian law enforcement assistance that may involve the use of the Reserve Components."[63]

DoDI 3025.21 establishes a policy that DoD "shall be prepared" to support civilian law enforcement consistent with military preparedness, as long as it does not violate legal limitations stipulated by the PCA. In fact, Enclosure 3 elaborates on permissible types of direct assistance, restrictions on direct assistance, exceptions to policy, and a paragraph explicitly stating assistance may not be provided if it adversely affects military readiness.[64] Enclosure 3 also

contains the paragraph on the approval authority, previously found in Enclosure 4 of DoD Directive 5525.5 referenced by DoD 5240.1-R. Paragraph 5b (Approval Authority) of Enclosure 3 states, "Requests that involve Defense Intelligence and Counterintelligence entities are subject to approval by the Secretary of Defense."[65] Again, it is important to point out that DoDI 3025.21 states it is not applicable to NG in a Title 32 or SAD status.

CNGBI 2000.01A, National Guard Intelligence Activities was published and signed by Chief of the National Guard Bureau, General Frank J. Grass on 24 July 2015. CNGB was delegated authority to establish and maintain instructions by the Secretary of Defense in DoDD 5105.77. CNGBI 2000.01A in effect closes the loop left open by DoDI 3025.21. It establishes a policy that "NG intelligence personnel operating in a Title 32 status operate as members of the Department of Defense intelligence component and must comply with all DoD guidance and Federal laws applicable to the component, to include Intelligence Oversight rules."[66]

The instruction further clarifies National Guard intelligence personnel operating in a SAD status are not members of a DoD Intelligence component, thus they cannot engage in DoD intelligence activities or use DoD intelligence equipment without the authorization of the Secretary of Defense or his or her designee.[67] CNGBI 2000.01A, lists responsibilities for all NG intelligence personnel; from the Director of National Guard Joint Staff Directorate of Intelligence's oversight, down to the individual intelligence analyst's responsibility to understand the mission and to accomplish intelligence oversight training.

CNGBI 3100.01A National Guard Counterdrug Support was published and signed by Chief of the National Guard Bureau, General Frank J. Grass on 22 June 2015. It outlines responsibilities under the Title 32 State Counterdrug (CD) Program. Every year, states are required to submit an annual CD support plan. The Secretary of Defense must approve the plan, but only after "certification by the Governor of the State or a civilian law enforcement official of

the State designated by the Governor has determined that any activities included in the plan are carried out in conjunction with Federal LEAs [Law Enforcement Agencies], and ensure State laws are enforced."[68] Furthermore, the state's attorney general must also certify state law does not prohibit missions outlined in the annual plans. CNGBI 3100.01A specifies when funds that are explicitly appropriated by Congress under Title 32 US Code Section 112, "States may only execute missions within their annual State Drug Interdictions and Counterdrug Activities Plan (State CD Support Plan) that have been approved by the Secretary of Defense."[69] Lastly, CNGBI 3100.01A states NG CD Program operational files and training materials (to include intelligence oversight and information collection) are subject to inspection by the NG Inspector General.[70]

Information vs. Intelligence

The terms information and intelligence are often used interchangeably, but these terms have two very distinct meanings. The meaning and context in which these terms when used in policy or regulation have potential legal implications.

Joint Publication (JP) 1-02 is the DoD Dictionary of Military and Associated Terms. It constitutes the "approved" DoD terminology to be used by all DoD components. JP 1-02 defines intelligence as:

1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.

2. The activities that result in the product.

3. The organizations engaged in such activities.[71]

The FBI defines intelligence as, "information that has been analyzed and refined so that it is useful to policymakers in making decisions - specifically, decisions about potential threats to national security."[72]

The term "information" is not defined in JP 1-02. It is frequently used as part of several terms in JP 1-02, such as information environment, information security, information assurance, and information operations.[73] "Information" appears 633 times in JP 1-02 either as part of a term or more predominately as part of a definition to another term.[74]

The Merriam-Webster Dictionary has four separate definitions of the word information. The first definition is the "communication or reception of knowledge or intelligence."[75] The next definition deals with communicated signals, data, or a message and the third definition is the act of informing against a person.[76] Finally, the last definition, according to Merriam-Webster, comes from a legal perspective and means "a formal accusation of a crime made by a prosecuting officer as distinguished from an indictment presented by a grand jury."[77]

The phrase "information sharing" became more prominent after the 9/11 Commission Report. One of the commission's recommendations specifically addressed *Unity of Effort in Sharing Information.*[78] The commission referred to information sharing in the context of sharing between members of the Intelligence Community. The commission stressed the importance of intelligence that could draw on all relevant sources of information (classified or unclassified).[79]

Fusion Centers

Fusion Centers grew out of a gap identified in the 9/11 Commission Report.[80] "Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners."[81] There are more than 70 fusion centers owned and operated by state and local government agencies. Their main role is to "conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism."[82]

Post 9/11, fusion centers did not have common information sharing standards, which created challenges. To solve this issue, the Department of Justice along with DHS and numerous local law enforcement partners created *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*.[83] Fusion centers collaborate with the DHS, DOJ, FBI, Office of the Director of National Intelligence (ODNI), Program Manager for the Information Sharing Environment (ISE), Office of National Drug Control Policy, and DoD.[84]

Fusion centers were not initially envisioned to have a cyber capability. A subsequent appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers* discussed cyber integration into fusion centers. However, it did not identify additional requirements for fusion centers, instead it stated fusion centers choosing to integrate a cyber capability, identify how they could "effectively integrate the information, resources, personnel, and expertise of cyber partners, cyber stakeholders, and the cyber community, to enhance fusion center information/intelligence sharing processes."[85] The appendix defined cyber partners as "any personnel or entities with whom the fusion center has a Memorandum of Understanding (MOU), a Memorandum of Agreement (MOA), a Nondisclosure Agreement (NDA), or a similar contract."[86] It also defined cyber stakeholders as "any personnel or entities with whom the fusion center has an established, ongoing, and close relationship that involves the exchange of information and intelligence."[87]

Converging Strategies

DoD Cyber Strategy

In April 2015, Secretary of Defense Ash Carter released the DoD Cyber Strategy. In his opening statement, Secretary Carter stated the purpose of the cyber strategy was to "guide the

development of DoD's cyber forces and strengthen its cyber defense and cyber deterrence posture."[88] He outlined the DoD's three cyber missions, "defend DoD networks, systems, and information; defend the United States and its interests against cyberattacks [*sic*] of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans."[89]

The cyber strategy called for five strategic goals:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations.
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.
3. Be prepared to defend the US homeland and the US vital interests from disruptive or destructive cyber attacks of significant consequence.
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.[90]

The third strategic goal specifically calls for DoD to work with interagency partners, and the private sector, to deter a significant cyber attack.[91] It also states "The Defense Department must develop its intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyberattacks [*sic*] before they can impact U.S. interests."[92]

Two of the key implementation objectives of the second strategic goal were to develop a framework and to exercise DoD's Defense Support to Civil Authorities (DSCA) as an integrated plan with DHS and other state and local authorities.[93] The objective included working with DHS, FBI, and other agencies to improve integration, training, and support.[94] The second key implementation objective was for National Guard forces to "exercise to coordinate, train, advise, and assist state and local agencies and domestic critical infrastructure and to provide support to law enforcement, Homeland Defense, and Defense Support of Civil Authorities activities in

support of national objectives."[95] The objective was limited by the existing and planned NG force structure.

Council of Governors, Joint Action Plan

The Joint Action Plan is a framework adopted in July 2014, by the states, the DHS, and DoD, to work together to improve overall cybersecurity. It provides for cybersecurity principles, implementation guidance, authorities, roles, and responsibilities. It explicitly states the "plan does not alter Federal and State law or existing legal authority. All expressed and implied powers of the President, the Governors, and the heads of Federal departments and agencies remain in full force and effect."[96]

As part of the implementation of the Joint Action Plan, the DoD and the Council of Governors agreed to continue to improve and clarify how views and information would be discussed in advance of proposals to change "state or federal laws, regulations, or policies, when such proposals would affect the roles and responsibilities of the National Guard in cyberspace in support of civil authorities."[97] In addition, the "DoD, following the exchange of views, information, or advice with the Council of Governors, will update or, as necessary, establish DoD policy regarding State use of DoD cyber-related resources assigned to the National Guard."[98]

Finally, regarding information sharing, the parties of the Joint Action Plan concurred that obtaining accurate situational awareness of cyber threats before they happen is critical. To that end, they agreed to "review and look for ways to increase the volume, timeliness, and quality of cyber threat information between DHS and SLTT government partners, leveraging efforts developed in response to EO 13636 and PPD-21."[99]

Analysis of Other Models

National Guard Counterdrug Program

The National Guard provides intelligence analysis in support of law enforcement, under the NG Counterdrug Program. This program was enacted by legislation as part of the 1989 National Defense Authorization Act (NDAA). The act authorized "the Secretary [of Defense] to provide to the Governor of a State funds sufficient to pay for all expenses of the National Guard of such State when engaged in drug interdiction assistance activities, provided that the Governor submits to the Secretary a plan specifying how such National Guard personnel are to be used."[100] It further directed the Secretary of Defense to consult with the state attorney general to verify its adequacy.[101]

Each fiscal year, Congress appropriates funds for the NG Counterdrug Program. After meeting all the requisite requirements, the individual state units receive the funds.[102] The primary use of this funding is paying for individuals placed on Title 32 Full-Time National Guard (FTNG) orders. Title 32 FTNG is similar to Title 32 AGR orders, except that funding for the orders are only through the current fiscal year (FY). In FY 2015, state plans' totaled approximately $146 million.[103]

An Alternate Approach to Cyber Support

In his 2013 paper, *A National Solution: Rethinking the Employment of Air National Guard Title 32 Status Citizen-Airman to Defend the Nation's Cyberspace Infrastructure,* Lt Col Maurice McKinney advocated for legislation and funding (similar to the NG Counterdrug Program) to employ Air National Guard members on orders in a Title 32 FTNG status.[104] He recommended the creation of an Air National Guard (ANG) Cybersecurity Team (CST) as well as an ANG Cyber Sovereignty Alert Program.[105]

Lt Col McKinney did not define the make-up of the ANG-CST, but did hint at it when he mentioned that ANG-CST *cyberspace operators* 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."[106] These are typically places where intelligence and information sharing take place.

Conclusions

1. Intelligence Activities Are Subject to Intelligence Oversight

EO 12333, DoD 5240.1-R, and CNGBI 2000.01A all state that intelligence activities are subject to intelligence oversight. CNGBI 2000.01A defines intelligence activities as "all activities that Department of Defense Intelligence Components are authorized to undertake pursuant to EO 12333 and includes activities conducted by 'non-intelligence' organizations."[107] It also explicitly points out "NG intelligence organizations, units, and staff organizations, and non-intelligence organizations that perform intelligence or intelligence-related activities, such as Eagle Vision and cyberspace activities, will establish [Intelligence Oversight] IO programs"[108] in accordance with DoD 5240.1-R.

2. Lack of Legal Clarity May Deter Intelligence Sharing

Regarding the use of cyber intelligence analysts in a state collaboration role, it is clear there are legal and regulatory limitations as well as intelligence oversight concerns that many in the National Guard either are not aware of or have intentionally avoided preventing oversight violations. The term "information" seems to be used interchangeably with "intelligence". The perspective from the Intelligence Community supports the conclusion that information is defined as raw, unprocessed data. Intelligence is information given context produced by analysis and

refinement. When the term "information sharing" appears in strategy, it is unclear whether the use is under the pretense it will not invoke any intelligence oversight scrutiny or meant to permit only the sharing of unrefined data.

3. The National Guard, with Approval, can be Utilized to Share Intelligence

One of the primary reasons that the National Guard is a good choice to help bridge the intelligence gap between the federal and state government is it gives the DoD a legal way to support the states. The Posse Comitatus Act prevents active-duty components from providing this type of support in state fusion centers. The National Guard, drawing its training authorities from Title 10 and funded by the federal government, is considered a state resource under the control of the governor while in a Title 32 status.

The National Guard intelligence analysts can support federal, state, and local law enforcement in a SAD status. National Guard intelligence analysts can also perform intelligence analysis in a Title 32 status. Analysis can be accomplished as training incidental to operations as long as it coincides with the units' Title 10 mission-essential task list and focuses on foreign intelligence. However, supporting federal, state, and local law enforcement in a Title 32 status, is not a quick or simple process, with each instance requiring the state's Adjutant General to submit a request to the Secretary of Defense (under Procedure 12 of DoD 5240.1-R) for approval through the CNGB.

4. Leveraging National Guard Skillsets can Solve Demand Challenges

DHS has a clear mandate from Presidential Policy Directives and Executive Orders to be the federal focal point for cyber information sharing between the federal government and states, territories, and the private sector. However, by Secretary Johnson's recent testimony before

Congress, it is evident that DHS does not have the required manpower with the appropriate skillset in many of the states.

The National Guard can help alleviate the skilled manpower shortage. In analyzing the 2015 DoD Cyber Strategy together with the Council of Governors' Joint Action Plan there appears to be a tacit desire to leverage the National Guard's skillset, authorities, and personal relationships in the community to safeguard critical infrastructure by looking for and sharing indications and warnings to prevent cyber attacks.

It is unclear whether Congress will enact legislation similar to the National Guard Counterdrug Program that will address the limitations and streamline the process to use the National Guard in this role. What is clear is this analysis shows NG cyber intelligence analysts in a Title 32 status, given clear "left and right bounds" with the appropriate approvals, proper oversight, and following all applicable laws and regulations, can share intelligence with state authorities without enacted legislation. However, a lack of a clear, streamlined approval process to permit the National Guard to share cyber threat intelligence with state governments remains an impediment to doing so.

Recommendations

The following recommendations do not address the answers from a tactical or operational standpoint. Those recommendations are outside the scope and prevue to answer in this research. Instead, these recommendations focus on the process and authorities that would be required so that states can leverage their ANG, and Army National Guard (ARNG) cyber intelligence analysts' capabilities to collaborate with state authorities to prevent cyber attacks on critical infrastructure.

1. Draft a Single Approval Request

NGB should draft a single request (under Procedure 12 of DoD 5240.1-R) that applies to all 54 states and territories and allows them to use both ANG and ARNG cyber intelligence analysts. Normally for states to be able to use NG cyber intelligence analysts in a Title 32 training status and share cyber threat intelligence with state fusion centers, each state would have to request approval from the Secretary of Defense. This approval is required by EO 12333, DoD 5240.1-R, and CNGBI 2000.01A. The request is a time-consuming process that requires staffing a package through both the NGB and the Office of the Secretary of Defense. Instead, NGB should submit a single action memorandum (with concurrence from the CNGB) requesting the required approval from the Secretary of Defense on behalf of all 54 states and territories. The action memorandum from the CNGB to the Secretary of Defense is appropriate. The CNGB's role is "a principal advisor to the Secretary of Defense, through the CJCS, on matters involving non-federalized National Guard forces, and on other matters as determined by the Secretary of Defense."[109]

Using the National Guard to share cyber intelligence with states and territories satisfies a few of the strategic goals discussed in the 2015 DoD Cyber Strategy. It would use the National Guard to "foster creative solutions to cybersecurity problems," help establish a partnership between state and local governments and the DoD, and it would further the development of adequate warning intelligence to disrupt cyber attacks. The action memorandum should mirror the intent stated in the Council of Governors Joint Action Plan to use state resources, including the "cyber-related resources assigned to the National Guard." Similar to the Joint Action Plan, the single action memorandum should clearly state it does not alter any existing laws, policies, or regulations. It only grants limited approval based on conditions defined in a Concept of Operations (CONOPs) and would be for a limited timeframe, to be re-evaluated periodically.

The periodic evaluations could take into account DHS' capability to fill skilled positions in the states as well as the willingness of the states, and the DoD to leverage NG cyber intelligence analysts in this manner.

2. Establish "Left and Right" Boundaries

NGB should draft a NG Cyber Intelligence Support CONOPs to be included with the action memorandum. The CONOPs should limit the support to analyzing foreign intelligence for the purpose of protecting critical infrastructure. Much of the concern surrounding intelligence personnel in state fusion centers has to do with the fear of the government "spying" on US persons.[110] By focusing the analysis on foreign intelligence, it establishes a clear guideline for intelligence analysts to follow and analyzing foreign intelligence, as outlined in EO 12333, and DoD 5240.1-R is permissible. Stating the purpose of the foreign intelligence analysis is to protect critical infrastructure fills a need identified by all levels of government. Protecting critical infrastructure is the primary reason for EO 12636 and PPD-21. These orders and directives call for partnerships between the federal and state entities. Narrowly scoping the cyber intelligence support will help set the "left and right bounds" and avoid potential intelligence oversight concerns outlined in EO 12333, DOD 5240.1-R, and CNGBI 2000.01A. To be clear, sharing cyber threat intelligence with personnel at state fusion centers would still require a "need to know" and only then sharing intelligence based on the level of security clearances of involved personnel. Support should be given on a part-time basis so that there is no interference with normal training and to limit exposure from a financial purpose violation.

3. Create a Model Similar to the National Guard Counterdrug Program

Model the CONOP similar to the National Guard CD Program but *without* the legislation that was passed to enable the CD Program. Under this recommendation, there is no requirement

for legislation, as the Secretary of Defense has the authority to approve intelligence support to law enforcement. Unlike the National Guard CD Program or the other approaches to National Guard cyber support, this recommendation would not require further funding keeping it resource neutral because the federal government already funds National Guard cyber intelligence analysts in a Title 32 status.

The CONOP should include an annual plan in the form of a memorandum of agreement (MOA) between the Adjutant General, and the state fusion centers. The process is similar to the National Guard CD Program annual plan submitted by the governor, verified by NGB and approved by the Secretary of Defense. The MOA would state the applicability, certify the legality, and list the specific support within the limits established by the CONOPs. Just as directorates within NGB verify the National Guard CD Program annual plan, the MOA would be subject to review by the NGB Director of Intelligence, the Judge Advocate, and the Inspector General to ensure the state's agreement is consistent with the approved CONOP and not in violation of any federal laws or regulations before approval.

Finally, the CONOP would also require that the State Joint Force Headquarters (JFHQ) maintain a list of all individuals participating in cyber intelligence support to the state fusion centers. These individuals should receive tailored intelligence oversight training annually to include relevant state laws and regulations. The State-JFHQ and the listed individuals would be subject to intelligence oversight inspections by NGB that would coincide with regularly scheduled intelligence oversight inspections performed by the NGB IG or the NGB Intelligence Directorate.

Summary

"The imperative to secure and protect the American public is a partnership shared at all levels including federal, state, local, tribal, and territorial. Partnerships

and collaboration must occur within and among intelligence, defense, diplomatic, homeland security, law enforcement, and private sector communities."

- National Strategy for Information Sharing and Safeguarding, 2012

Twenty years ago cyber attacks on critical infrastructure and key resources were considered science fiction. Today, as witnessed by cyber attacks perpetrated in Ukraine, cyber attacks against critical infrastructure and key resources are a very real threat. This type of attack could have devastating effects on individual states or the United States as a whole.

There appears to be a desire from the federal and state governments to prevent this type of cyber attack from happening, but so far the focus has been on response and resiliency. This research consolidated the current information on authorities, executive orders, directives, and regulations and answered the question, "How can the National Guard legally aid in the prevention of cyber-attacks by providing cyber threat intelligence to state governments?" The National Guard, in a Title 32 status, can play an integral role in preventing these attacks by sharing intelligence with state fusion centers. While prerequisites and approvals must be accomplished, the recommendations represent a way forward and an attempt to satisfy goals stated by federal and state governments. The National Guard is uniquely positioned to prevent cyber attacks by sharing intelligence and thereby "Move Left of Boom."

Notes

1. Department of Homeland Security, *Alert IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure*, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (accessed 1 June 2016).
2. Ibid.
3. "Council of Governors Joint Action Plan for State-Federal Unity of Effort on Cyber Security", 2014, 1, http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf (accessed 28 February 2016).

4. "Homeland Security Secretary Jeh Johnson Testimony on Fiscal Year 2017 Budget", C-SPAN.org, 8 March 2016, video, 1:36:54, http://www.c-span.org/video/?406187-1/homeland-security-secretary-jeh-johnson-testimony-fiscal-year-2017-budget.

5. Department of Defense, *Cyber Strategy*, (Washington, DC: Secretary of Defense, April 2015), 7.

6. Ibid., 9.

7. Ibid., 2.

8. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, 11, http://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (accessed 28 February 2016).

9. Rick Atkinson, "About Left of Boom: The Fight Against Roadside Bombs", *The Washington Post*, 30 September 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/09/28/AR2007092801888.html.

10. Department of Defense, *Cyber Strategy*, 7.

11. *Armed Forces, U.S. Code 10* (1956).

12. *Armed Forces, U.S. Code 10* (1956). *§§* 12301

13. Eric V. Larson and John E. Peters, *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options*, RAND Report MR-1215-A, 2001, 243.

14. U.S. Northern Command Factsheet, *The Posse Comitatus Act*, 16 May 2013.

15. *National Guard, U.S. Code 32 (1956).*

16. Department of Defense Instruction (DoDI) 1215.06, *Uniform Reserve, Training, and Retirement Categories for the Reserve Components,* 19 May 2015, 11.

17. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010 (As Amended Through 15 February 2016), 2.

18. *National Guard, U.S. Code 32 (1956), §§ 708.*

19. Ibid.

20. DOD 7000.14-R, *Financial Management Regulation Volume 14, Chapter 1*, May 2015, 1-6.

21. *Veterans – Military Affairs, Ohio Revised Code 5923 (1997), §§ 5923.21.*

22. NGAUS Fact Sheet, http://www.ngaus.org/sites/default/files/Guard%20Statues.pdf (accessed 13 June 2016).

23. Ibid.

24. Executive Order (EO) 12333, United States Intelligence Activities, 4 December 1981.

25. Ibid.

26. Ibid.

27. Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, 12 February 2013.

28. Enhanced Cybersecurity Services (ECS) | Homeland Security, https://www.dhs.gov/enhanced-cybersecurity-services, (accessed 17 May 2016).

29. EO 13636, Improving Critical Infrastructure Cybersecurity.

30. Ibid.

31. Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, 12 February 2013.

32. Ibid.

33. Ibid.

34. Ibid.

35. Ibid.
36. Ibid.
*37. Supplemental Tool: Connecting to the NICC and NCCIC, https://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Connecting%20to%20the%20NICC%20and%20NCCIC_508.pdf
38. Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, 12 February 2013.
39. DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* December 1982, 13.
40. Ibid.
41. Ibid.
42. Ibid.
43. Ibid., 15.
44. Ibid., 16.
45. Ibid., 21.
46. Ibid., 22.
47. Ibid.
48. Ibid.
49. DoD Instruction (DoDI) 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, 27 February 2013, 1.
50. DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* December 1982, 56.
51. Ibid., 57.
52. DoD Directive (DoDD) 5105.77, *National Guard Bureau (NGB),* 30 October 2015, 1.
53. Ibid., 1-2.
54. Ibid., 2.
55. Ibid.
56. Ibid.
57. Ibid., 4.
58. Ibid.
59. Ibid., 15.
60. Ibid., 16.
61. DoD Instruction (DoDI) 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, 27 February 2013, 1.
62. Ibid., 2.
63. Ibid., 10.
64. Ibid., 23.
65. Ibid.
66. Chief National Guard Bureau Instruction (CNGBI) 2000.01A, *National Guard Intelligence Activities,* 24 July 2015, 1.
67. Ibid., 2.
68. Chief National Guard Bureau Instruction (CNGBI) 3100.01A, *National Guard Counterdrug Support,* 22 June 2015, B-1.
69. Ibid.
70. Ibid., B-2.
71. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 114.

72. Federal Bureau of Investigation, “FBI – Intelligence Defined,” https://www.fbi.gov/about-us/intelligence/defined (accessed 2 June 2016).

73. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

74. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (count on the term “information).

75. Merriam-Webster Dictionary, “Intelligence | Intelligence Definition by Merriam-Webster”, http://www.merriam-webster.com/dictionary/intelligence (accessed 6 June 2016).

76. Ibid.

77. Ibid.

78. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. Government Printing Office, 2011, 416.

79. Ibid.

80. Official Website of the Department of Homeland Security, “About Fusion Centers | Homeland Security”, https://www.dhs.gov/state-and-major-urban-area-fusion-centers, (accessed 6 June 2016).

81. Ibid.

82. Official Website of the Department of Homeland Security, “National Network of Fusion Centers Fact Sheet | Homeland Security”, https://www.dhs.gov/national-network-fusion-centers-fact-sheet, (accessed 6 June 2016).

83. Official Website of the Department of Homeland Security, “Fusion Center Foundational Guidance | Homeland Security”, https://www.dhs.gov/fusion-center-foundational-guidance, (accessed 6 June 2016).

84. Official Website of the Department of Homeland Security, “National Network of Fusion Centers Fact Sheet | Homeland Security”, https://www.dhs.gov/national-network-fusion-centers-fact-sheet, (accessed 6 June 2016).

85. Department of Justice, Office of Justice Programs, Global Information Sharing Toolkit, “GIST - Document Detail - Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers”, http://it.ojp.gov/GIST/178/File/Cyber%20Integration%20for%20Fusion%20Centers.pdf, 1, (accessed 6 June 2016).

86. Ibid.

87. Ibid.

88. Department of Defense, *Cyber Strategy*, iv.

89. Ibid.

90. Ibid., 7-8.

91. Ibid., 14.

92. Ibid.

93. Ibid., 22.

94. Ibid., 22.

95. Ibid., 23.

96. “Council of Governors Joint Action Plan for State-Federal Unity of Effort on Cyber Security,” 2014, 1, http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf (accessed 28 February 2016).

97. Ibid., 3.

98. Ibid.

99. Ibid., 4.

100. *National Defense Authorization Act of 1989*, HR 4481, 100th Congress, https://www.congress.gov/bill/100th-congress/house-bill/4481.

101. Ibid.

102. U.S. Government Accountability Office, *DRUG CONTROL Additional Performance Information Is Needed to Oversee the National Guard's State Counterdrug Program*, GAO-16-133, (Washington, DC, October 2015), 27, http://www.gao.gov/assets/680/673260.pdf.

103. Ibid., 34.

104. Lt Col Maurice M. McKinney, *A National Solution: Rethinking The Employment of Air National Guard Title 32 Status Citizen-Airmen to Defend the Nations Cyberspace* (Maxwell AFB, AL: Air University, 2013), iii, (accessed 25 April 2013), http://www.au.af.mil/au/awc/awcgate/awc/mckinney.pdf.

105. Ibid., 13.

106. Ibid., 14.

107. Chief National Guard Bureau Instruction (CNGBI) 2000.01A, *National Guard Intelligence Activities,* 24 July 2015, GL-2.

108. Ibid., 2.

109. DoD Directive (DoDD) 5105.77, *National Guard Bureau (NGB),* 30 October 2015, 4.

110. Michael German and Jay Stanley, *What's Wrong with Fusion Centers?* American Civil Liberties Union, (Washington DC, 2007), 5.

BIBLIOGRAPHY

Armed Forces, U.S. Code 10 (1956*).*

Atkinson, Rick. "About Left of Boom: The Fight Against Roadside Bombs." *The Washington Post*, 30 September 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/09/28/AR2007092801888.html.

Carter, Ash. Secretary of Defense. *The Department of Defense Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Chief National Guard Bureau Instruction (CNGBI) 2000.01A. *National Guard Intelligence Activities,* 24 July 2015.

Chief National Guard Bureau Instruction (CNGBI) 3100.01A. *National Guard Counterdrug Support,* 22 June 2015.

Council of Governors. "Joint Action Plan for State-Federal Unity of Effort on Cyber Security." 2014. http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.

Department of Homeland Security. "Cyber-Attack Against Ukrainian Critical Infrastructure." Alert IR-ALERT-H-16-056-01. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Department of Homeland Security. "Enhanced Cybersecurity Services (ECS) | Homeland Security." https://www.dhs.gov/enhanced-cybersecurity-services.

Department of Homeland Security. Official Website. "About Fusion Centers | Homeland Security." https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

Department of Homeland Security. Official Website. "Fusion Center Foundational Guidance | Homeland Security." https://www.dhs.gov/fusion-center-foundational-guidance.

Department of Homeland Security. Official Website. "National Network of Fusion Centers Fact Sheet | Homeland Security." https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

Department of Homeland Security. "Supplemental Tool: Connecting to the NICC and NCCIC." https://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Connecting%20to%20the%20NICC%20and%20NCCIC_508.pdf.

Department of Defense (DOD) 5240.1-R. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* December 1982.

Department of Defense (DOD) 7000.14-R. *Financial Management Regulation Volume 14, Chapter 1,* May 2015.

Department of Defense Directive (DoDD) 5105.77. *National Guard Bureau (NGB),* 30 October 2015.

Department of Defense Instruction (DoDI) 1215.06. *Uniform Reserve, Training, and Retirement Categories for the Reserve Components,* 19 May 2015.

Department of Defense Instruction (DoDI) 3025.21. *Defense Support of Civilian Law Enforcement Agencies,* 27 February 2013.

Department of Justice. Office of Justice Programs. Global Information Sharing Toolkit. "GIST - Document Detail - Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers," http://it.ojp.gov/GIST/178/File/Cyber%20Integration%20for%20Fusion%20Centers.pdf.

Executive Order 12333. United States Intelligence Activities. 4 December 1981.

Executive Order 13636. Improving Critical Infrastructure Cyber Security. 12 February 2013.

Federal Bureau of Investigation. "FBI – Intelligence Defined." https://www.fbi.gov/about-us/intelligence/defined.

House, White. "Cyberspace Policy Review: Assuring a trusted and resilient information and communications infrastructure." White House, United States of America (2009).

German, Michael., and Jay Stanley, *What's Wrong with Fusion Centers?* American Civil Liberties Union. (Washington DC, 2007).

Johnson, Jeh. "Homeland Security Secretary Jeh Johnson Testimony on Fiscal Year 2017 Budget." C-SPAN.org. 8 March 2016. video, 1:36:54. http://www.c-span.org/video/?406187-1/homeland-security-secretary-jeh-johnson-testimony-fiscal-year-2017-budget.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 8 November 2010 (As Amended Through 15 February 2016).

Kean, Thomas H., Lee H. Hamilton, Richard Ben-Veniste, Bob Kerrey, Fred F. Fielding, John F. Lehman, Jamie S. Gorelick et al. "The 9/11 Commission Report." National Commission on Terrorist Attacks Upon the United States, Washington DC, 2004.

Larson, Eric, V., and John E. Peters, *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options.* RAND Report MR-1215-A, 2001.

McKinney, Maurice, M., Lt Col, A *National Solution: Rethinking The Employment of Air National Guard Title 32 Status Citizen-Airmen to Defend the Nations Cyberspace.* (Maxwell AFB, AL: Air University, 2013).

Merriam-Webster Dictionary. “Intelligence | Intelligence Definition by Merriam-Webster.” http://www.merriam-webster.com/dictionary/intelligence.

National Guard, U.S. Code 32 (1956*).*

National Defense Authorization Act of 1989. HR 4481. 100th Congress. https://www.congress.gov/bill/100th-congress/house-bill/4481.

National Guard Association United States (NGAUS). “NGAUS Fact Sheet.” http://www.ngaus.org/sites/default/files/Guard%20Statues.pdf.

Obama, Barack. "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience." Washington, DC (2013).

U.S. Government Accountability Office. *DRUG CONTROL Additional Performance Information Is Needed to Oversee the National Guard's State Counterdrug Program.* (Washington, DC, October 2015). http://www.gao.gov/assets/680/673260.pdf.

U.S. Northern Command. Factsheet. *The Posse Comitatus Act.* 16 May 2013.

Veterans – Military Affairs. Ohio Revised Code 5923 (1997). *§§ 5923.21*.