National Guard Intelligence Support to Domestic Operations

A Monograph
by
MAJ Mark L. Coble
United States Army National Guard

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

AY 2009

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
21-05-2009	Monograph	JUL 2008 – MAY 2009

4. TITLE AND SUBTITLE
National Guard Intelligence Support to Domestic Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mark L. Coble, MAJ, US Army National Guard

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
250 Gibbon Avenue
Fort Leavenworth, KS 66027

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
100 Stimson
Fort Leavenworth, KS 66027

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC, SAMS

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The commission formed after the terrorist attacks of September 11, 2001 identified a need for a better domestic intelligence capability, and policy decisions since then have directed increased information sharing between the intelligence community and the collective law enforcement community. This monograph outlines how the new operational environment, which includes the establishment of a new combatant command and the establishment of the Department of Homeland Security, affects domestic intelligence operations through a review of current regulations and policies affecting domestic intelligence operations. It advocates provision of intelligence support to established state level intelligence centers by each state's National Guard predominantly through information sharing, with the National Guard assets serving as a conduit for information between the intelligence community and the state intelligence fusion centers. It is beneficial to the each state's National Guard Joint Forces Headquarters to support this because of the capability for increases situational awareness, with little change to existing regulations due to the requirement to maintain a common operating picture.

15. SUBJECT TERMS
National Guard, Intelligence, Domestic Operations, Civil Support, Homeland Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			COL Stefan Banach
(U)	(U)	(U)	(U)	50	**19b. PHONE NUMBER** *(include area code)* 913-758-3300

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

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

MAJ Mark L. Coble

Title of Monograph: National Guard Intelligence Support to Domestic Operations

Approved by:

_____ Monograph Director
Dan G. Cox, Ph D.

_____ Director,
Stefan Banach, COL, IN School of Advanced
Military Studies

_____ Director,
Robert F. Baumann, Ph.D. Graduate Degree
Programs

Abstract

NATIONAL GUARD INTELLIGENCE SUPPORT TO DOMESTIC OPERATIONS

The commission formed after the terrorist attacks of September 11, 2001 identified a need for a better domestic intelligence capability, and policy decisions since then have directed increased information sharing between the intelligence community and the collective law enforcement community. This also brings into question the role of military intelligence within domestic operations, and specifically the role and relationships of the National Guard within the framework of state and local intelligence fusion centers.

In order to understand the limits of military intelligence support to domestic operations, an appreciation of the history of intelligence oversight and the policy, directives, and regulations covering military intelligence support is necessary. To be able to predict future trends requires a review of the changes to intelligence sharing brought about by the attacks of September 11, 2001. This monograph outlines how the new operational environment, which includes the establishment of a new combatant command and the establishment of the Department of Homeland Security affects domestic intelligence operations through a review of current regulations and policies affecting domestic intelligence operations.

This monograph advocates provision of intelligence support to established state level intelligence centers by each state's National Guard. Because of current legal restrictions, this support should be predominantly through information sharing; with the National Guard assets serving as a two-way conduit for information between the intelligence community and the state intelligence fusion centers. It is beneficial to the each state's National Guard Joint Forces Headquarters via increased level of situational awareness which will occur due to the assets physical presence in the fusion centers. This can be accomplished with little change to existing regulation due to the requirement to maintain a common operating picture. This will require the management of a domestic intelligence program versus maintaining a risk avoidance posture.

TABLE OF CONTENTS

I. INTRODUCTION

As officers in the military, we swear an oath to "support and defend the Constitution against all enemies, foreign and domestic."[1] This oath has two parts that serve as major themes and balance points for this monograph. What role should the military, and specifically National Guard assets, play within domestic intelligence operations given the legal constraints placed on the Department of Defense (DoD) through Congressional intelligence oversight, and given the necessity of recent intelligence sharing initiatives under the Department of Homeland Security? All debate on this subject flows from this balance between physically securing the homeland and securing the moral foundation, the protection of civil liberties, from which our country was born.

An inquiry into intelligence operations focusing on the differences between domestic intelligence operations and traditional military intelligence operations, and the restrictions placed upon military intelligence professionals regarding domestic operations show a clear difference, via restrictions placed upon the military, between the conduct of domestic military intelligence operations and military operations outside the United States. Yet with the demise of the Soviet Union, and a recently realized understanding that for the foreseeable future this environment will be defined by a global struggle against a violent extremist ideology that seeks to overturn the international state system[2], the utility of intelligence techniques and trained intelligence professional focused on trans-border threats is clear. The challenge the military faces is a problem of clearly understanding the boundaries imposed by regulation and changes in policy in the aftermath of 9/11. Often at the policy level, policy makers will adopt a risk avoidance attitude vice a risk management one simply because a clear understanding of the boundaries of action have not been completely explored. Thus, the intent of this monograph is to explore the boundaries through an analysis of the history and creation of policy documents, commentaries associated with them,

---

[1] Department of the Army, DA Form 71, Oath of Office, Military personnel, Jul 1999,1

[2] Department of Defense, *National Defense Strategy*, 2008, 2

and evolution of the systems that are currently in place, assessing if there are opportunities to effectively use National Guard intelligence assets to improve current systems. A further focus of this inquiry will be on the policies enacted that restrict the use of the military and the intelligence community within our borders, and changes within the policy realm as the threat has moved from outside our borders to inside, thus necessitating a change for the intelligence community. Current intelligence structures that have full-time National Guard participation, and regional intelligence fusion cells under the auspices of the Department of Homeland Security rounds out the scope of the inquiry. The legality of intelligence sharing, and potential pitfalls that reduce the efficiency and effectiveness of intelligence sharing between state/regional fusion centers and USNORTHCOM (as the Department of Defense (DoD) combatant command in charge of homeland security) are potential points of friction between current law and the goals outlined in the National Strategy for Homeland Security.

The author believes that National Guard intelligence activities can serve a supporting role that is in line with both the letter and spirit of current standing Executive Orders and Department of Defense Directives (DoDD) regarding domestic intelligence support. Moreover, National Guard assets can serve as a vital information bridge between state and local assets and DoD information, intelligence, and consequence management assets. Standardizing open source intelligence products and data mining capabilities, and expanding current intelligence support to civil authorities while sustaining current intelligence oversight programs to ensure compliance with regulatory requirements will enhance the capabilities of state and local fusion centers and Defense Support to Civil Authorities operations.

SIGNIFICANCE OF RESEARCH

As Defense Secretary Gates stated in the National Defense Strategy, “The core responsibility of the Department of Defense is to defend the United States from attack upon its territory at home and to secure its interests abroad. As the spreading web of globalization presents new opportunities and challenges, the importance of planning to protect the homeland against previously unexpected threats

increases. Meeting these challenges creates a tension between the need for security and the requirements of openness in commerce and civil liberties".[3]

Further, the emergence of state and regional information and intelligence fusion centers as a response to the new security requirements after the 9/11 reinforces the understanding of the nature that the threat posed by globalization and a change from State versus State conflict has upon the intelligence community. This shows the necessity of a change in intelligence capacity from a purely extraterritorial focus to a trans- border one. The requirements inherent in this change in focus show a need to standardize, create, and share information in order for defense leaders and planners, in conjunction with the interagency community and the states, to gain and maintain a common operation picture within the confines of current statutory requirements.

The National Guard serves well to bridge this interagency gap because of its dual role within Title 32[4] and Title 10[5], and due to lesser restrictions on supporting law enforcement entities than other DoD assets because of a lack of *Posse Comitatus*[6] restriction. The subject of this monograph goes further, exploring and attempting to clarify the threshold of legal restrictions to domestic intelligence operations. Due to the increased domestic terror threat, there is a necessity for an additional information sharing bridge that has traditionally been termed intelligence sharing (and thus restricted to DoD). This has been tasked within strategic guidance documents, and within the new national intelligence framework. Coupled with the emergence of state fusion centers, there exists a need to maximize the utility of Department of Defense intelligence resources for homeland security and homeland defense, while

---

[3] Department of Defense, *National Defense Strategy*, 2008, 6-7

[4] US Congress, US Code Title 32 outlines the organization of the National Guard. By common usage, a Title 32 status considers the service member as under state control being paid by the federal government

[5] US Congress, US Code Title 10 outlines the organization of the Armed Forces of the US

[6] .", Posse Comitatus Act, US Code 18, section 1385, accessed from Domestic Operations Law Handbook, 2006, 14. The Posse Comitatus Act States:"Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both

following the regulations that keep these resources from potentially being used against our citizens . The author postulates that the National Guard has the assets and processes, within the existing legal framework, to maximize intelligence sharing and serve to gain and maintain a common operating and information picture within its role of civil support to domestic authorities, thus ameliorating a current point of friction between the federal and state/local law enforcement community. The National Guard, operating at the individual state level can also provide a communication bridge between the Department of Defense intelligence community and state/local entities.

THE ISSUE OF DOMESTIC INTELLIGENCE

To fully explore the issue of domestic intelligence, and to serve as a framework for inquiry, the author posed additional research questions. How do domestic intelligence operations differ from "normal" or foreign intelligence operations? What is homeland defense and how does it differ from homeland security, and why is this difference important for us? What is the history of intelligence oversight, and how do current Executive Orders, DoD Directives, and Army Regulations conform to this intelligence oversight process? How does the National Guard fit into this framework within the DoD in regards to intelligence oversight, and how does the National Guard fit within the intelligence community? How has domestic intelligence and counterintelligence changed in response to the terrorist attacks on 9/11, and how has Congress changed its policies towards domestic intelligence in light of 9/11? How has the Department of Homeland Security evolved, and what information sharing structures have evolved since its inception? What additional problems are still found within that system, and how can the National Guard, with its dual role affect them? What are the implications of the emergence of information and intelligence fusion centers? How do local intelligence fusion centers meet the intent of local support to homeland security and what are the current issues with meeting this intent?

Domestic intelligence as a component of homeland security and homeland defense is a relatively new topic, particularly federal support and coordination with state and local authorities. Thus, most of the sources are monographs and theses on current or emerging policies and debate on policy direction and

research projects at various military and civilian colleges. The first group of sources are the laws, policies, regulations, and doctrine regarding the establishment of the Department of Homeland Security (DHS), the USA PATRIOT ACT, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), how these affect the National Security Strategy and the National Strategy for Homeland Security, and the military's response and tasking from them. Included in the doctrine are the definitions of intelligence and the utilization of intelligence by the military. This is important because it establishes a common lexicon between the military and the intelligence community which is somewhat absent as we look at emerging organizations working within the domestic intelligence field. Commissioned works by the Congressional Research Service and RAND Corporation help to clarify the background documentation given to government officials to help either interpret or influence policy decisions. Closely related to these are the many policy statements and speeches made by President Bush and those within his administration. A review of Army regulations, National Guard Bureau Regulations, Joint Publications and Army doctrine regarding domestic operations and intelligence ties the policy decisions to action at the operational and tactical level.

A majority of the current commercial works are books describing the intelligence community or the intelligence process. Jeffrey Richelson's and Mark Lowenthal's work on the subject serve well to describe the intelligence community and also to provide updates and the evolution of it.[7] Commentary external to the Government regarding domestic intelligence effectiveness and the balancing of intelligence activities and the maintenance of civil liberties have been mainly focused on reshaping the intelligence community and advocating an agenda of reform along ideological lines. Two books by Richard Posner provide timely analysis of the evolution of intelligence policy reform outside government institutions and works commissioned by the government as well as provide useful debate over the role of

[7] In particular, Jeffrey Richelson's, "The US Intelligence Community, 5thEdition", 2008, And Lowenthal's "Intelligence: From Secrets to Policy: 4th Edition" serve as excellent resource books that have been updated by the author and thus shows the evolution of the intelligence community, and changes based upon policy and 9/11.

the federal government within domestic intelligence.[8] While his main premise; the need for a separate, MI5 style domestic agency as the principal counterterrorism node is outside the topic of this monograph, his analysis of domestic intelligence does provide a voice external to the government and is useful within this debate.

JP 1-02 defines intelligence as "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. The term is also applied to the activity which results in the product and to the organizations engaged in such activity."[9] Information is defined as," 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation."[10] Key to these definitions is the understanding that an intelligence product is created as a result of manipulation of information using a process. But, intelligence is more than a product. Intelligence is also an activity, the dialogue between customers and consumers of the product and the organizations engaged in the production of intelligence. Typical consumers of intelligence as a product are other analysts, planners, and decision and policy - makers across the spectrum of levels of authority and responsibility. Important within our definition of intelligence is the capability to disseminate the product of analysis to all consumers , while still understanding and maintaining security of the product. It is also important to put the collection and analysis activities into perspective, to relate these activities to the needs of the consumers, and the feedback built in to the intelligence process. The joint intelligence process consists of six categories of intelligence operations; planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. In many situations, the various

---

[8] Richard Posner" Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11" and "Uncertain Shield: The US Intelligence System in the throes of Reform" provide a solid commentary of policy actions from 2002 through 2005

[9] Department of Defense, Joint Publication 1-02,*Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994, 270

intelligence operations occur nearly simultaneous with one another, or may be bypassed altogether.[11] How each of these categories of intelligence operations affects current domestic intelligence operations and National Guard capabilities will be explored in future sections of this paper.

There are numerous intelligence collection disciplines through which the US intelligence community collects intelligence to support informed national security decision-making at the federal level and the allocation of tactical military and law enforcement resources at the local level. The collection disciplines are generally referred to as those which fall within national technical means or nontechnical means, and typically they are defined by the nature of their source. Technical means include signals intelligence (SIGINT), measurement and signatures intelligence (MASINT), and imagery intelligence (IMINT). Non-technical means include human intelligence (HUMINT) and open source intelligence (OSINT). Traditionally technical sources have fallen under the direction of the DoD, and non-technical means under the CIA. Access to the products of these sources varies dependent upon the classification of the source and product. The creator of the product is the classification authority, as specified by regulation (in the case of the Army, AR 380-5, Department of the Army Information Security Program), and requests to reclassify and declassify follow regulatory guidance as described in AR 380-5. This is important as initiatives to improve information and intelligence sharing across federal and state entities emerge as a response to 9/11.

An additional intelligence discipline is counterintelligence. Counterintelligence is defined as "Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[12] Counterintelligence, though, is more than a defensive activity. Three types of counterintelligence illustrate this; stopping an adversary's

---

[10] Ibid. 262

[11] Department of Defense, Joint Publication 2-0, *Joint Intelligence*, 22 June 2007, I 6-7

efforts to penetrate your own intelligence system, gaining information about an opponent's capabilities to collect against yourself, and after identifying these efforts using them against the adversary.[13] The first type of counterintelligence activity points us to a major friction point between members of the intelligence community and outside agencies; the previous necessity of adopting compartmentalization and a "need to know" philosophy. Compartmentalization is a counterintelligence response to the efforts of foreign intelligence services' efforts to gain information on our intelligence activities, and the means and methods of collection.[14] The "need to know" standard is an effective method for counterintelligence, but it also serves to impede the sharing of intelligence, especially between agencies. The intelligence community began stressing the "need to share" between agencies in 2003, and in 2007, the Director of National Intelligence further addressed the need for a shift in paradigm away from "need to know" to the "responsibility to provide".[15] This goes above the "need to share" because this is referring to sharing information and intelligence outside the intelligence community. Ways to accomplish this are part of the conclusion of this monograph.

The next two terms are linked, and have only recently been added to the lexicon with their current definitions; homeland defense and homeland security. Homeland defense is defined as, "The protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the President."[16] Homeland security is defined as, "A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage

---

[12] Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* , 23 March 1994, 130

[13] Mark Lowenthal, "Intelligence: From Secrets to Policy: 4th Edition", 2008, 151

[14] Ibid. 153-154

[15] Ibid. 154

[16] Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* , 23 March 1994, 245

and recover from attacks, major disasters, and other emergencies that occur."[17] At the federal level, civil support and homeland defense are separated, and both together describe DoD support to homeland security. By definition the lead agency for homeland defense is the DoD with the DoD taking more of a supporting role within the larger encompassing term homeland security. Joint Publication 3-27 *Homeland Defense* and Joint Publication 3-28 *Civil Support* serve as supporting documents for implementation of The National Strategy for Homeland Security, Strategy for Homeland Defense and Civil Support, and the National Response Plan (NRP), which communicate processes, roles, and responsibilities for consequence management operations. These national strategies, policies, and processes define how the government should react in a disaster response and the integration of intelligence operations and resources as well as information sharing expectations between the DoD and State/Local and Federal agencies.

All of these documents are recent additions to the body of directives and strategies regarding domestic operations, but they all outline restrictions placed upon the DoD regarding domestic intelligence operations by the United States Congress in the 1970's. These restrictions are congressional responses to the perceived abuses of power by the intelligence community.

II. HISTORY OF DOMESTIC INTELLIGENCE RESTRICTIONS

The history of Congressional oversight of domestic military intelligence activities dates back to the 1970's. In its final report entitled, *Intelligence Activities and the Rights of Americans*, the United States Senate claimed during the 1960s intelligence activity carried out by the FBI and the military progressed from being focused against groups with the potential backing of foreign governments to those that protested the Vietnam war and civil rights abuses by the government, often without regard for the consequences to American liberties.[18]

The intelligence agencies of the United States, sometimes supported by public opinion and often in response to pressure from administration officials or the Congress, frequently disregarded the law in

[17] Ibid., 245

their conduct of massive surveillance and aggressive counterintelligence operations against American citizens. Between 1972 and 1974, some of the activities were curtailed, partly in response to the moderation of the domestic crisis; but all too often improper programs were terminated only in response to exposure, the threat of exposure, or a change in the climate of public opinion, such as that triggered by Watergate.[19] By Executive Order[20], and DoD Directive the policy since that time generally gives the FBI responsibility for domestic collection of intelligence. Other national security agencies are to refrain from domestic intelligence collection or operations.

DoD Directive 5240.1 *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, outlines this policy, and Army Regulation (AR) 381-10, US Army Intelligence Activities implements the DoD Directive within the Army. AR 381-10 contains both broad policy guidance and very specific directions for approval of specialized investigative and collection techniques. The chapters in AR 381-10 outline 15 procedures and two clarifying chapters that enable DoD intelligence components to perform effectively their authorized functions while ensuring that activities affecting US persons[21] occur in a manner that protects the Constitutional rights and privacy of such persons. AR 381-10 applies to all Army intelligence components or activities as well as any organization, staff, or office used for foreign intelligence or counterintelligence purposes.

AR 381-10 defines intelligence activities as all activities necessary for the conduct of foreign relations and the protection of national security pursuant to Executive Order 12333. Executive Order 12333 defines these activities – for the foreign intelligence and counterintelligence elements of the Army – as "military and military-related foreign intelligence and counterintelligence [gathering] . . . and

---

[18] United States Senate, “The Growth of Domestic Intelligence”, Washington D.C. CRS, 1976, 3

[19] Ibid, 3

[20] Specifically Executive Order 12333 which has been renewed by every administration since Reagan

[21] Executive Order 12333, note 2 paragraph 3.4 defines a US Person as, ”a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association with a substantial number of members who are citizens of the US, or are aliens lawfully admitted for permanent residence, or a corporation that is incorporation in the US.

information on the foreign aspects of narcotics production and trafficking." As defined by AR 381-10, intelligence components include all of the following Active Army, Army Reserve, and Army National Guard (ARNG) activities that typically conduct a military intelligence mission or intelligence operations. Per the regulation, because military intelligence is exclusively a federal mission, AR 381-10 controls the activities and training of the Army National Guard when using military intelligence resources and assets that the federal government has provided, including activities or training that takes place in Title 32 status.[22] This is a very important portion of the regulation because it ensures that all Army National Guard intelligence personnel, when receiving federal pay, are required to comply with this regulation. Further, even where the Soldiers are on State Active Duty (thus under the pay and authority of the state), they must comply with this regulation if they are using any federal equipment.[23] The regulation goes on to specify that all intelligence components must not infringe upon the rights of any United States person, must protect the privacy rights of all persons entitled to such protection, be based upon a lawfully assigned function, employ the least intrusive, lawful technique, and comply with all regulatory requirements regarding holding of information, etc.[24]

Especially important to the regulation and germane for greater understanding of both the restrictions and the unrestricted areas as the author describes the boundaries of domestic intelligence is the definition of domestic collection. Per AR 381-10, information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of official duties. For information to be "received for use" and therefore "collected" by an Army intelligence component, an employee must take some action that demonstrates intent to use or retain the information received (such as producing intelligence, an investigative summary, or electronic storage of received data). Establishment of "unofficial files" and the like may not be used to avoid the application of this

---

[22] Department of the Army, *Intelligence Oversight Guide*, June 2007, 1-2 - 1-3

[23] Ibid, 1-3

[24] Ibid,, A-1

definition of collection. Data acquired by electronic means is "collected" only when it has been processed into intelligible form. Information held, or forwarded to a supervisory authority, solely for the purpose of making a determination about the collectability of that information under this procedure (and not otherwise disseminated within the component) is not considered to be collected.[25]

Further, information may be collected on a US person under specific circumstances if the collecting agency has the mission to collect, to protect, or if the person consents, if the information is open source, if the person is an employee of the DoD, a contractor of the DoD, or if the person has connections with foreign intelligence services, is subject of an international counterintelligence objective, poses a threat to personnel and physical security of DoD employees, installations, operations, or official visitors.[26]

Typically, violations of this regulation occur when Force Protection or antiterrorism information is incorrectly included in intelligence products, both of which are the Provost Marshall's job. This delineation of responsibility does not mean that military intelligence components should not pass information of this type to the appropriate authorities, when Army intelligence activities gather information that leads to a reasonable belief that a crime has been committed, they must refer the matter to the appropriate law enforcement agency.

The key point is that intelligence components should not collect, retain, and disseminate this kind of information for military intelligence purposes. Other violations may occur when units provide support to civilian law enforcement agencies, especially when after-action reports and threat assessments are brought back from the support missions and incorporated into US Army intelligence files. When the intelligence personnel are on authorized missions supporting a civilian law enforcement agency, they may collect certain information on US persons. That information, however, remains the property of the law enforcement agency, and the intelligence component may not retain this information in intelligence files.

---

[25]Department of the Army, Army Regulation 381-10, *US Army Intelligence Activities*, 1 July 1984, 1

Individuals with military intelligence training may be detailed to support law enforcement efforts based upon their specific skills, but their activities should not be co-mingled with work in their military intelligence field or create the perception that a US Army military intelligence component is collecting information on US citizens.

DoD Intelligence assets are authorized to assist Civilian Law Enforcement Authorities only upon the approval of the Secretary of Defense, and for the following purposes; investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities. Protecting DoD employees, information, property, facilities, and information systems. Preventing, detecting, or investigating other violations of law. Providing intelligence personnel and specialized equipment and facilities to federal authorities and, when lives are endangered, to state and local authorities in accordance with DoD Directive 5525.5.[27] DoD Directive 5525.5 outlines DoD assistance to interagency community for law enforcement support, and generally authorizes usage of assets when the usage does not affect the mission readiness of the organization, except where it is not in compliance with DoDD 5240.1.

How does the National Guard fit into this framework within the DoD in regard to domestic operations, intelligence oversight, and how does the National Guard fit within the overall intelligence community? The National Guard has been defending the homeland and providing support to civil authorities since it's inception in colonial Massachusetts in 1636. Organized as State Militias, National Guard members are subject to control by the executive branch of their respective states and territories. They also fall under the rules and regulations of the Department of Defense, and serve as reserve of the military. Largely unused as an expeditionary force during the Cold War, the National Guard focused much attention on its homeland security mission; providing military support to civil authorities through domestic disturbance and disaster response. Since the collapse of the Soviet Union, and the changing

---

[26] Ibid, 2

predominant style of warfare; moving away from conventional threats to unconventional threats, the importance of the homeland security mission for the National Guard has also changed. The National Defense Authorization Act for Fiscal Year 2008 directs the Secretary of Defense, in consultation with the Secretaries of the Army and the Air Force, and the Chairman of the Joint Chiefs of Staff to develop and prescribe a revised charter for the National Guard Bureau. The National Guard Bureau (NGB) is the federal military administrative, policy, and logistical coordination center for the Army and Air National Guard. During National Guard Domestic Operations, the National Guard Bureau provides policy guidance and facilitates assistance, when needed, by locating and coordinating National Guard units and resources. In its role as the channel of communication, the National Guard Bureau assists the Secretary of Defense in preparing a plan for coordinating the use of the National Guard and members of the Armed Forces on active duty when responding to natural disasters, acts of terrorism, and other man-made disasters by providing information gathered from Governors, the Adjutants General, and other state civil authorities responsible for homeland preparation and response.[28]

Therefore to understand the structure of the National Guard, is to understand that the National Guard Bureau does not control the organizations within the separate states, but only provides coordination and guidance. The Title 32 – Title 10 "dual hat" status of the National Guard of the United States (Reserve Force) and the National Guard (Militia of the States and Territories) affords the National Guard flexibility to act as a bridge within a tiered incident response framework: local-state-federal; and provide the means for maintaining unity of effort.

But, neither the National Guard holistically or as a community of separate state entities, or the National Guard Bureau are members of the intelligence community. At this time, the National Guard Bureau does not have a dedicated intelligence infrastructure; capable of conducting the intelligence process and providing an intelligence product for intelligence consumers. There is not a necessity for

---

[27] Department of the Army, *Intelligence Oversight Guide*, June 2007, A-4-A-5

NGB to produce intelligence, but it is an intelligence consumer because of its role coordinating domestic operations support between the DoD and the states.[29] This is a new role for NGB , and was implemented as a response to both the 9/11 attacks and the aftermath of Hurricane Katrina. As already specified, all National Guard intelligence activities are required to conform to DoD directives and regulations regarding collection on US persons. The only exception to this would be State Active Duty (not funded by DoD) in a situation where there is no federal funding for the equipment, or as part of counter narcotic support, or potentially as part of a civil support mission involved in consequence management (described below). National Guard Regulations 500-1 (National Guard Domestic Operations, 2008), 500-2 (National Guard Counter Drug Support), and 500-3 (Weapons of Mass Destruction Civil Support Management) all deal with emergency employment of Army and other Resources. Within the regulation outlining National Guard support to domestic operations and Weapons of Mass Destruction Civil Support Management, there is no mention of specific intelligence operations tasks, and only passing reference to information operations. There is a section regarding intelligence oversight and requirements to follow all aspects of DoDD 5240.1 outlined in the National Guard Counter Drug Support Regulation.

The intelligence community before 9/11 can best be understood as being divided along two lines. The first was the DoD/CIA (technical versus non-technical means) divide. The CIA—doing human intelligence collection and all-source analysis was an independent entity, while agencies performing signals and imagery intelligence were located within DoD. The second line was the foreign/domestic divide. The National Security Act of 1947 forbade the CIA from performing internal security functions. At the same time, the FBI protected its role as the premier domestic intelligence and law enforcement agency. Moreover, as previously stated, the abuses committed by intelligence agencies in the 1960s and early 1970s led to reluctance across the intelligence community to cross the foreign/domestic divide. This

---

[28] National Guard Bureau, NGR 500-1, *National Guard Domestic Operations*, 2008, 3

[29] National Guard Regulation 500-1, National Guard Domestic Operations, 2008, 5. Chapter 4 outlines the mission of the National Guard Bureau in regards to Domestic Operations.

was not such a large issue as long as the predominant threat were other nation-states using industrial-age capabilities congruent with our own. This created a situation where domestic collections worked more towards rules of evidence and information to support criminal conviction of miscreants versus typical intelligence analysis operations.

III. CHANGES TO DOMESTIC INTELLIGENCE CAUSED BY 9/11

Many changes to the intelligence community were recommend by the 9/11 Commission in its aftermath. Five main recommendations for action from the 9/11 report were; unifying strategic intelligence and operational planning against terrorists across the foreign-domestic divide with a National Counterterrorism Center, unifying the intelligence community with a National Intelligence Director, creation of a networked-based information-sharing system that transcends traditional governmental boundaries, unifying and strengthening congressional oversight to improve quality and accountability, and strengthening the FBI and homeland defenders.[30] Many of these issues were apparent prior to the publishing of the Commission's report, and were incorporated into the USA PATRIOT Act, which had specific sections adjusting information sharing across agencies within the Federal government (Section 203 and 204), and the State and local governments, through "maintaining and operating regional information sharing systems that are responsive to the needs of participating enforcement agencies in addressing multijurisdictional offenses and conspiracies, and that are capable of providing controlling input, dissemination, rapid retrieval, and systematized updating of information to authorized agencies" and "establishing and operating secure information sharing systems to enhance the investigation and prosecution abilities of participating enforcement agencies in addressing multi-jurisdictional terrorist conspiracies and activities".[31] This was part of the impetus to the creation of state and local Information Fusion Centers.

---

[30] National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 2004, 399-400

[31] US Congress, *USA PATRIOT Act*, 2001, Section 701(4)

The creation of the Department of Homeland Security (DHS) was another change whose impetus was the 9/11 attacks. In June 2002, as part of the proposal for the creation of the DHS, President Bush outlined the necessity of a single entity focusing the efforts for homeland security; that responsibilities for homeland security were dispersed among more than 100 governmental organizations.[32] Additionally, this organization would synthesize and analyze homeland security intelligence from multiple sources, coordinate communications with state and local governments, private industry, and the American people about threats and preparedness, help train and equip first responders, and manage federal emergency response activities, and reducing duplicative and redundant activities that drain critical homeland security resources.[33] Regarding Intelligence and threat analysis, the DHS would fuse and analyze intelligence and other information pertaining to threats to the homeland from across the intelligence community. The proposal included a plan to merge under a single entity the capability to identify and assess current and future threats to the homeland, map those threats against current vulnerabilities, issue timely warnings, and immediately take or effect appropriate preventive and protective action. Also, the department would be responsible for comprehensively evaluating the vulnerabilities of America's critical infrastructure, including food and water systems, agriculture, health systems and emergency services, information and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons.[34]

The document emphasizes that while the federal government is the primary entity responsible for taking the lead and providing the plans, funds, and priorities for this security, the country's critical assets and populace will never fully be protected without the complete cooperation of everyone at all levels to include state and local governments, private organizations, and individual citizens. Working closely with

---

[32] The White House, *The Department of Homeland Security*, June 2002,1

[33] Ibid,1-2

[34] Ibid. 1-2

state and local officials, other federal agencies, and the private sector, the Department of Homeland Security would help ensure that proper steps are taken to protect high-risk targets, and consolidate and streamline relations with the federal government for infrastructure protection and information support to America's state and local governments. DHS would contain an intergovernmental affairs office to coordinate federal homeland security programs with state and local officials. It also would give state and local officials one primary contact instead of many when it comes to matters related to training, equipment, planning, and other critical needs such as emergency response.[35] Pitfalls within the DHS in regard to vertical (between subordinate agencies and state and local authorities) and horizontal coordination and communication were a specific lesson learned in the aftermath of Hurricane Katrina. These continue to be addressed as of this date.

On October 1, 2002, President Bush established USNORTHCOM with a mission to anticipate and conduct Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests. Its Area of Responsibility includes air, land, and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico and the Straits of Florida. In providing civil support, USNORTHCOM generally operates through established Joint Task Forces subordinate to the command. In most cases, support will be limited, localized and specific. When the scope of the disaster is reduced to the point that the Primary Agency can again assume full control and management without military assistance, USNORTHCOM will exit, leaving the on-scene experts to finish the job.[36] While Northern Command has no direct liaison authority with the Department of Homeland Security, or other federal agencies – this is the task of the Department of Defense – it will establish effective working relationships and cooperative efforts to improve coordination and information

---

[35] Ibid, 3

[36] United States NORTHCOM website (on-line); accessed at http://www.northcom.mil/About/index.html ; internet; on January 2, 2009.

flow, in particular through the assignment of interagency partners as permanent staff to US USNORTHCOM's Headquarters. USNORTHCOM's Combined Intelligence and Fusion Center is tasked with collation of intelligence from the National Security Agency (NSA), CIA, the FBI and other agencies as well as open source intelligence in order to provide indications and warnings, long term threat and vulnerability assessments for specific events and areas, targeting tips to law enforcement, current intelligence and summaries, and management of requirements.[37] In September 2008, Commander USNORTHCOM, signed USNORTHCOM's first Theater Campaign Plan, focusing on three areas; anticipating threats to continental security, improving homeland defense and civil support plans and capabilities, and strengthening relationships with their mission partners, the interagency community and the militaries of Canada and Mexico.[38]

In response to the 9/11 Commission recommendations, President Bush issued four Executive Orders on 27 August 2004; the Strengthened Management of the Intelligence Community[39] amending Executive Order 12333, establishment of a National Counterterrorism Center[40], Strengthening the Sharing of Terrorism Information to Protect Americans [41], and Establishing the President's Board on Safeguarding Americans' Civil Liberties[42]. The amendments to Executive Order 12333 created a Director of National Intelligence (DNI), but did not give the DNI power over all elements of the Intelligence Community, in particular to the intelligence agencies within the DoD.[43]

---

[37] Jeffrey T. Richelson, *The Intelligence Community, 5th Edition,* 2008, 123-124

[38] US Congress, Statement of GEN Renuart, CDR USNORTHCOM to House Armed Services Committee, 18 MAR 2009,17

[39] Executive Order 13355

[40] Executive Order 13354

[41] Executive Order 13356

[42] Executive Order 13552

[43] Executive Order 13355 did not provide the DNI with the authority for oversight into the budgets of the intelligence community members traditionally associated with DoD

The Executive Order creating the National Counterterrorism Center restricted its counterterrorism activities. The NCTC would not have the authority to direct covert counterterrorism operations abroad or at home, and though it would be involved in planning of operations, it would not execute them but would serve as a coordination center between agencies in regards to counter terror activities. Operations execution remained with the FBI, CIA, and Pentagon depending on the activity.

The third Executive Order directed all Executive Branch agencies to promptly share information relating to terrorism with other agencies with counterterrorism functions. Policy decisions worked to prevent this exchange of information prior to 11 September 2001. It ordered the DCI to establish common standards across the intelligence community and to establish an Information Systems Council that will plan and oversee an interoperable terrorism-information-sharing environment.[44] Execution of this executive order will be addressed in later sections.

The final executive order was created to ensure the safeguard of legal rights of all Americans. The Deputy Attorney General is the Chair and the Under Secretary for Border and Transportation Security of the Department of Homeland Security is the Vice-Chair. Other members are senior officials across the federal government.[45]

Within months of the creation of these Executive Orders, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), created to improve the effectiveness of the intelligence community. This legislation augmented the previously listed Executive Orders aimed at providing specific Administration direction, including creation of an Office of Director of National Intelligence, outlining additional duties and responsibilities to include additional power pertaining to budgeting and policy within the intelligence community, as well as legislative support for the creation of the National Counterterrorism Center. An important concept defined in the IRTPA was "national

---

[44] Executive Order 13356 section 2 made it the duty of the heads of agencies holding intelligence to disseminate that information and coorperate with its dissemination

[45] Melanie Gutjar, *The Intelligence Archipelago, The Community's struggle to reform in the Globalized Era*, Washington D.C., Joint Military Intelligence College Press, 2005, 85-86

intelligence", which refers to all intelligence, regardless of the source from which it is derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests, the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.''[46] This is an important concept because of understanding that a clear division of "foreign intelligence" and "domestic intelligence" no longer is a useful separation in a globalized information environment, hence all elements within the intelligence community need to share information to the greatest extent possible. The IRPTA also required the President to create an intelligence sharing environment that was outlined in Executive Order 13388, issued on October 25, 2005, which required that "agencies shall, in the design and use of information systems and in the dissemination of information among agencies; give the highest priority to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, the interchange of terrorism information among agencies, the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and the protection of the ability of agencies to acquire additional such information"[47]. Concurrently, protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implemented above.

Application of the tasks and charter outlined in the IRPTA was delineated in the National Intelligence Strategy of 2005; integrate the domestic and foreign dimensions of US Intelligence so that there are no gaps in understanding of threats to national security, bring additional depth and accuracy to intelligence analysis, and ensure intelligence resources generate future capabilities as well as present

---

[46] US Congress, PL 108-458, *Intelligence Reform and Terrorist Prevention Act of 2004*, Dec 2004, Section 1012

[47] Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, October 2005, Section 1

results. National intelligence must be collaborative, penetrating, objective and far-sighted, tailored to the threats of the 21st century.[48] The primary task of an integrated intelligence community remains to inform and warn decision-makers as well as military commanders, but in addition, to inform domestic law enforcement and homeland security authorities in the field.

Three specific documents serve as principal supporting documents to the National Intelligence Strategy. The National Strategy for Information Sharing (2007), the Defense Intelligence Strategy (2008), and the Department of Homeland Security Information Sharing Strategy (2008) outline necessary changes in the previous culture that predominated within the intelligence community and provide steps that need accomplished in order to meet the requirements of Executive Order 13388.

The focus of the National Strategy for Information Sharing is improving the sharing of homeland security, terrorism, and law enforcement information related to terrorism within and among all levels of governments and the private sector.[49] Within the National Strategy for Information Sharing, the access to timely and accurate information regarding those who want to attack us, their plans and activities, and the targets that they intend to attack drives the need for a change in the current communication and coordination policy. The information shared will enhance efforts to identify threats, identify persons involved in terrorism related activities, and implement information-driven and risk-based detection, prevention, deterrence, response, protection, and emergency management efforts.[50] It enumerates that experience has shown that there is no single source for information related to terrorism. Intelligence is derived by gathering, fusing, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. It points out that because there is not a single source of information that can be turned into intelligence products, and because important information can come through the efforts of the intelligence community, other federal agencies, state, tribal, and local law enforcement and homeland

---

[48] Office of the Director in National Intelligence, *National Intelligence Strategy*, Oct 2005, 2-3

[49] The White House, *National Strategy for Information Sharing*, October 2007, 3

[50] Ibid. 2

security authorities, or the private sector, information must be shared to gain a common picture. As one can see, this is a departure from previous guidance regarding domestic intelligence sharing and collection.

The Defense Intelligence Strategy also outlines the need to evolve with the current threat and cross traditional boundaries in order to fully support the military and policy customer. "The deep integration of defense intelligence into the larger Intelligence Community, the evolution of our collaboration with homeland defense counterparts, and the fostering of committed international partnerships are all outcomes of this fundamental change."[51] Key to this evolution is information management. "…We must not only leverage the capabilities of our partners but also improve our ability to ingest and archive large amounts of data, and extract and disseminate to our customers and partners all relevant information."[52] But there are inherent pitfalls associated with technology, "Because data management and information extraction will be done increasingly in a networked environment, more research on availability, confidentiality, and the integrity of data is vital."[53] The Defense Intelligence Strategy outlines four strategic goals and multiple objectives under those goals. Germane to this monograph is Strategic Objective 1.3, "Facilitate Homeland Defense through all-domain (maritime, air, space, land, and cyber) awareness, integration and collaboration with national, homeland defense, law enforcement and international partners." [54] Three priorities specify how to achieve this objective; promote cooperation with national state, local, tribal and international entities to provide timely intelligence products and services in support of homeland defense. Encourage and promote robust cyber countermeasures and awareness across the defense infrastructure. Improve counterintelligence support to computer network operations to facilitate efforts to anticipate, detect, trace, attribute, and counter efforts to exploit and attack US government information systems.[55]

---

[51] Department of Defense, *Defense Intelligence Strategy*, 2008, i

[52] Ibid, ii

[53] Ibid, ii

[54] Ibid, 12

[55] Ibid,12

The necessity of effective information flow for the Department of Homeland Security (DHS) is outlined in its mission statement. "…prevent and protect against terrorist attacks; respond to both man-made and natural disasters; perform the law enforcement and other crucial functions of the Department's component agencies; and play a central role in augmenting the Nation's ability to gather, analyze and disseminate information and intelligence."[56] To achieve dissemination, the DHS must "…foster information sharing, consistent with law, regulation and policy, in each of the following ways: i) internally within DHS, ii) horizontally within the US government between both law enforcement agencies and the intelligence community, iii) vertically with State, local, territorial, tribal and private sector partners, and iv) horizontally with the law enforcement and intelligence agencies of foreign allies and appropriate international institutions."[57]

The understanding that there is no longer a dividing line at the national border separating responsibility for security transcends party affiliation and the policies of the administration. In Presidential Study Directive 1, President Obama outlined this idea for his National Security staff, "…Homeland Security is indistinguishable from National Security—conceptually and functionally, they should be thought of together rather than separately."[58] The President went on to reiterate the necessity for information sharing and a trans-border architecture, "…In assessing and proposing structural reforms, this review shall consider…how to strengthen interagency coordination…within a cohesive and integrated structure…and how to ensure seamless integration between international and domestic efforts to combat transnational threats"[59]

---

[56] Department of Homeland Security, *Department of Homeland Security Information Sharing Strategy*, 2008, 2

[57] Ibid, 2

[58] The White House, Presidential Study Directive-1, 23 FEB 2009, 1-2

[59] Ibid,2

IV. NATIONAL GUARD SUPPORT TO NATIONAL INTELLIGENCE

To be of operational use, intelligence must be timely, accurate, usable, complete, relevant, objective, available, and disseminated to those decision-makers and interagency operators who need it for successful HD and CS operations.[60] Intelligence assessments help the commander determine the magnitude of the threat, which forces to deploy, the most efficient manner in which to deploy those forces, and probable enemy reactions.[61] Building upon the history of regulation and the necessity of intelligence support to HD and CS, an enumeration of the joint intelligence process and evaluation of National Guard capabilities within each process will inform the way ahead.

The joint intelligence process consists of six categories of intelligence operations; planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. Intelligence planning and direction is most effective when it happens well ahead of the possible crisis. The most likely threat scenarios are used as the core of the planning effort and the intelligence planner identifies the gaps in information regarding the potential adversary and the operational environment. This helps formulate the requirements. The intelligence staff must also be aware of the intelligence and information requirements of higher, adjacent, subordinate, and supporting, and interagency elements. A request for information will lead to either a production requirement if the request can be answered with information on hand or a collection requirement if the request demands collection of new information. Collection planning and requirement management are major activities during planning and direction, matching requirements with collection capabilities. Finally, intelligence architecture planning requires early identification and integration of operational architectures, anticipated intelligence database access, production requirements, and dissemination requirements must be coordinated throughout the intelligence system.[62]

---

[60] Department of Defense, JP 3-27, *Homeland Defense*, 2007, VII-2

[61] Ibid, VII-2

[62] Department of Defense, Joint Publication 2.0, *Joint Intelligence*, 2007, I-8 – I-13

National Guard capabilities within intelligence planning are significant and potentially pose the greatest gain in efficiency for state fusion centers. Knowledge of the intelligence process and the capability to conduct detailed planning are skills that set the military apart from most of the interagency partners at the federal and state levels. The capability of identifying gaps in information, preparing a system of requirements and tasking the right assets to complete these requirements provides direction to the discipline. Important within planning is the establishment or adherence to specific standard reporting formats, database formats and establishment of routine reports for the push and pull of information throughout the system.

Collection includes those activities related to the acquisition of data required to satisfy the requirements specified in the collection plan. Collection operations management involves the direction, scheduling, and control of specific collection platforms, sensors, and HUMINT sources and alignment of processing, exploitation, and reporting resources with planned collection.[63] Due to restrictions already covered, National Guard forces cannot collect on US persons. Collection can be completed on other gaps in information; infrastructure, demographics, trends that inform effects of specific natural disasters to name a few.

During processing and exploitation, raw collected data is converted into forms that can be readily used by decision-makers at all levels, intelligence analysts and other consumers. Processing and exploitation includes imagery exploitation, data conversion and correlation, document translation, and signal decryption, as well as reporting the results of these actions to analysis and production elements.[64] National Guard assets to conduct this are extremely limited, and fall outside the scope of allowed actions by regulation.

During the analysis and production phase, all available processed information is integrated, evaluated, analyzed, and interpreted to create products that will fill gaps in information or requests for

---

[63] Ibid, I-14

information from other agencies. Analysis and production is done primarily by all-source analysts that fuse together information from all intelligence disciplines.[65] National Guard assets have analysis elements that are trained in completion of this task, and have conducted this task during deployments in support of the Global War on Terror over the past 8 years, as well as support to counterdrug initiatives since 1991.[66] The paradigm used within counterdrug support serves well as the most likely scenario for routine analyst use in steady support to civil authorities; "The National Guard does not conduct Intelligence activities of its own in counterdrug support program missions. National Guard members support the criminal information analysis activities of LEAs. Criminal information comes into temporary possession of National Guard members supporting LEAs but is not retained by the National Guard."[67]

The dissemination and integration process is facilitated by a variety of means; written, verbal, in database format or as a briefing to name a few. The needs of the customer, the criticality of the intelligence, and capability to access determines the means of presentation. The diversity of dissemination paths reinforces the need for communications and computer systems interoperability among DOD organizations, and the interagency community. Intelligence organizations must initiate and maintain close contact with users to ensure that the product has been received and meets their requirements. If they fail to do this, all other aspects of the intelligence effort are rendered meaningless. After intelligence products are delivered, intelligence personnel and organizations are responsible for continuing to support users as they integrate the intelligence into their decision-making and planning processes. Rather than being the end of a process, the integration of intelligence is a continuous dialogue between the user and the producer. How or even whether intelligence is used is ultimately up to the user. The role of the producer

---

[64] Ibid. I-14

[65] Ibid. I-15

[66] National Guard Regulation 500-2, National Guard Counterdrug Support, 2008,1

[67] Ibid, 11

is to ensure that the user has the best intelligence possible for decision-making.[68] National Guard capabilities, due to connectivity through DoD network access provide a dissemination and communications bridge between state/local authorities and DoD agencies. While not tasked directly, National Guard forces have the capability to serve as a liaison between DoD agencies and state/local agencies to ensure that the needs of both customers are met.

Evaluation and feedback are continuously performed during each portion of the intelligence process. Intelligence planners, collectors, analysts, and disseminators coordinate and cooperate to determine if any of the various intelligence operations require improvements. Individual intelligence operators aggressively seek to improve their own performance and the performance of the activities in which they participate.[69] National Guard capabilities, due to connectivity through NIPR and SIPR access provide a dissemination and communications bridge between state/local authorities and DoD agencies. National Guard forces have the capability to serve as a liaison between DoD agencies and state/local agencies to ensure that the needs of both customers are met.

Because of the standardization of intelligence training within the Army, the experience of tactical intelligence operations throughout the force due to deployments in support of the Global War on Terror, and experiences supporting civil authorities in steady state operations such as counterdrug operations as well as natural disaster support at the local level, National Guard intelligence capabilities can provide augmentation and liaison to state and local agencies as well as serve the needs of the DoD for local intelligence support. The greatest capabilities, due to regulation, training, and experience are in the planning, dissemination, and evaluation aspects of the intelligence process. An examination of the state and local intelligence fusion centers will provide an assessment of current gaps within the intelligence process at the local level.

---

[68] Department of Defense, Joint Publication 2.0, Joint Intelligence, 2007, I-19 – I-20

[69] Ibid, I-20

V. THE EMERGENCE OF INTELLIGENCE FUSION CENTERS

A fusion center is defined as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[70] Among the primary focuses of fusion centers are the intelligence and fusion processes, through which information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information (e.g., risk assessments and suspicious activity reports) that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity. It is recommended that the fusion of public safety and private sector information with law enforcement data be electronic through networking and utilizing a search function. Examples of the types of information incorporated into these processes are threat assessments and information related to public safety, law enforcement, public health, social services, and public works. The ultimate goal is to provide a mechanism through which government, law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources. Horizontal and vertical communication is critical for a fusion center to be effective.[71]

In the aftermath of 9/11, and based upon recommendations made by the 9/11 Commission previously stated in this monograph, the federal government began working with state and local officials to find a way to assist with their information-sharing efforts, primarily through the development of policy and guidelines, and later with financial support. In December 2004, the Department of Homeland Security called upon every state to establish at least one fusion center and urged additional centers for large urban

[70] US Department of Justice, *Fusion Center Guidelines, Executive Summary*, 2006, 2

areas and interstate regions with common interests. DHS promised the state Homeland Security Advisors that it would provide "current and actionable and unclassified information" that can be immediately disseminated to local law enforcement.[72] DHS chose not to expand the legal definition of the Federal Intelligence Community to include state, tribal, and local entities, which would have imposed considerable costs on tribal, state, and local jurisdictions.[73] Training, monitoring compliance, and congressional oversight, provision of secure infrastructure, security clearances and secure communications are the major costs associated with inclusion into the intelligence community.[74]

Instead, the DHS has invested in establishment of the Homeland Security Information Network (HSIN), a web based platform at the Sensitive but Unclassified level of clearance. The HSIN was created to interface with existing unclassified systems and is focused on vertical and horizontal collaboration within four major areas; Intelligence and Analysis, Law Enforcement, Emergency Management, and Critical Sectors. A major byproduct of the HSIN infrastructure is real-time interaction between States and the National Operations Center, with the goal of gaining situational awareness and establishing a common operating picture.[75]

The Department of Justice (DOJ) in coordination with the Global Justice Information Sharing Initiative and the Criminal Intelligence Coordinating Council (CICC), a DOJ-sponsored group whose members include the Major City Chiefs, International Association of Chiefs of Police, Major County Sheriffs and many other law enforcement and public safety organizations, undertook the challenge of creating the *Fusion Center Guidelines*. These guidelines, which complement the President's *National Strategy for Information Sharing*, were an important first in many steps in formalizing the federal

---

[71] Ibid. 2-4

[72] Homeland Security Advisory Council, "*Intelligence and Information Sharing Initiative-Final Report*, December 2004", 1

[73] Ibid.

[74] This is covered in Executive Order 12333 on national intelligence activities.

government's relationship with state and local fusion centers. The guidelines also served as a roadmap for the Department of Homeland Security which used these guidelines when determining their involvement in the fusion centers.

In addition, fusion centers are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan* (NCISP). The NCISP is the blueprint for law enforcement administrators to follow when enhancing or building an intelligence function, and focuses on establishment of a mechanism to promote intelligence-led policing, intelligence training, technology architecture to provide secure and seamless sharing of information, one that also leverages existing systems and networks while allowing the flexibility for upgrades. It also provides an outreach plan to promote timely and credible intelligence sharing, a model for intelligence process principles and policies, while respecting and protecting an individual's privacy and civil rights.[76] It embraces intelligence-led policing, community policing, and collaboration and serves as the foundation for the *Fusion Center Guidelines.*[77] But, as pointed out in the CRS report to Congress, the Guidelines have the following limitations; they are voluntary, the philosophy outlined in them is generic and does not translate theory into practice, and they are oriented toward the mechanics of fusion center establishment,[78] not in the establishment of a common understanding of intelligence.

Ideally, the fusion center involves every level and discipline of government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. The intent of the founders of the fusion center process states that a fusion center should be organized and coordinated, at a minimum, on a statewide level, and each state should establish and maintain a center to facilitate the fusion process. Though the foundation of fusion centers is the law

---

[75] Department of Homeland Security website, (HSIN); accessed at http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm ; internet;on February19, 2009.

[76] US Department of Justice, *National Criminal Intelligence Sharing Plan*, June 2005, 2

[77]US Department of Justice, *Fusion Center Guidelines, Executive Summary*, 2006, 3

[78] CRS Report for Congress, *Fusion Centers: Issues and Options for Congress*, 2007, 10

enforcement intelligence component, each individual fusion center and customer base is tasked to evaluate their respective jurisdictions to determine what public safety and private sector entities should participate in their fusion center.

Intelligence fusion centers are not under the direct control of the federal government and were formed based upon local conditions. According to a CRS report to Congress, fusion centers are state-created entities largely financed and staffed by the states, and there is no one "model" for how a center should be structured. State and local law enforcement and criminal intelligence seem to be at the core of many of the centers. Although many of the centers initially had purely counterterrorism goals, for numerous reasons, they have increasingly gravitated toward an all-crimes and even broader all-hazards approach. While many of the centers have prevention of attacks as a high priority, little "true fusion," or analysis of disparate data sources, identification of intelligence gaps, and pro-active collection of intelligence against those gaps which could contribute to prevention has been occurring. Some centers are collocated with local offices of federal entities, yet in the absence of a functioning intelligence cycle process, collocation alone does not constitute fusion.[79] Additionally, because the intelligence fusion centers are responsive and responsible to local leadership more than to any federal entity, a lack of standards for reporting and products exists. A potential way to get around this issue is through federal liaison and augmentation with state and local fusion centers.

The federal government resource augmentation for fusion centers has come primarily from two agencies, the Federal Bureau of Investigation (FBI) and the DHS. The FBI has provided support to the fusion center effort by co-locating staff in the fusion centers, facilitating the security clearance process and assisting in rent payments in joint occupancy fusion centers.[80] As an example of the support and the growing importance of fusion centers, the DHS, in addition to providing direct support in the form of grant dollars, is committing to putting a DHS analyst in all state and local fusion centers. Participation in

[79] Ibid, 2

the fusion center process assists local government policy makers and those responsible for the protection of the community with not only pertinent intelligence with a local application; it provides an opportunity to develop networks and relationships that will be critical in any future catastrophic event. The placement of an analyst in the local fusion centers will also assist in the quality of reporting and products emanating from the fusion centers.

This, though helpful, will not be enough to change the differences in philosophy and lexicon between the intelligence community's definition of intelligence and law enforcement's definition. David Carter, a criminal intelligence expert states, "In the purest sense, intelligence is the product of an analytic process that evaluates information collected from diverse sources, integrates the relevant information into a cohesive package, and produces a conclusion or estimate about a criminal phenomenon by using the scientific approach to problem solving (i.e., analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy direction to law enforcement decision-makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.[81]

Law enforcement intelligence (LEINT) is thus "the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality."[82] Being product focused, this definition demonstrates the LEINT process as linear versus the cyclical, continuous, process followed by the intelligence community. Inherent in the definition of the intelligence process is continuous communication and feedback that permeates the process as the intelligence producer and consumer through the dialogue of the system; requests for information, collection requirements, standardized products and schedules. This vertical and horizontal dialogue provides the framework for a networked communication methodology that is currently missing within the DHS, and by extension the fusion centers. From the 2008 Department of

---

[80] Ibid, 38

[81] David L. Carter, *Law Enforcement Intelligence: A guide for State, Local, and Tribal Law Enforcement Agencies*,2004, 7

Homeland Security Information Strategy a core mission of DHS, "1. Fostering information sharing is a core DHS mission… 2. DHS must use the established governance structure to make decisions regarding information sharing issues…3. DHS must commit sufficient resources to information sharing… 4. DHS must measure progress toward information sharing goals…5. DHS must maintain information and data security and protect privacy and civil liberties."[83] A main challenge that DHS identifies are the barriers to information sharing between the law enforcement and intelligence community. Lack of trust stems from fears that shared information will not be protected adequately or used appropriately horizontally or vertically, between law enforcement and the intelligence community at the federal level, and at the local level as well. "For example, law enforcement and the intelligence community are concerned that competing information uses will compromise ongoing investigations, sources and methods. State, local, territorial, tribal and private sector partners are willing to share information with the federal government, but want assurances that information held at the Federal level will be shared adequately with them."[84]

As one of its challenges, DHS has enumerated one of the fundamental principles of the intelligence process; dissemination. "The Department must ensure(s) the right information gets to the right people at the right time. The need for an information sharing environment to encompass and address these complexities has slowed the process of developing information sharing protocols at the policy level even more than at the technological level."[85]

This shows that the conceptual challenges are the largest ones that face DHS and their system of fusion centers. The DHS Lessons Learned Information Sharing network solicited feedback from subject matter experts from across the country. The shortfalls can be broken into three categories; a lack of higher

---

[82] Ibid,10

[83] Department of Homeland Security, *Information Sharing Strategy*, 2008, 5

[84] Ibid, 5-6

[85] Ibid, 6

level guidance on organizing and providing a local framework of intelligence structures and networks. Two-way tasking and requirements and capabilities guidance; a lack of specific points of contact at the federal government to send specific intelligence requests for information and an associated lack of understanding of the Federal Intelligence Community and products available to them. Also, a lack of a standardized training program for analysts reduces the capacity for standardization of products within the network.[86]

VI. NATIONAL GUARD SUPPORT TO STATE FUSION CENTERS

Exploration of National Guard capabilities to support State Intelligence Fusion Centers, and by extension the DHS will focus on three areas: National Guard Counter Drug program, the recently created Weapons of Mass Destruction – Civil Support Teams (WMD-CST) and the emerging State Joint Force Headquarters structures. Each are covered in a separate National Guard Regulation, dealing with National Guard support to Civil Authorities. Important to note is that at the State level, there is a requirement to gain situational awareness, and communicate a common operating picture to the National Guard Bureau. Because maintenance of a common operating picture is an already tasked requirement, resources are available to accomplish this requirement, and coordination and collaboration with the state fusion centers is necessary.

THE NATIONAL GUARD COUNTERDRUG PROGRAM

Using the National Guard Counterdrug program as a paradigm of support for intelligence fusion centers would provide an immediate group of ready and relevantly trained analysts. These analysts are capable of following the processes and procedures of the intelligence community, have direct ties to Department of Defense databases as well as a high probability for deployment experiences. Because of their additional ties to the state or location of the fusion center, they would be knowledgeable of local

---

[86] Department of Homeland Security website, (LLIS); accessed at https://www.llis.dhs.gov/index.doc, internet, on February,19, 2009

conditions, and could serve as an efficient intermediary between the local and intelligence community organizational cultures.

In 1989, Congress created the National Guard Counterdrug Support Program in the National Defense Authorization Act and directed the National Guard to provide counterdrug support to local, state, and federal law enforcement agencies. The National Guard provides counterdrug support in two major areas: assisting law enforcement to stop the flow of drugs and assisting community based organizations to reduce the demand for drugs. Intelligence analyst support is one of eighteen missions authorized by the Secretary of Defense for the National Guard Counterdrug Support Program. Intelligence personnel are tasked to "…receive and process incoming reports from multiple sources in accordance with established LEA procedures. They would assist in evaluating the information, analyzing trafficking group composition, disposition, strengths, and weaknesses. They can also help evaluate current intelligence holdings and identify intelligence gaps and additional requirements."[87] Under NGR 500-2, the National Guard does not conduct Intelligence activities of its own in Counterdrug Support Program missions. National Guard members support the criminal information analysis activities of Law Enforcement Agencies. Information on US Persons comes into temporary possession of National Guard members supporting LEAs but is not retained by the National Guard. Intelligence oversight training is included in doctrinal training given to each member at initial entry, and repeated annually for all personnel. Specialized training as covered by regulations pertaining to care and handling of information on US Persons by members performing linguist support, investigative case and analyst support, and aerial reconnaissance is handled individually.[88] Thus, there already exists a core group within each state that has accomplished an intelligence support to civil authority mission for almost two decades.

---

[87] Joint Chiefs of Staff, JP 3-07.4 *Joint Counterdrug Operations*, 2007, III-24-25

[88] National Guard Bureau, NGR 500-2, *National Guard Counter Drug Support*, 2008, 11

There are three additional characteristics of National Guard counterdrug intelligence personnel that provide a ready force in support of state fusion centers; a mature and stable force, a locally focused and responsive, and well trained in Department of Defense Intelligence Doctrine. Because of the nature of National Guard Soldiers, there is little turnover within the system; Soldiers typically stay in the same state they start out in. This has the effect of sustaining institutional memory. Typically, they also are residents from birth of the state they serve in, and thus have a better grasp of local conditions, paradigms and policies that would shape the intelligence fusion centers from their local area. Finally, and balancing the previous two characteristics is the understanding that these Soldiers have completed individual intelligence training. Dependent upon level of training completed, they have received an institutional education on the intelligence system as practiced by the federal intelligence community, and thus have an understanding of the process and procedures that provide a framework for institutional and systemic success. These analysts also continue to be part of an organized unit, and receive periodic individual and collective training on the newest intelligence tactics techniques and procedures, as well as being subject to deployments with their units, and thus exposed to deployed combat intelligence missions, and intelligence products created at the operational and strategic level.

The counterdrug program currently, but indirectly, supports current domestic counter terror operations due to the link between drug trafficking and terrorism in the United States. This link has become more evident in recent years and is demonstrated in two different ways. First, terrorists can enter the country using the same routes used by criminals to smuggle drugs and weapons.[89] While conducting normal duties analyzing intelligence for drug investigations, National Guard counterdrug personnel are apt to run across information containing suspicious activities that may involve terrorists. Thus, it should not be either National Guard Support to counterdrug operations or support to state intelligence fusion

[89] National Guard Bureau, *Counterdrug Link to Homeland Security*, 1

centers, but should be in addition to the current system, using the counterdrug as a paradigmatic point of departure for fusion center augmentation.

NATIONAL GUARD WMD-CST

The Weapons of Mass Destruction - Civil Support Teams (WMD-CST) are National Guard units designed to provide a specialized capability to respond to a Chemical, Biological, Radiological, Nuclear, or Explosive (CBRNE) incident primarily in a Title 32 operational status within the United States and its territories. It is tasked to support the civil authorities by providing a disciplined, well trained, and well equipped organization to supplement local, state, and federal efforts to manage the potentially catastrophic effects of terrorism, or provide special technical support to augment specific needs of the Incident Commander. They are designed and trained to provide initial assessment of CBRNE events and advice and assistance to the Incident Commander, State Emergency Management, the State's Joint Forces Headquarters (JFHQ-State), the Adjutant General (AG), the Governor, and other key officials, including representatives of federal agencies.[90] They are tasked with gaining and maintaining the interagency relationships that are necessary for incident response, communicating with the same agencies that make up the state fusion centers. As such, while pre-incident intelligence activities are not part of their force structure or their mandate, and while they are most capable of providing incident response, the WMD-CST's have three main areas that would allow them to provide effective control over intelligence analysts assigned to state fusion centers. WMD-CST's are tasked with providing incident support to the same population as the state fusion centers, thus they are in need of the same information that the fusion centers produce. The WMD-CST's are tasked with being on the front lines of response from DoD, yet fall under the National Guard Bureau (NGB) and their States (Title 32) for their daily activities, hence *Posse Comitatus* restrictions do not apply to them. They are required to be on ready alert and are tasked with incident response, thus they need responsive intelligence, and have an interest in preparing standardized

anticipatory intelligence and data sharing across state boundaries, which would lead to a network of information across the country, and linkage to USNORTHCOM as well as NGB. Necessary to achieving this would be intelligence augmentation to the team outside their current deployable table of organization, and adjustment of authorization that changes their orientation from purely incident response to addressing augmentation of the local intelligence framework. A positive aspect of the addition of an intelligence section for DoD, and the elegance for each state that has a WMD-CST as part of their force structure , is the funding by DoD for this element. States will not have to take analysts out of hide to accomplish this domestic intelligence task.

STATE JOINT FORCES HEADQUARTERS

Per NGR 500-1, National Guard Domestic Operations fall into three mission areas: Homeland Defense, National Guard Civil Support, and National Guard Baseline Operating Posture. Homeland defense, for which DoD serves as the primary federal agency and military forces are used to conduct military operations in defense of the Homeland. Under National Guard Civil Support the National Guard normally serves in a supporting role to other primary state or federal agencies by providing assistance to US civil authorities at the federal, state, tribal, and local levels. The conduct of required planning, training, and exercises, as well as some ongoing mandated domestic operations outlines the National Guard Baseline Operating Posture.[91] The general focus of the National Guard Baseline Operating Posture is to maintain readiness and situational awareness to conduct all assigned missions in both its state and federal roles. The intent is to assist in deterring and preventing attacks on the US Homeland, maintain situational awareness and detect threats or concerns and conduct mandated ongoing domestic operations e.g., counterdrug operations.[92] Implied within this definition of baseline operating posture is a necessity

---

[90] National Guard Bureau, NGR 500-3, 2006, 1

[91] National Guard Bureau, NGR 500-1, 2008, 5

[92] Ibid, 6

to maintain some degree of intelligence preparation of the domestic operational environment; a traditional task of intelligence.

At the State level, the Joint Forces Headquarters (JFHQ-State) provide command and control of National Guard forces for the Governor. The JFHQ-State is also responsible for providing situational awareness/common operating picture information to the NGB and other national level headquarters before and during selected domestic operations and for providing joint reception, staging, onward movement, and integration (JRSOI) of all inbound forces during a national emergency or disaster response.[93]

Thus, an argument can be made that close coordination or collaboration to create and maintain common operating picture between JFHQ-State and the various state intelligence fusion centers is imperative. To accomplish this at the JFHQ-State could use similar assets used by either the WMD-CST or counter drug augmentation initiatives. The customer base would be the same in all three cases. The difference would be the reporting chain, and additional supporting tasks in case of an incident, the status and force structure of these assets; either within the WMD-CST, or assigned to each state's JFHQ.

VII. CONCLUSION

The National Guard played a significant civil support role before 9/11 in responding to state emergencies, WMD incidents, and supporting LEAs in drug control efforts. After 9/11, Congress, DoD and the National Guard have leveraged and augmented the state emergency and WMD capabilities in order to provide an enhanced response to terrorist attacks. USNORTHCOM and NGB partner to conduct training and exercises for each state Joint Force Headquarters Joint Task Force commanders and staffs. NORTHCOM and NGB action officers coordinate daily on deliberate and crisis action planning

[93] Ibid, 7

requirements.[94] The necessity to gain situational awareness and maintain a common domestic operating picture demonstrates a need for intelligence preparation of the operational environment. To accomplish this requirement would either require the establishment of robust intelligence sections at the state Joint Forces Headquarters level, with an equally robust oversight system, or a capability to integrate or liaise with established state fusion centers and other state agencies that can assist with providing the information to maintain situational awareness. Either way, this is a task that has been specified by the National Guard Bureau to the state JFHQs. With the specification of this requirement needs to come resources to accomplish it; either through the provision of funding to create domestic J2 sections (with required oversight) or the quantification and codification of a relationship between local fusion centers and each of the state JFHQs. Clarifying this relationship is the task of the National Guard Bureau because it will necessitate provision of forces as well as a potential for changes in federal law, much like the establishment of the counterdrug program. Integration of these assets into the state fusion centers would provide both the DoD and DHS with economies far above their cost; the efficiency of a common lexicon between the National Guard intelligence assets and DoD which would then be passed to the fusion centers. The efficiencies of a directly responsive set of collectors (with the understanding they are not reporting on US persons) in all 50 states, capable of providing specific information to DoD to meet the needs of the federal intelligence consumer; either policy makers, intelligence analysts, or USNORTHCOM elements. They also can be responsive to their local fusion centers, providing an efficient conduit to Department of Defense databases and providing information to local decision makers and analysts. This would have to be tempered with disclosure training, and would be another oversight issue that would have to be funded by DoD via NGB.

An area for further research is an exploration of the increased domestic operations requirements balanced against the increased utilization of National Guard assets deployed overseas. The National

---

[94] US Congress, Statement of GEN Renuart, CDR USNORTHCOM to House Armed Services Committee, 18 MAR 2009, 15

Guard performs a dual-role of supporting civilian authorities domestically and acting as a reserve for the Active Army and Air Force during periods of conflict. As has been addressed by other authors within the past few years, the reserve components are much more an operational reserve now versus their traditional role as a strategic reserve.[95] A balance between the expeditionary (outside of the NORTHCOM AOR) and homeland security/ homeland defense missions needs to be determined. This is especially important as the potential for employment in support of missions along the US-Mexico border are evaluated.[96]

Another area for further research is standardization of reporting across the interagency within and outside the intelligence community and between the federal and state levels. While National Guard intelligence personnel can serve to provide information between the intelligence community and state/ local fusion centers, the standardization of data moving between these levels and between agencies at the federal level could provide the most efficient and effective increase in domestic intelligence capability. The capabilities to utilize a conceptual system that has been proven to work across the spectrum of operations needs to be adopted by all stakeholders as the standard. The technology exists for networked coordination, true fusion of information, and effective dissemination that balances security and privacy concerns with provision of the right intelligence to the right customer. Utilization of National Guard intelligence professionals to facilitate this process and serve as a bridge between state agencies and the federal intelligence community is a solution to this issue until such time as the Department of Homeland

---

[95] Commission on the National Guard and Reserves, Strengthening America's Defenses in the New Security Environment, Second Report to Congress, March 2007, x

[96] From a statement by Roger Rufe, Director of the Office of Operations Coordination and Planning, US DHS before the Committee on Homeland Security, Subcommittee on Border, Maritime and Global Counterterrorism: "Requests for DOD capabilities to support the interagency response are nested in the well-established existing Federal request for assistance process (utilizing Title 10 and Title 32 forces when approved by the Secretary of Defense) and internal State emergency management procedures (National Guard in State Active Duty or Title 32 status). DOD support would be requested only if DHS Components are overwhelmed or do not have the resident capabilities to fulfill the mission. Areas of potential DOD support include [Southwest Border-InteragencyTask Force] staffing, where DOD planning expertise can be used, as well as other military-unique capabilities, executed either by the National Guard in State Active Duty or Title 32 status) or by Title 10 DOD forces. In accordance with section 377 of Title 10, U.S. Code, such support would be provided by DOD on a reimbursable basis." US Congress, House Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism, 12 March 2009, 4

Security and the state fusion centers share a common lexicon, have a home-grown intelligence analysis capacity that is responsive to the DoD (because of its homeland defense mission) and to the intelligence community (because of its requirement to conduct trans-national intelligence fusion). All of this has to be balanced with upholding privacy considerations, and responsiveness to local conditions while following state and federal law. This is of particular importance as we face the potential for increased numbers of National Guard Soldiers and Airmen deployed in support of border security missions along our southern border. Their need for timely, accurate, usable, complete, relevant, and objective intelligence is no less than a Soldier deployed to Iraq or Afghanistan.

BIBLIOGRAPHY

BOOKS

Doubler, Michael D. *The National Guard and the War on Terror:Operation Enduring Freedom and Defense Transformation*. Washington, D.C. National Guard Bureau Historical Services Division, 2008

Gutjar, Melanie. *The Intelligence Archipelago, The Community's struggle to reform in the Globalized Era*, Washington D.C., Joint Military Intelligence College Press, 2005.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy. 4th ed*. Washington, D.C. CQ Press, 2009

Posner, Richard A. *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*. Lanham, MD: Rowman and Littlefield Publishers, 2005

_____. *Uncertain Shield: The US Intelligence System in the Throes of Reform*. Lanham, MD: Rowman and Littlefield Publishers, 2005

Richelson, Jeffrey T. *The Intelligence Community,5th ed*, Philadelphia, PA: Westview Press, 2008

Turabian, Kate L. *A Manual for Writers of Research Papers, Theses, and Dissertations*. 7th ed. Chicago: University of Chicago Press, 2007.

GOVERNMENT PUBLICATIONS

Department of the Army, *Intelligence Oversight Guide*, June 2007

_____. Army Regulation 381-10, *US Army Intelligence Activities*, Washington, DC: Government Printing Office, 1 July 1984

_____. *Domestic Operations Law Handbook for Judge Advocates*, Charlotte WV: Center for Law and Military Operations, 2006

Department of Defense, *Defense Intelligence Strategy*, Washington, DC: Government Printing Office, 2008

_____. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* , Washington, DC: Government Printing Office, 23 March 1994

_____. Joint Publication 2-0, *Joint Intelligence*, Washington, DC: Government Printing Office, 22 June 2007

_____. Joint Publication 3-07.4 *Joint Counterdrug Operations*, Washington, DC: Government Printing Office, 2007

_____. Joint Publication 3-27, *Homeland Defense,* Washington, DC: Government Printing Office, 2007,

_____. Joint Publication 3-28, *Civil Support*, Washington, DC: Government Printing Office, 2007

Department of Homeland Security, *Department of Homeland Security Information Sharing Strategy*, Washington, DC: Government Printing Office, 2008

Department of Justice, *National Criminal Intelligence Sharing Plan*, Washington, DC: Government Printing Office, June 2005

_____. *Fusion Center Guidelines, Executive Summary*, Washington, DC: Government Printing Office, 2006

National Guard Bureau, NGR 500-1, *National Guard Domestic Operations*, Washington, DC: Government Printing Office, 2008

_____. NGR 500-2, *National Guard Counter Drug Support*, Washington, DC: Government Printing Office, 2008

_____. NGR 500-3, *National Guard Civil Support Teams*, Washington, DC: Government Printing Office,2006

_____. *Counterdrug Link to Homeland Security*, Washington, DC: Government Printing Office, 2007

Office of the Director in National Intelligence, *National Intelligence Strategy*, Washington, DC: Government Printing Office, Oct 2005

US Congress, *USA PATRIOT Act*, Washington, DC: Government Printing Office, 2001

_____. PL 108–458, *Intelligence Reform and Terrorist Prevention Act of 2004*, Washington, DC: Government Printing Office, 2004

_____. Statement of Roger Rufe, Director of the Office of Operations, Coordination and Planning, Department of Homeland Security, before the House Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism, Washington DC: Government Printing Office, 12 March 2009

_____. Statement of GEN Renuart, CDR USNORTHCOM to House Armed Services Committee, Washington DC, Government Printing Office,18 March 2009

US President (Bush), Executive Order 13353, Establishing the President's Board on Safeguarding Americans' Civil Liberties, Washington, DC: Government Printing Office ,27 August 2004

_____. Executive Order 13354, National Counterterrorism Center, Washington, DC: Government Printing Office , 27 August 2004

_____. Executive Order 13355, Strengthened Management of the Intelligence Community, Washington, DC: Government Printing Office , 27 August 2004

_____. Executive Order 13356, Strengthening the Sharing of Terrorism Information to Protect Americans, Washington, DC: Government Printing Office ,27 August 2004

_____. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, Washington, DC: Government Printing Office ,October 2005

_____. *The Department of Homeland Security*, Washington, DC: Government Printing Office June 2002

_____. *National Strategy for Information Sharing*, Washington, DC: Government Printing Office October 2007

US President (Obama), Presidential Study Directive-1, Washington, DC: Government Printing Office, 23 February 2009

OTHER PUBLICATIONS

Commission on the National Guard and Reserves, Strengthening America's Defenses in the New Security Environment, Second Report to Congress, Washington, DC: Government Printing Office , March 2007

CRS Report for Congress, *The Growth of Domestic Intelligence*, Washington D.C.: Congressional Research Service, 1976

_____. *Fusion Centers: Issues and Options for Congress*, Washington, D.C.: Congressional Research Service, 2007

Homeland Security Advisory Council, *Intelligence and Information Sharing Initiative: Final Report – December 2004*, Washington, DC: Government Printing Office, 2005

The 9/11 Commission. "Final Report of the National Commission on Terrorist Attacks Upon the United States" W.W. Norton & Company, Inc., April 2005.

INTERNET SITES

Carter, David L. *Law Enforcement Intelligence: A guide for State, Local, and Tribal Law Enforcement Agencies*, accessed from US Department of Justice Community Oriented Policing website: http://www.cops.usdoj.gov/, internet: on February, 18, 2009

Department of Homeland Security website, (HSIN); accessed at http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm ; internet; on February 19, 2009.

Department of Homeland Security website, (LLIS); accessed at https://www.llis.dhs.gov/index.doc, internet, on February 19, 2009.

United States NORTHCOM website (on-line); accessed at http://www.northcom.mil/About/index.html ; internet; on January 2, 2009.