NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FUSING INTELLIGENCE WITH LAW ENFORCEMENT INFORMATION: AN ANALYTIC IMPERATIVE

by

Christopher C. Thornlow

March 2005

Thesis Advisor:	Robert L. Simeral
Second Reader:	Steven B. Ashby

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Fusing Intelligence with Law Enforcement Information: An Analytic Imperative			**5. FUNDING NUMBERS**
6. AUTHOR(S) LCDR Christopher C. Thornlow, USN			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The tragedy of 11 September 2001 revealed two major shortcomings: the US military and the Department of Defense's inability to respond quickly to and defend against the threat posed by foreign terrorists to the United States, and the inability of the Intelligence and Law Enforcement Communities to fuse and analyze foreign threat intelligence with domestic law enforcement information in a timely fashion to provide adequate indications and warning of such an attack. The United States Northern Command Intelligence Directorate (J2) has the primary mission in providing accurate, timely, and relevant indications and warnings of potential threats to the Commander, USNORTHCOM. The USNORTHCOM J2 must be able to use all intelligence sources, including law enforcement information, to better understand the potential threats and capabilities arrayed against it. This enables the USNORTHCOM J2 to provide the Commander, USNORTHCOM an all-source, fused analytic assessment of potential threats as the command carries out its mission to "deter, prevent, and defeat threats and aggression aimed at the United States," and thus fulfilling the command's role as the Department of Defense's primary lead command in homeland defense and homeland security.

14. SUBJECT TERMS Intelligence, Law Enforcement; PATRIOT Act; September 11; 9/11; Terrorism; Terrorists; Homeland Security; Homeland Defense; Counterterrorism			**15. NUMBER OF PAGES** 73
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FUSING INTELLIGENCE WITH LAW ENFORCEMENT INFORMATION: AN ANALYTIC IMPERATIVE

Christopher C. Thornlow
Lieutenant Commander, United States Navy
M.P.A, Troy State University, 1993
B.S., Jacksonville University, 1985

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2005

Author: Christopher C. Thornlow

Approved by: Robert L. Simeral, CAPT, USN (Ret)
Thesis Advisor

Steven B. Ashby, CAPT, USN
Second Reader/Co-Advisor

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The tragedy of 11 September 2001 revealed two major shortcomings: the US military and the Department of Defense's inability to respond quickly to and defend against the threat posed by foreign terrorists to the United States, and the inability of the Intelligence and Law Enforcement Communities to fuse and analyze foreign threat intelligence with domestic law enforcement information in a timely fashion to provide adequate indications and warning of such an attack. The United States Northern Command Intelligence Directorate (J2) has the primary mission in providing accurate, timely, and relevant indications and warnings of potential threats to the Commander, USNORTHCOM. The USNORTHCOM J2 must be able to use all intelligence sources, including law enforcement information, to better understand the potential threats and capabilities arrayed against it. This enables the USNORTHCOM J2 to provide the Commander, USNORTHCOM an all-source, fused analytic assessment of potential threats as the command carries out its mission to "deter, prevent, and defeat threats and aggression aimed at the United States," and thus fulfilling the command's role as the Department of Defense's primary lead command in homeland defense and homeland security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

A number of people and organizations are owed a debt of gratitude for allowing me to participate in this program and to complete this thesis. First are my classmates from both cohorts. The friendships and relationships that I have developed through this program will last me a lifetime. I have grown both professionally and personally over the last eighteen months and I thank each and every one of you.

I want to thank those within the U.S. Northern Command that made my participation possible, especially Mr. Michael Noll who provided me with a great recommendation securing my selection into the program. His insights and guidance on several important issues facing the Intelligence Community, U.S. Northern Command Intelligence, and Homeland Defense were invaluable to the formulation of this thesis.

The staff and professors within the Naval Postgraduate School's Center for Homeland Defense and Security need special recognition. Your hard work and dedication to the advancement of knowledge for homeland security and your assistance to us along the way during this process is truly admirable. I particularly would like to thank my advisor, Mr. Robert Simeral, and CAPT Steve Ashby for their guidance and assistance in the completion of the thesis research and development.

Lastly, I want to express my deepest appreciation to my family; I know it was difficult for me to be gone as much as I was to participate in this program, whether it was in Monterey or holed up in a library doing research. We have weathered some difficult times and I can only hope the best is yet to come.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. 9/11 AND ITS AFTERMATH

The tragedy of 11 September 2001 had a profound impact on the United States in many ways. Many books and articles have been written on these affects, including the deliberations and reports from national commissions to explore what went wrong, what level of impact the attack imparted on the U.S., and what the future might bring. Of the many reports, commentaries, books, and articles, the attack revealed two major shortcomings: the US military and the Department of Defense's inability to respond quickly to and defend against the threat posed by foreign terrorists to the United States, and the inability of the Intelligence and Law Enforcement Communities to fuse and analyze foreign threat intelligence with domestic law enforcement information in a timely fashion to provide adequate indications and warning of such an attack. The Department of Defense's response to the former was the creation of the United States Northern Command. The creation of this command provided a single Combatant Commander to have both a war fighting role against foreign threats to the homeland, as well as a role in support of civil affairs within the continental United States when called upon to do so. The response to the later has been many and varied, with the creation of several new intelligence entities, collaborations between existing intelligence and law enforcement agencies and organizations, and the creation of collaborative networks to facilitate the flow of information between the law enforcement and intelligence communities.

The creation of the US Northern Command brought with it the commensurate creation of its intelligence arm, the Intelligence Directorate. The US Northern Command (USNORTHCOM) Intelligence Directorate (J2) has the primary mission in providing accurate, timely, and relevant indications and warnings of potential threats to North America to the Commander, USNORTHCOM. In order to do this effectively, the USNORTHCOM J2 must be able to use all intelligence sources, including law enforcement information, to better understand the potential threats and capabilities arrayed against it. This enables the USNORTHCOM J2 to provide the Commander, USNORTHCOM an all-source, fused analytic assessment of potential threats as the command carries out its mission to "deter, prevent, and defeat threats and aggression

aimed at the United States," and thus fulfilling the command's role as the Department of Defense's lead command in homeland defense and homeland security.

One of the greatest difficulties faced by the USNORTHCOM J2 is access to and incorporation of law enforcement information into its analysis of potential threats to the USNORTHCOM area of responsibility (AOR) and the U.S. homeland. [1] The task of fusing intelligence data with law enforcement information would seem rather easy at first glance; however, there are several barriers (such as legal restrictions and cultural differences) that have developed over time that make this a more difficult and challenging task. The Intelligence Community traditionally focuses on foreign threats, outside of the United States. It collects information via a variety of means, both human and technical, and for the purposes of this paper is defined as "traditional intelligence." Intelligence analysts that work within the Department of Defense (DoD), including those in the USNORTHCOM J2, are familiar working with this type of intelligence information.

Law enforcement agencies (such as the Federal Bureau of Investigation (FBI), US Customs Service, as well as state and local police departments) also work with intelligence information, but this type of data is referred to as "law enforcement information." These agencies's primary focus is internal to the United States, trying to prevent and solve crimes occurring within our borders. Again, their information is obtained by a variety of means, both human and technical, but this information is not ordinarily classified similarly to that information obtained by the other elements of the Intelligence Community (noted above) and has legal restrictions that limit access by DoD intelligence analysts. Because of this, this type of intelligence information is defined as "non-traditional" intelligence since analysts outside of the law enforcement community do not routinely have access to or use this type of information.

The melding of all available information is defined as 'fusion analysis,' bringing together all sources of information, looking at each piece in concert with the other, and

1 The AOR 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, Puerto Rico and the U.S. Virgin Islands. The defense of Hawaii and the territories and possessions in the Pacific remain the responsibility of U.S. Pacific Command. For more information see the U.S. Northern Command Website at http://www.northcom.mil/index.cfm?fuseaction=s.who_homefront. [5 March 2005]

then developing one complete analytic picture by "fusing" these disparate pieces of data into one whole. The USNORTHCOM J2 must be able to use all intelligence sources, including law enforcement information, to better understand the potential threats and capabilities arrayed against the homeland. This understanding is essential in order to provide "timely, accurate and relevant" indications and warning to the Commander, USNORTHCOM.

B. OBJECTIVES

This thesis looks at the challenges faced by USNORTHCOM J2 counterterrorism analysts as they try to produce products that are "accurate, timely, and relevant," using all available information sources, including law enforcement information. The thesis has six chapters. Chapter I: "Introduction" describes the challenges created by the terrorist attacks of 9/11, and sets the stage for the discussion of the creation of the USNORTHCOM and its Intelligence Directorate, and defines the difference between national security intelligence and law enforcement information.

Chapter II: "'Separate but Equal' Communities" goes further to describe the national Intelligence Community and its major elements, and the elements of the Law Enforcement Community, focusing on the federal level of government. It then further elaborates on the distinction between intelligence information and law enforcement information. Areas of discussion will concentrate on cultural differences, cooperation and communication. In the *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001,* one of the major problems mentioned inherent in the Intelligence Community was that the FBI and CIA failed to cooperate effectively prior to the 9/11 attack which allowed al-Qa'ida operatives to move freely within the United States to plan and conduct their attack.[2] This dynamic between the Law Enforcement and the Intelligence Communities will be further explored.

Chapter III: "DoD, U.S. Northern Command, and the Northern Command Intelligence Directorate" goes into greater detail on the creation of USNORTHCOM, the

[2] U.S. Congress, Senate and House. Permanent/Select Committees on Intelligence. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 with additional views* (107th Cong., 2d sess., 2002), 45.

first major unified military command with the primary responsibility for Homeland Defense. The chapter discusses the difference between homeland defense and homeland security and the roles that the USNORTHCOM plays in each. The chapter concludes with a discussion of the USNORTHCOM J2, explaining its mission and goals and sets the baseline for the need for more law enforcement information to create all-source fusion intelligence products.

Chapter IV: "Breaking Down the Walls" explores more deeply the problems existing in the sharing of law enforcement information with military intelligence entities, specifically the USNORTHCOM J2. The chapter evaluates the legal basis of sharing this data, including a discussion of any legal barriers that would preclude sharing. In a recently published Naval Postgraduate School thesis, Todd Gleghorn points out that "[t]he primary reason the conceptual and operational distinctions are made [between foreign and domestic intelligence operations] is to protect the civil liberties of the American public. Thus, the rules that govern the conduct of domestic security (law enforcement) and foreign intelligence operations are different."[3] A review of Executive Order 12333 [4] is necessary to understand the ground rules that military intelligence analysts must follow. Similarly, the USA PATRIOT Act of 2001[5] continued to clarify what the intelligence analyst could and could not do with information derived from intelligence and law enforcement collection. The chapter continues with a discussion of the cultural and political barriers, created over time, which are the real inhibitors to a free flow of information between the Intelligence Community and Law Enforcement entities.

Chapter V: "Prescriptions for Change" looks at possible recommendations for increased collaboration and cooperation across the divide that has been built up between law enforcement agencies and military intelligence entities such as the USNORTHCOM J2. The first section discusses the recent focus of information sharing; that is, the balance

---

[3] Gleghorn, Todd E. *Exposing the Seams: The Impetus for Reforming U.S. Counterintelligence* (Monterey, Naval Postgraduate School, 2003), 59.

[4] U.S. President. Executive Order. "United States Intelligence Activities, Executive Order 12333," *Federal Register 46*, no. 59941 (4 December 1981). Available [Online]: http://www.fas.org/irp/offdocs/eo12333.htm [20 February 2005].

[5] Charles Doyle, *The USA PATRIOT Act: A Sketch* (Washington, D.C.: Congressional Research Service Report for Congress, 18 April 2002. Library of Congress Congressional Research Service, Order Code RS21203), 1.

between "need to know" and "need to share." The recent debate on information sharing has hinged on this need to be able to provide all available information balanced against the need to protect sources and methods. The chapter then moves to a brief discussion of the most recent reforms suggested by the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, and implemented by the *Intelligence Reform and Terrorism Prevention Act of 2004*, and how they will relate to USNORTHCOM. These recent reforms support USNORTHCOM J2 efforts to receive all available law enforcement information that is legally available to military counterterrorism analysts to receive, retain, and use. The two stage process to establish whether domestic intelligence on US Persons is allowed to be shared with USNORTHCOM J2 analysts is tackled, including defining the "reason to believe" a connection exists with transnational terrorism. The chapter closes with a discussion on the diffusion of analytic talent across the Intelligence Community and how USNORTHCOM J2 can be a vital contributor to the process.

Chapter VI: "A More Perfect Union" summarizes the challenges of sharing law enforcement information with military intelligence analysts, focusing on future reforms and the impact these prescriptions will have on the USNORTHCOM J2. It ends with a call for continued reassessment of established programs and policies to ensure future information sharing and collaboration across the intelligence / law enforcement divide.

C. WHAT WILL NOT BE ADDRESSED

Many changes have already taken place within the last eighteen months during the research and writing of this thesis. Because of that, this thesis cannot cover *all* the reforms in detail as they are spelled out in the recent *Intelligence Reform and Terrorism Prevention Act of 2004*. Although the reforms of the community, the relationships between the members, and the future organizational structure are important topics, they are not all central to the discussion of access to law enforcement information by USNORTHCOM J2 counterterrorism analysts. Only those aspects of the legislation central to the theme of information sharing will be addressed. Additionally, the creation of a National Intelligence Director, although very important, will be tangential to the question of increased information flow to USNORTHCOM. This position *will* have the

ultimate responsibility of ensuring information and intelligence is widely disseminated to increase cooperation and coordination across the community. However, a discussion of all the responsibilities of the new leadership position is not central to this thesis and therefore will not be addressed.

There has been much discussion over the last two years concerning the creation of a domestic intelligence agency, separate from the Federal Bureau of Investigation (FBI). Much talk has focused on the need to strip intelligence activities from the FBI, allowing them to concentrate on law enforcement activities due to the different nature of law enforcement and intelligence work.[6] Although this debate has been put aside for the time being, the elements of this discussion will not be addressed as a possible solution for the increased access to and fusion of law enforcement information by USNORTHCOM intelligence analysts. [7]

Lastly, this thesis is not a debate about the relevance or importance of open source material, also known as OSINT. In the world of counterterrorism analysis, *all* information is relevant to the fusion of a coherent and accurate product. Additionally, the thesis is not about how information is collected. The threat posed by transnational terrorists to the U.S. is not the same as the traditional Cold War threat posed by other nation-states. These threats do not operate in the same manner as traditional enemies have in the past; they do not have traditional militaries (army, navy, or air forces) that the U.S. military can posture against and prepare for. The Intelligence Community needs to be able to mine all areas of intelligence, to include traditional national technical means (e.g., information collected by satellite reconnaissance), as well as human intelligence (HUMINT), and those sources of information openly available to the analysts over the Internet, in libraries, magazines and newspapers around the world (OSINT). This thesis

[6] See Chapter III and Chapter IV for a more detailed look at the differences between intelligence and law enforcement information, as well as the different cultural mind set of how the FBI and the analysts with the Intelligence Community treat and deal with information.

[7] The National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, and the resulting *Intelligence Reform and Terrorism Prevention Act of 2004*, decided not to remove domestic intelligence responsibilities from the FBI. In fact, the Commission stated that "We do not recommend the creation of a new domestic intelligence agency. It is not needed if our other recommendations are adopted…".

does not place one type of information over the other; it focuses on the fusion of *all* sources of information into one "accurate, timely and relevant" intelligence product provided to senior decision and policy makers.

THIS PAGE INTENTIONALLY LEFT BLANK

II. 'SEPARATE BUT EQUAL' COMMUNITIES

A. NATURE OF THE THREAT

The 9/11 attacks forever altered the relationships between, and activities of, the Intelligence and Law Enforcement Communities, raising counterterrorism analysis to one of their most important disciplines. Although the rise in transnational terrorism was observed prior to 11 September, neither community responded quickly to counter it. The Director of Central Intelligence (DCI) George Tenet, provided an assessment to the Senate Intelligence Committee in February 2001, almost seven months before 9/11, stating, "[T]he threat from terrorism is real, it is immediate, and it is evolving. State sponsored terrorism appears to have declined over the past five years, but transnational groups — with decentralized leadership that makes them harder to identify and disrupt — are emerging…[Osama] bin Ladin and his global network of lieutenants and associates remain the most immediate and serious threat." [8]

Although counterterrorism analysis is a primary focus area for the Intelligence Community, it is quite different from traditional strategic analysis and military threat analysis conducted during the Cold War and through the first part of 2001. Traditional intelligence analysis, looking at threats stemming from primarily nation-states, is more linear in most cases. This type of analysis lends itself to more static and observable indications and warnings. The use of 'checklists' and indicator 'stoplight charts,' changing in color from green (no threat or normal activity) to yellow (increased activity) to red (potential threat activity) is commonplace. Over the years, the technical side of intelligence collection has been the preeminent source of information for intelligence analysts. Counterterrorism analysis, however, "must provide structure to information that can be highly fragmentary, lacking in well-defined links, and fraught with deception. It must infer specific strategies and plans from small pieces of information. It must find

[8] Congress, Senate, Select Committee on Intelligence: *Statement by Director of Central Intelligence George J. Tenet before the Senate Select Committee on Intelligence on the "Worldwide Threat 2001: National Security in a Changing World" (as prepared for delivery)* (107th Cong., 7 February 2001).

common threads among seemingly disparate strands. And unlike the terrorist, who needs only a single vulnerability to exploit, the analyst must consider all potential vulnerabilities." [9]

In order to meet this threat and develop accurate and timely intelligence, both the Law Enforcement and Intelligence Communities must work together. In the past, there was disagreement as to whether terrorism was a law enforcement problem or an intelligence concern. After 9/11, there is no longer a debate. In today's threat environment, terrorism can be viewed as *both* a law enforcement concern and as a threat to the national security of the United States, which is the realm of the Intelligence Community: "The need for information extends beyond simply following individuals, it also requires knowledge of what is being said on the streets and in the mosques of Brixton or Boston – it is doing 'foreign intelligence' domestically." [10] Therefore, accurate and timely intelligence from both law enforcement and national security intelligence sources is critical to the security of the U.S. Thomas Kean, the Chairman of the National Commission on Terrorist Attacks upon the United States Commission (also known as the 9/11 Commission) stated, "[t]hese agencies are the most important in the war on terror – more important than the Army" and that getting them to share information is "absolutely vital in the national interest." [11]

So what is the difference between "traditional intelligence" and "non-traditional intelligence?" The Markle Foundation Task Force on National Security in the Information Age published a report entitled "Protecting America's Freedom in the Information Age" and provided a good description of the differences between the two types of information, highlighting one of the greatest difficulties in the different approaches to intelligence analysis:

> Law enforcement information is information collected to investigate, solve, and prosecute crimes. Law enforcement is primarily reactive. That is, although sometimes law enforcement operations prevent crime, usually

[9] Jeffrey A. Isaacson, and Kevin O'Connell, "Beyond Sharing Intelligence, We Must Generate Knowledge,"RAND Corporation, (http://www.rand.org/publications/randreview/issues/rr.08.02/intelligence.html) [20 February 2005].

[10] Gregory F. Treverton, "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons," *Intelligence and National Security, Vol 18., No. 4 (*Winter 2003*),* 134.

[11] John Diamond, "Panel Now Faces Difficult Task of Finding Fixes," USA *Today*, 15 April 2004, 2.

> they solve crimes after they occur…in the course of investigations and prosecutions of suspected terrorists, law enforcement officials gather a great deal of information about terrorists.
>
> The purpose of intelligence is to provide warning, help assess threat vulnerabilities, identify policy opportunities, and assist policymakers in national security decision-making. Unlike information collected for law enforcement, the purpose of intelligence collection is to prevent harm. Because of the potentially devastating effects of a terrorist attack, counterterrorism is seen increasingly as more of an intelligence challenge than a law enforcement challenge. [12]

In order to better understand the difference between "traditional intelligence" and "non-traditional intelligence," a look at the two communities is necessary.

B. THE U.S. INTELLIGENCE COMMUNITY

Intelligence has been defined as "the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers."[13] There are several ways to describe the National Intelligence Community; by function (management and execution); by activities (collection, analysis, covert action and counterintelligence); or by which Executive Branch department or independent agency each intelligence organization falls under (Department of Defense, Department of State, Department of Justice, Central Intelligence Agency, etc.). [14] However you describe it, the Intelligence Community is a vast network of organizations and agencies that collect, analyze and produce intelligence products to support policymakers. For the members of the Intelligence Community, "intelligence means puzzle solving or mystery framing that is good enough for action. The goal is policy. The context is a blizzard of uncertainty, often one that cannot be melted into clear contours. And the standard is "good enough to act…". [15]

---

12 "Creating a Trusted Network for Homeland Security." *Second Report of the Markle Foundation Task Force on National Security in the Information Age.* By Zoe Baird and James L. Barksdale, co-chairmen (New York: The Markle Foundation, 2003), Appendix B, i, iii.

13 Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003), 8.

14 Lowenthal, 13, 29.

15 Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge, Cambridge University Press. 2001), 167.

The Intelligence Community is an eclectic group of organizations and agencies with processes and procedures that are at times complimentary, and at others duplicative. It is made up of "agencies and offices whose work is often related and sometimes combined, but who work for different clients and under various lines of authority and control." [16] There has been no master plan for the development of the community. Its development has occurred over several decades, with the creation of several agencies that specialize in distinct areas of intelligence activities of collection, analysis, covert action and counterintelligence. One of the most influential pieces of legislation in the development of today's community was the National Security Act of 1947 which "gave the legal basis to the Intelligence Community" [17] and established the Central Intelligence Agency (CIA). One of the most important aspects of this legislation, with particular regard to this thesis, was the fact that the CIA could not have a domestic intelligence role or have any law enforcement capability. [18] These roles and responsibilities were the purview of the Federal Bureau of Investigation (FBI). This distinction was reinforced and emphasized in the 1970s during the Church Committee hearings (a more detailed description is provided in Chapter IV).

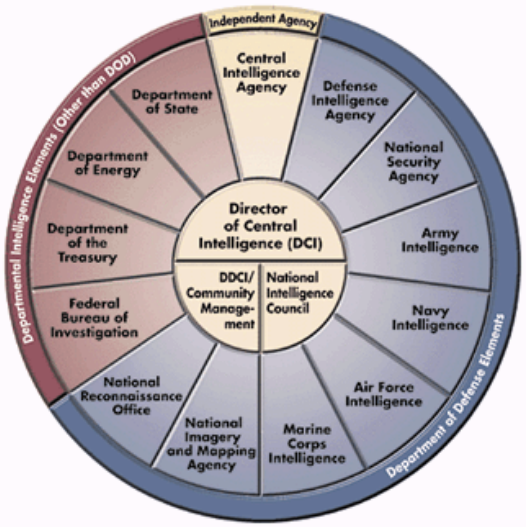

Figure 1. The Intelligence Community

[16] Lowenthal, 10.

[17] Lowenthal, 18.

[18] Lowenthal, 19.

The Department of Defense (DoD) controls much of information and data identified as national security intelligence in today's Intelligence Community; "the panoply of agencies … vastly outnumber the CIA, in terms of both people and dollars." [19] Whether it is the collectors of intelligence (such as the National Security Agency or the National Geospatial Intelligence Agency), or analytic units (the Defense Intelligence Agency and service specific intelligence units), the DoD collects, processes and analyzes most of the intelligence the community creates. One area, however, that the DoD does not provide the majority of information is in domestic intelligence, which is the primary responsibility of the FBI and the rest of the Law Enforcement Community.

C. THE U.S. LAW ENFORCEMENT COMMUNITY

The Law Enforcement Community is represented at all three levels of government (federal, state and local) and its primary members are police and security forces. The members of the Law Enforcement Community are first and foremost concerned with the enforcement of the laws within their jurisdictions. For the members of this community, the collection of 'intelligence' is not a primary responsibility. In fact, for the FBI and other law enforcement organizations, "intelligence is instrumental on another sense, not for policy but for cases. Intelligence means tips to wrongdoing or leads to wrongdoers. The goal is convictions. The context is individual cases. And the standard is the courtroom. It is beyond a reasonable doubt." [20]

The FBI is the leader of the community, and is the largest law enforcement entity at the federal level; it is also a member of the Intelligence Community (see Figure 1.). Although it is the largest representative from the federal government in the law enforcement community, there are other federal law enforcement organizations that are integral to homeland security, including the Customs and Border Patrol (CBP), Immigrations and Customs Enforcement (ICE), and the Drug Enforcement Agency (DEA). [21] States and local representation with in the Law Enforcement Community is

---

[19] Lowenthal, 25.

[20] Treverton, *Reshaping National Intelligence for an Age of Information*, 167.

[21] Many of these federal law enforcement agencies now are part of the Department of Homeland Security, or DHS.

made up of State Police and Highway Patrol officers, city and county police organizations. Coordination between the different levels of the community take place on specific crimes, or on task forces developed around types of crimes (such as organized crime, motor vehicle theft, kidnappings, etc.). The Joint Terrorism Task Force (JTTF), for example, is designed specifically to share information related to terrorism within the U.S. between the federal law enforcement agencies and the state and local entities. There are JTTFs at each of the FBI's 56 field offices, as well as in ten other locations around the country.

D. INTELLIGENCE VS. LAW ENFORCEMENT INFORMATION

To successfully counter terrorism and prevent attacks from occurring on US soil, a closer cooperation between the Intelligence and Law Enforcement Communities is essential. The plans for the 9/11 attacks were formulated and hatched in al-Qa'ida training facilities and compounds in Southwest Asia, but the specific operatives that conducted the attacks needed to train and operate within the US to complete the attack. Foreign intelligence may have told us about such planning and may have possibly identified potential operatives and support personnel, but law enforcement information would have to have been developed concerning the activities of the hijackers once they were in the US. The need for a closer cooperation between the Intelligence and Law Enforcement Communities is clear: the globally interconnected world can bring the transnational terrorism threat to the homeland, reinforcing the need to combine these two sources of information together in one intelligence product. Prior to and immediately following the 9/11 attacks, this was not always the case. In fact, "some believe terrorist acts may have been facilitated by continuing poor information exchanges between intelligence and law enforcement agencies and by blurred lines of organizational responsibility." [22]

Coordination between the two communities has been marked by secrecy, lack of communication and an indifference to what the other agencies are doing. Their approaches to intelligence collection and analysis are completely different and their

22 Richard Best, Jr., *Intelligence to Counter Terrorism: Issues for Congress* (Washington, D.C.: Congressional Research Service Report for Congress, 27 May 2003), i.

viewpoints on the role and importance of intelligence are different. Coordination, then, and the sharing of traditional and non-traditional intelligence "is likely to prove to be very difficult, challenging constitutional limits on domestic law-enforcement activity while drawing intelligence officers ever closer to proceedings that could compromise sources and methods of intelligence collection." [23]

The attacks on 9/11, however, reemphasized the need for increased coordination and information flow between the two communities. As the two worlds grow closer together (and in some cases collide), many barriers to better cooperation need to be understood and removed. Each community needs to begin to understand the cultural and legal restrictions that have been built over time in order to provide better solutions for cooperation and information sharing. In the world of counterterrorism analysis, "intelligence agencies work alongside law enforcement agencies that have far different approaches to gathering evidence, developing leads, and maintaining retrievable databases. Policies and statutes are being modified to facilitate a closer relationship between the two sets of agencies, but closer cooperation has raised difficult questions about using intelligence agencies in the U.S. and about collecting information regarding U.S. persons." [24]

---

[23] Richard Best, Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S* (Washington, D.C.: Congressional Research Service Report for Congress, 3 December 2001), 4.

[24] Best, *Intelligence to Counter Terrorism: Issues for Congress*, 1, 2.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DOD, U.S. NORTHERN COMMAND, AND THE NORTHERN COMMAND INTELLIGENCE DIRECTORATE

The attacks on 11 September 2001 revealed a major shortcoming in the DoD: the military's inability to respond quickly to and deter the threat posed by foreign terrorists to the United States. The primary response to this shortcoming was the establishment of the first combatant command on US soil solely dedicated to defend the United States, the U.S. Northern Command. Although all major military combatant commands have the responsibility of defending the United States against attack, this is the first command with the authority for defense of the continental United States.

A. HOMELAND SECURITY AND HOMELAND DEFENSE

The first step in understanding the need for the establishment of a combatant commander with the specific responsibility for protecting and defending the U.S. is to better define and understand the difference between homeland security and homeland defense.

Homeland security is the "concerted national effort to prevent terrorist attacks within the US, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[25] The key to homeland security (and the underlying concept in the National Strategy for Homeland Security) is to secure the U.S. from terrorist attacks, with a primary focus being protecting the country against such attacks. This means a comprehensive program across all levels of government to secure the safety of the people, the national infrastructure, our economy, and our democratic way of life. It also means protecting it from both domestic and international terrorism, which can cover a wide spectrum of potential threats and attack venues. One of the most significant roles the DoD plays in homeland security is that of support to civil authorities. DoD assets, including military forces, can be called upon to support civil authorities in the aftermath of an attack to support federal, state, and local levels of government in the consequence management of an event.

[25] Office of Homeland Security, National Strategy for Homeland Security, (Washington, 2002) 2.

Homeland defense, on the other hand, is "the protection of U.S. territory, domestic population and critical infrastructure against military attacks emanating from outside the United States." [26] The DoD and the U.S. military are the primary player in homeland defense and occurring on land, in the air, at sea, and in cyberspace. The primary function of homeland defense is to deter and defeat an attack as far away from the homeland as possible; the U.S. military projects its power globally in order to accomplish this. It is also capable of applying military force against those threats in the approaches to, and directly on, the homeland.

DoD has the primary and most significant role in homeland defense. First, the military provides security to the U.S. by projecting power overseas and conducting military operations abroad. The U.S. military is the leading force in the Global War on Terrorism, attacking outside the US those groups and entities that threaten to strike at the U.S. from within the homeland. Most international (or transnational) terrorists operate outside the U.S. and will have to come to the homeland to conduct their attacks. [27] Bringing the fight to these transnational terrorist groups in other countries before they come to the U.S. has been defined as the "away game." If these groups decide to attack here in North America, the U.S. military can provide protection with military forces, defending the homeland against such attacks on our soil. Continuing with the sports analogy, it stands to reason that this has been termed the "home game."

When an event occurs that requires federal response, be it a natural disaster or an attack from transnational terrorists, it is necessary to determine who the "lead federal agency" is to manage the event for the U.S. government. In simplistic terms, the lead federal agency for homeland defense will be the DoD, and its primary representative, USNORTHCOM. The lead federal agency for homeland security issues will be some

---

[26] The U.S. Northern Command website tries to make clear the distinction between homeland defense and homeland security. It states "Homeland defense is the protection of U.S. territory, domestic population and critical infrastructure against military attacks emanating from outside the United States. In understanding the difference between HLS and HLD, it is important to understand that NORTHCOM is a military organization whose operations within the United States are governed by law, including the Posse Comitatus Act that prohibits direct military involvement in law enforcement activities. Thus, NORTHCOM's missions are limited to military homeland defense and civil support to lead federal agencies." For more information, see http://www.northcom.mil/index.cfm.

[27] All of the 9/11 hijackers came from other countries, most of whom were Saudi Arabian citizens.

other government agency, not the DoD. If DoD (and in turn, USNORTHCOM) becomes involved, it will be at the request of the lead federal agency in charge of the event.

B. THE CREATION OF THE U.S. NORTHERN COMMAND

DoD recognized that its response to the 9/11 attack was inadequate. Although response forces mobilized immediately following the attacks in assistance of civil authorities, the military response *before* the attacks was slow, uncoordinated and inadequate to meet the threat. The final report of the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) noted that "[a]t no point before 9/11 was the DoD fully engaged in the mission of countering al Qaeda, though this was perhaps the most dangerous foreign enemy then threatening the United States." [28] Additionally, the Commission found that the Department of Defense and the North American Aerospace Defense Command (NORAD), "which had been given the responsibility for defending U.S. airspace, had construed that mission to focus on threats coming from outside America's borders. It did not adjust its focus even though the intelligence community had gathered intelligence on the possibility that terrorists might turn to hijacking and even use of planes as missiles." [29] The immediate response to the attack revealed that although there were a multitude of military forces arrayed in the U.S. before and on 9/11 that were capable of defending the homeland against attack, there was no "unity of command," no single commander to turn to in defense of the country, to marshal and lead the forces against the threat/attack.

USNORTHCOM was created following the issuance of the Unified Command Plan of 2002. The Unified Command Plan (UCP) is a document, approved by the President, which establishes each of the combatant commanders and unified commands. It sets forth in writing the roles and missions for each commander, their roles and responsibilities over specified geographic and functional areas. As stated previously, the 9/11 attacks demanded a realignment of DoD's resources in order to better defend against and respond to aggression from today's threats before they occur. UCP 2002 was one of

---

[28] National Commission on Terrorist Attacks Upon the United States, Thomas H. Kean and Lee H. Hamilton. *The 9/11 Commission Report.* (Washington, D.C.: 2004), 351.

[29] National Commission on Terrorist Attacks Upon the United States, 427-8.

the most far-reaching efforts to realign and reshape the DoD in over 50 years; not since the establishment of the Defense Department in 1947 has the military realigned so radically.

It has always been the responsibility for the U.S. military to defend the country; it is a cornerstone in the oaths that are taken by every service member. Yet, there has never been a central command authority to explicitly address threats to the homeland. USNORTHCOM is the first combatant command established with the primary responsibility of protecting the homeland. The creation of USNORTHCOM allows DoD to develop "unity of command" over those roles and missions defined as homeland defense and Military Assistance to Civil Affairs (or MACA). Its area of responsibility covers the land, airspace, and the sea approaches to the United States and its geographic responsibility covers Canada, Mexico, portions of the Caribbean and the waters of the Atlantic and Pacific oceans surrounding the U.S.

Figure 2. US Northern Command Seal

The importance of the unity of command that USNORTHCOM provides cannot be overstated. The terrorist attacks that occurred on 9/11 made it very clear that the strategic environment we operate in has changed significantly from what it was just a few years ago. We now realize that we are vulnerable to attacks from within – attacks that can come unexpectedly inside North America and that demand a rapid, determined response.

Most combatant commands have a mission focused on military defense. USNORTHCOM is different from other military combatant commanders in that it provides both military defense and military support to civil authorities if needed and when directed. USNORTHCOM's stated mission is to "conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; and as directed by the President or Secretary of Defense, provide military assistance to civil authorities including consequence management operations." [30] This mission statement shows the dual tasking of defense *and* support.

Initial Operating Capability (IOC) is the first capability level to be attained by a command to begin operations. It is by no means the final step, but it establishes a benchmark for the command to conduct operations and carry out its responsibilities. USNORTHCOM reached IOC on 01 October 2002 when UCP 2002 became effective with the start of the U.S. Government Fiscal Year 2002. When a command is considered "fully operational" and is able to carry out all assigned missions and responsibilities, the command is said to have reached Full Operational Capability, or FOC. USNORTHCOM reached FOC on September 11, 2003 – less than one year after its stand-up, and symbolically two years to the day of the attack on the World Trade Center and the Pentagon by al-Qa'ida terrorists.

[30] U.S. Northern Command, *U.S. Northern Command's Strategic Vision,* (Colorado Springs, CO, 2003), 12.

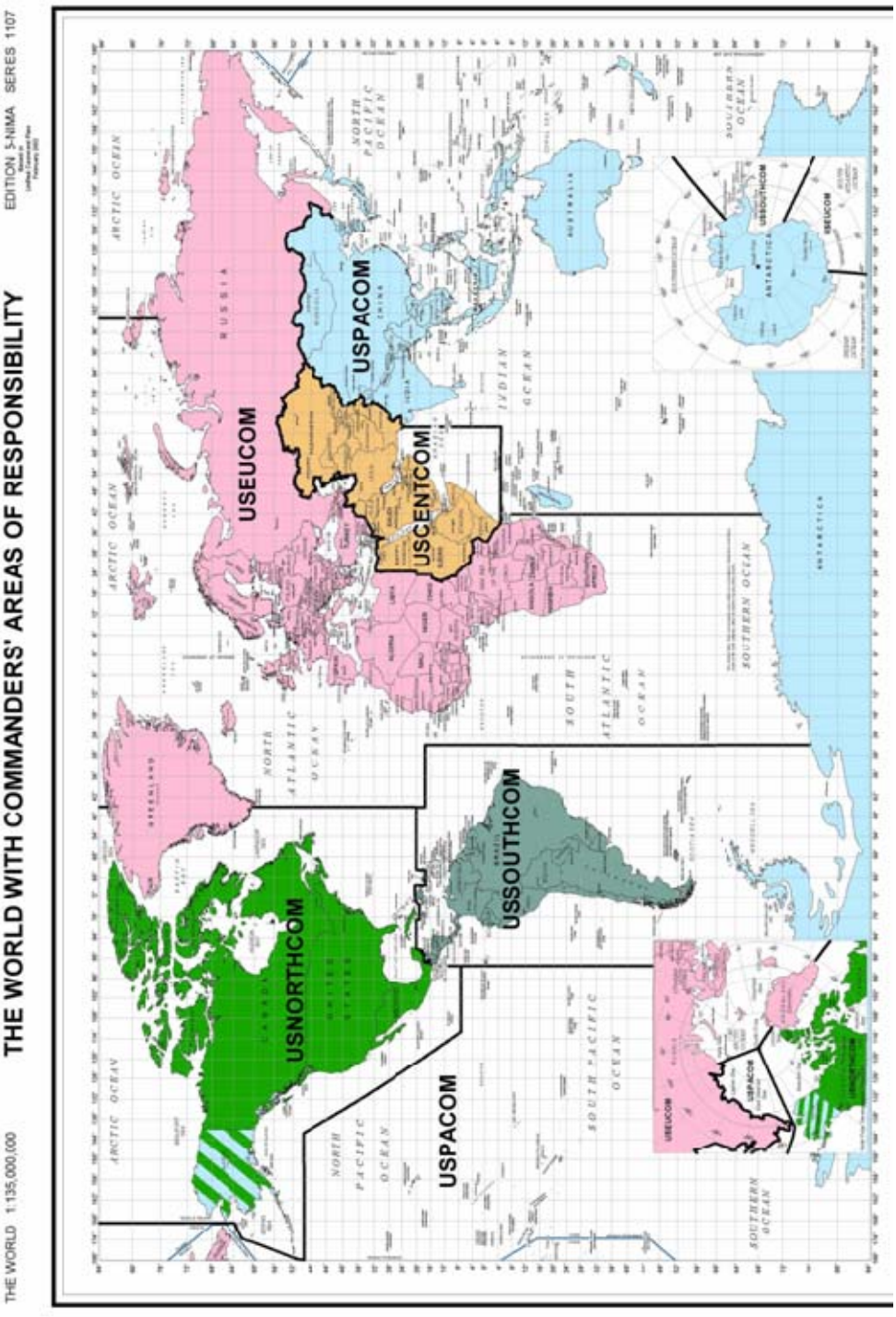

Figure 3. Regional Combatant Commander Areas of Responsibility

C. U.S. NORTHERN COMMAND INTELLIGENCE DIRECTORATE (J2)

Each combatant command contains several different organizational directorates on its staff that have primary responsibility over specific areas of concern. These include directorates focusing on operations (J3), planning (J5) and of course, intelligence (J2). The US Northern Command Intelligence Directorate (USNORTHCOM J2) has the primary responsibility to provide 'accurate, timely, and relevant' indications and warnings of potential threats against North America to the Commander, USNORTHCOM and to those forces assigned to him. This enables the Commander to be able to situate his forces to defend the country from external threats, and to prepare to deploy forces in a civil support role if attacks occur within the AOR. The J2's mission is to "provide predictive and actionable estimates and timely warning of worldwide threats against North America using all-source intelligence and law enforcement information," being the "eyes and ears" for the Commander and his assigned forces "to ensure [he] is not only prepared to react, but more importantly, to be proactive" in order to "both deter and protect." [31]

With the responsibility for homeland defense intelligence, the J2 has a dual focus: intelligence analysis of external threats to the U.S. (the 'away game') and possible foreign linkages to threats internal to the U.S. and the USNORTHCOM AOR (the 'home game'). [32] This dual focus makes the USNORTHCOM J2 ideally situated to make the most of the fusion of traditional and non-traditional intelligence information, creating that fused analytic picture for both the Commander USNORTHCOM and the rest of the Intelligence Community. The J2's Combined Intelligence and Fusion Center (CIFC) is the key to this fusing of information: General Ralph Eberhart, USNORTHCOM's first commanding officer stated, "Our Combined Intelligence and Fusion Center collates and analyzes data. Our goal is to connect the dots to create a clear threat picture, playing our appropriate military role as part of the interagency team." [33]

---

[31] U.S. Northern Command, Sustained Vigilance: Intelligence Support for North America's Homeland Defense (Colorado Springs, CO, 2003), 1, 5.

[32] The "away game" intelligence is important because transnational terrorists plan their attacks against the U.S. outside our national boundaries, and outside the USNORTHCOM AOR. J2 analysts need to keep apprised of data external to the U.S. to ensure that USNORTHCOM and homeland defense equities are analyzed in the correct context.

[33] Sustained Vigilance, 6.

In order to accomplish its mission, USNORTHCOM J2 must be able to use all intelligence sources, including law enforcement information, to understand fully the potential threats and capabilities arrayed against it. This fused, all-source intelligence picture enables the USNORTHCOM J2 to provide the Commander, USNORTHCOM an in-depth and complete analytic assessment of any potential threats in order for the command to carry out its mission of defense of the homeland. The goal of the J2 is to "be a leader in the analytical community by embracing collaboration across the intelligence, law enforcement, and inter-agency areas to ensure optimum efficiency and effectiveness." [34]

[34] Sustained Vigilance, 10.

IV. BREAKING DOWN THE WALLS

A. WHY AREN'T WE SHARING ACROSS THE DIVIDE?

The events of 9/11 revealed the dysfunctional nature of the information sharing relationship between the Law Enforcement and Intelligence Communities. It also revealed the fundamental differences between the two communities: "The law enforcement/national security divide is especially significant, carved deeply into the topography of American government. The national security paradigm fosters aggressive, active intelligence gathering. It anticipates the threat before it arises and plans preventive action against suspected targets. In contrast, the law enforcement paradigm fosters reactions to information provided voluntarily, uses ex post facto arrests and trials governed by rules of evidence, and protects the rights of citizens." [35] In fact, this distinction between the two communities is entrenched within the cultures and policies of the specific communities. For example, Section 9-90.210(A) of Volume 9A of the *Department of Justice Manual* states:

> Although both are arms of the executive branch, the federal law enforcement and intelligence communities have very distinct identities, mandates and methods. The mission of the former is to identify, target, investigate, arrest, prosecute, and convict those persons who commit crimes in violation of federal laws. The mission of the latter is to perform intelligence activities necessary for the conduct of foreign relations and the protection of the national security, including the collection of information and dissemination of intelligence; and the collection of information concerning espionage, international terrorist activities, and international narcotics activities. [36]

There are significant differences in the cultures that make up each community, as well as legal restrictions that have been established over time. These specific legal restrictions were created to protect civil liberties of U.S. citizens, but the result was the limitation of law enforcement and intelligence information cross over between the two communities, and the resulting cultures that make up each community reinforced these restrictions, both real and perceived. These barriers are entrenched within both the Law Enforcement and Intelligence Communities, and removing them to increase cooperation

[35] Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S,* 9.

[36] Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S,* 15.

and information flow may be difficult to do, but will be essential to provide increased information sharing between the two.

B. LEGAL BARRIERS

Many of the barriers to improved communication and information flow between the two communities were erected by Congress to stem abuses by these organizations during the 1960s. Following several scandals in the abuse of intelligence collection activities against U.S. citizens, many protective barriers were erected: "In response to these FBI abuses [COINTELPRO in the 60s, against the Committee in Solidarity with the people of El Salvador (CISPES) in the 80s], the Department of Justice imposed domestic intelligence collection standards on the [Intelligence Community], including the FBI. For example, in 1976, Attorney General Edward H. Levi issued specific guidelines governing FBI domestic security investigations. Congress also established House and Senate intelligence oversight committees to monitor the IC. And President Carter signed into law the Foreign Intelligence Surveillance Act of 1978, which established legal procedures and standards governing the use of electronic surveillance within the U.S." [37] In fact, the National Security Act of 1947, which established the CIA, "specifically precluded the Agency from having any responsibilities for law enforcement or internal security." [38]

Because of these scandals and infringements on the civil rights of many Americans during these periods, "in the mid-1970s, Congress's first-ever inquiry into intelligence, the Senate Select Committee on Intelligence Activities, headed by then-Senator Frank Church (D-Idaho), investigated abuses of the rights of Americans…the Congress's response was to *raise* the walls between intelligence and law enforcement – for instance, by creating a special court, the Federal Intelligence and Surveillance Court (FISC), to review applications for national security, as opposed to law enforcement, wiretaps and surveillance." [39] Based on these "widespread criticisms of domestic spying

---

[37] Alfred Cumming and Todd Masse. *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress* (Washington, D.C.: Congressional Research Service Report for Congress, 6 April 2004), 48.

[38] Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, 9-10.

[39] Gregory F. Treverton, *Intelligence, Law Enforcement, and Homeland Security* (Washington, D.C.: The Century Foundation, 21 August 2002), 2.

by the CIA and other intelligence agencies," the actions of Congress and the agencies involved "served to build walls of separation between the [law enforcement and intelligence communities] that were widely recognized in practice even if cooperation on narcotics and terrorism was officially allowed." [40] The emphasis then was for law enforcement to focus internally on domestic intelligence activities inside the United States and for the Intelligence Community to focus outward on intelligence activities in foreign countries. This alleviated the Intelligence Community on its concern about activities that could be considered infringements on the civil rights of U.S. citizens because "[i]ntelligence collected abroad on foreign persons does not raise Fourth Amendment search-and-seizure issues," [41] as well as First Amendment concerns on freedom of speech.

The attacks by al-Qa'ida on 9/11, however, showed that terrorism can occur within the U.S. and include the actions of persons that may be considered "U.S. Persons." [42]. Therefore, "[i]ntelligence collected on U.S. persons, or within the U.S. … [can] raise some of these constitutional issues, but when the purpose of the collection is for national security, courts have allowed greater flexibility for intelligence collection than for law enforcement, particularly when the threat can be shown to be a foreign power." [43]

1. What Does the Law Actually Say?

Are there actual restrictions which preclude counterterrorism intelligence analysts at USNORTHCOM J2 from viewing and using law enforcement-derived intelligence in their analytic products? A look at the governing laws and instructions for military intelligence analysts reveals that although there are some restrictions, they are not so onerous as to preclude law enforcement agencies from providing this information to USNORTHCOM J2 counterterrorism analysts for use in all-source, fused analytic intelligence products.

---

[40] Best, Intelligence and Law Enforcement: Countering Transnational Threats to the U.S, 10.

[41] Second Report of the Markle Foundation Task Force on National Security in the Information Age, Appendix B, iii.

[42] The definition of "US Persons" is addressed later in this chapter on page 28.

[43] Second Report of the Markle Foundation Task Force on National Security in the Information Age, Appendix B, iii.

Following the 9/11 attacks by al-Qa'ida, "Congress passed the USA PATRIOT Act, a principal purpose of which was to remove perceived restrictions on closer law enforcement-intelligence cooperation in order to support counterterrorist efforts. Modifications to the Foreign Intelligence Surveillance Act (FISA) for the same purpose were enacted shortly thereafter as part of the FY2002 Intelligence Authorization Act (P.L. 107-108)...". [44] The PATRIOT Act encourages an increased transfer of information from law enforcement to intelligence agencies and analysts. The Act "affords the U.S. intelligence community greater access to information unearthed during criminal investigation."[45] Section 203 of the Act "broadens the law enforcement community's ability to share information" including "previously unattainable Grand Jury information with any intelligence, national security, or national defense official when the information is of foreign or counterintelligence value." [46]

There are those that consider this expanded ability to pass law enforcement information to intelligence as ripe for abuse, however, "the premise of the USA-PATRIOT Act is that information about foreign terrorists acquired by law enforcement agencies, including grand jury information, should be available to intelligence agencies. Analysts would be able to put together the larger picture of groups plotting against U.S. interests." [47] This will allow both the law enforcement agencies and the Intelligence Community to get a more complete picture of the potential threat arrayed against the U.S. The current FBI Director, Robert Mueller believes that the PATRIOT Act has helped not only the flow of information from his agency to the rest of the Intelligence Community, but has helped to change the focus of his agents and analysts. It is his belief that "the FBI can now, '…move from thinking about 'intelligence as a case' to finding 'intelligence in the case.'" [48]

---

[44] Best, *Intelligence to Counter Terrorism: Issues for Congress*, 5.

[45] Doyle, *The USA PATRIOT Act: A Sketch*, 3.

[46] Regan K Smith, "Military Module," *Military Intelligence Professional Bulletin* (Jul-Sep 2002), 6.

[47] Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S*, 31.

[48] Cumming, 50.

2. Executive Order 12333 and Department of Defense Instructions

The fact is that Intelligence Community counterterrorism analysts were already able to use certain types of domestic intelligence before the passage of the USA PATRIOT Act. Previously existing law already made it possible for intelligence analysts to collect, retain and disseminate certain types of law enforcement information under specific guidelines. The USA PATRIOT ACT did not change or alter Executive Order 12333, United States Intelligence Activities (EO 12333), which "stipulate[s] that certain activities of intelligence components that affect U.S. persons be governed by procedures issued by the agency head and approved by the Attorney General." [49] This order states, "[t]he United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats." [50] It goes on to say that, "[t]o the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort." [51] It allows organizations within the Intelligence Community to collect, produce, and disseminate intelligence for the "protection of the national security of the United States" using information "concerning, and the conduct of activities to protect against … hostile activities directed against the United States by foreign powers, organizations, persons, and their agents…". [52] This includes domestic intelligence on US persons, both collected and disseminated by law enforcement agencies (such as the FBI) or by the members of the Intelligence Community themselves.

---

[49] Michael P. Ley. "From the Editor," *Military Intelligence Professional Bulletin* (Jul-Sep 2002), 2.

[50] U.S. President. *Executive Order*. "United States Intelligence Activities, Executive Order 12333".

[51] U.S. President. *Executive Order*. "United States Intelligence Activities, Executive Order 12333".

[52] U.S. President. *Executive Order*. "United States Intelligence Activities, Executive Order 12333".

3. Department of Defense Instruction 5240.1-R

A second document that is very important in this discussion is DoD Instruction 5240.1-R, "Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons," which sets the ground rules for the use of information on "US persons" for military intelligence analysts. This instruction, signed by both the Secretary of Defense and Attorney General of the United States, expands on EO 12333 and is the governing document for military intelligence analysts (such as those within the USNORTHCOM J2) on how to implement the rules contained in EO 12333.

In order for USNORTHCOM J2 analysts to see and use information that may be considered domestic intelligence (generated from law enforcement sources), two important criteria must be met. The first is the understanding of what a "US person" is. By definition, a "US person" is:

1. A United States citizen;
2. An alien known by the DoD intelligence component concerned to be a permanent resident alien;
3. An unincorporated association substantially composed of United States citizens or permanent resident aliens;
4. A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person;
5. A person or organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained. An alien in the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained;
6. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence. [53]

The second critical criterion is establishing a nexus with transnational terrorism. DoD Instruction 5240.1-R states that information on US persons can be collected, analyzed and disseminated by military intelligence analysts if such person(s) "are reasonably believed to be engaged in, or about to engage in, intelligence activities on

[53] U.S. Department of Defense, DoD Instruction 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons* (Washington, D.C.: Government Printing Office, December 1982) 12.

behalf of a foreign power, or international terrorist activities" or are "in contact with persons described …above, for the purpose of identifying such person and assessing their relationship with persons described [above]." [54]

As shown, pre-existing law allows the exchange of certain domestic intelligence information on US Persons (as defined by law and military instructions) to military intelligence analysts. The USA PATRIOT Act "did not fundamentally alter the framework under which DOD conducts intelligence activities-the Act primarily affected the law enforcement community. All the current laws and regulations remain in effect for intelligence components."[55] Simply put, the alleged legal barrier stopping information flow of law enforcement information to USNORTHCOM J2 counterterrorsim analysts really does not exist. USNORTHCOM J2 analysts are by law able to view domestic intelligence on US Persons if a nexus with transnational terrorism is determined. The crux of this second criteria, therefore, is the definition of "*reasonably believed to be engaged*" in transnational terrorism. [56]

C. CULTURAL/POLITICAL BARRIERS

One of the largest challenges to information sharing, if not the largest, is the "respective bureaucratic cultures, modes of operation, sources of information, and oversight structures" and that the FBI "tend to give higher priority to tactical information" which "may have to be used in a public trial and its origins revealed to a defendants lawyer. Law enforcement agencies typically work on a case-by-case basis." [57] Intelligence agencies, on the other hand, support the national security policymakers which "require[s] a continuous stream of information from the CIA and other intelligence agencies about world conditions, especially about countries, groups, and individuals working against U.S. interests. There is no end-point to these requirements; even a favorable evolution of events…does not mean the end of the need for up-to-date information." [58] Intelligence agencies use, at times, less specific information, and "may,

54 DoD Instruction 5240.1-R, 16-17.

55 Smith, 6.

56 A more in depth discussion of "reason to believe" is covered in Chapter V, Section C.1.

57 Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S*, 15.

58 Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S*, 15.

moreover, seek rumors and gossip that could never stand up in court. Such information may, nonetheless, provide the best indication of a fluid political situation in another country that could directly affect U.S. interests." [59] The principle difference is that law enforcement agencies look for information that supports a 'burden of proof' whereas intelligence agencies use information that supports an 'analytic threshold' to provide a picture of the potential threat. This distinction is solidified in directives and operating instructions for the FBI. The *Department of Justice Manual (*DOJM) states:

> Although coordination on matters of common concern is critical to the proper function of the two [i.e., law enforcement and intelligence] communities, prosecutors must be aware of the concomitant need of both communities to maintain a well-delineated separation between criminal prosecutions and foreign intelligence activities, in which less-stringent restraints apply to the government. Not to do so may invite the perception of an attempt to avoid criminal law protections by disguising a criminal-investigation as an intelligence operation. The judicial response to that may be the suppression of evidence in the criminal case…. [60]

The organization's leadership prior to 9/11 reinforced this cultural barrier. The Markle Foundation Task Force found that "[t]he FBI is fundamentally a law enforcement agency. Its culture is that of a law enforcement agency, and the system rewards success in law enforcement such as arrests, prosecutions, and convictions. The disciplines of law enforcement and intelligence differ in critical ways, and FBI special agents primarily are taught the law enforcement view of how and why information is collected." [61] In fact, "[t]he FBI's traditional reliance on an aggressive, case-oriented, law enforcement approach did not encourage the broader collection and analysis efforts that are critical to the intelligence mission. Lacking appropriate personnel, training, and information systems, the FBI primarily gathered intelligence to support specific investigations, not to conduct all-source analysis for dissemination to other intelligence agencies." [62]

---

[59] Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S*, 16.

[60] Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S*, 20.

[61] Second Report of the Markle Foundation Task Force on National Security in the Information Age, Appendix B, v.

[62] U.S. Congress, Senate and House. Permanent/Select Committees on Intelligence. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 with additional views.* (107th Cong., 2d sess., 2002), 45.

This institutional barrier to sharing information, or for understanding the need to go beyond the 'case approach' to using or collecting intelligence, has hampered counterterrorism investigations for years. Over the years, "agents were barred from searching open sources, such as the Internet, without first opening a formal investigation. Agents had a deeply ingrained habit of keeping information to themselves and filing reports." [63] What this did was focus FBI personnel to move "away from counterterrorism work and toward the traditional pursuit of such crimes as Mob activity, kidnapping and white-collar offenses…'[t]raditional agents who weren't good on the street were put into intelligence,' said Jack Lawn, a veteran FBI agent who later ran the Drug Enforcement Administration." [64]

There are critics that believe "the FBI's law enforcement culture is too entrenched, and resistant to change, to be easily influenced by FBI Headquarters directives emphasizing the importance of intelligence in preventing terrorism. They cite the Gilmore Commission [65], which concluded, "[t]he Bureau's long-standing traditional organizational culture persuades us that, even with the best of intentions, the FBI cannot soon be made over into an organization dedicated to detecting and preventing attacks rather than one dedicated to punishing them." [66] The Markle Foundation report continues that "[The FBI] are simply not accustomed to – and in fact their culture discourages – a focus on a customer other than a prosecutor. Finally, the FBI has not traditionally valued, rewarded, or even understood analysis, which is critical to intelligence." [67]

This reinforcement of the culture comes from the many layers within the FBI leadership, to the point that "one senior state law enforcement official stated that the FBI leadership is '…still being led by individuals who have a criminal law mindset.'" [68] This

---

63 Michael Duffy. "How To Fix Our Intelligence," *Time*, 26 April 2004.

64 Duffy.

65 The Gilmore Commission, also known as the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, assessed the capabilities for responding to terrorist incidents in the U.S. involving weapons of mass destruction. Response capabilities at the Federal, State, and local levels were examined. Information on the Commission can be found at http://www.rand.org/nsrd/terrpanel/charter.html [05 March 2005].

66 Cumming, 18.

67 Second Report of the Markle Foundation Task Force on National Security in the Information Age, Appendix B, vi.

68 Cumming, 33.

fear of change may be due to the potential that the release or leak of information collected during an investigation would somehow get in the hands of those that would misuse the information: "One of the principle reasons that federal agencies do not widely share information with one another and, especially, with state and local governments and with private sector entities is fear that the information would be leaked to the media and the public – and thus to our nation's adversaries as well – thereby putting lives at risk, jeopardizing intelligence sources and methods, compromising law enforcement investigations or prosecutions, or violating individual civil rights." [69]

The DoD does not get off free and clear in this sense; they are also at fault in erecting a cultural and political barrier to the sharing of law enforcement information to other intelligence organizations, even within the DoD. The excesses of the DoD counterintelligence units during the 1960s and early 1970s made the military intelligence community reflexive to separate domestic intelligence and law enforcement information away from foreign intelligence. It partitioned off domestic intelligence and law enforcement information away from most foreign intelligence analysts and placed this information solely with counterintelligence units (the US Air Force Office of Special Investigation, the Naval Investigation Service (now the Naval Criminal Investigation Service), and the US Army's Criminal Investigation Division). To further raise this barrier, these units would look at domestic intelligence and law enforcement information generated in the US only if it related to threats against DoD installations, facilities and/or personnel. Intelligence Oversight policies were constructed and put into place to regulate and control the activities of military intelligence organizations and units, exacerbating the impression that there were severe restrictions on the use of domestic intelligence in national security intelligence products and analysis.

What we have seen, though, is that these instructions have clear guidelines that actually *allow* counterterrorism analysts to view, use and retain domestic intelligence and law enforcement information in their analyses. The instructions that govern Intelligence Oversight (such as DoD Instruction 5240.1R described above) set up the two step criteria to determine if the information can be used and disseminated to military counterterrorism

69 Second Report of the Markle Foundation Task Force on National Security in the Information Age, Appendix B, 22.

analysts if the connection to transnational terrorism can be made. What became the practice, however, was a distancing from this type of information, a more stringent application of the instructions than was required by law which in essence stopped domestic intelligence and law enforcement data from ever reaching counterterrorism analysts.

THIS PAGE INTENTIONALLY LEFT BLANK

V. PRESCRIPTIONS FOR CHANGE

A. FOCUS: 'NEED TO SHARE' AND 'NEED TO KNOW'

The key to the discussion of fusing law enforcement information with national security intelligence data is information sharing. This is one of the biggest challenges the Intelligence and Law Enforcement Communities must overcome: "We must not lose sight of the fact that the purpose of improving information analysis and sharing is to provide better information throughout the federal government, and ultimately also to state and local governments, the private sector, and our citizens, so that collectively we are all better prepared." [70] The debate has been framed recently as a change from a culture of a "need to know" to one of a "need to share" information. As has been described in the previous chapter, the greatest barrier to increased information sharing does not lie in the law; the legal basis for the sharing of law enforcement information with the Intelligence Community, and more specifically the USNORTHCOM J2, already exists. The greatest challenge, therefore, lies in the cultures of the institutions, organizations and their personnel that have created impediments to the free flow of information from one group to the next.

After the attacks of 9/11, no one in the Intelligence or Law Enforcement Communities will come out and say that they are against information sharing, or that they believe that sharing across agencies and communities is a bad idea. Everyone will say that increased information sharing is necessary for the agencies within the two communities to conduct all-source, fused analysis to accurately portray the current threat picture (i.e., "connect the dots"). However, the policies and actions of these agencies have not always run true to these stated desires. The ingrained cultural differences among the organizations have restricted the flow of information between agencies, and even between departments within the agencies themselves. There appears to be a reflexive unwillingness to share information between them. Agencies have created overly restrictive policies about what can be, or should be, shared internally and externally. The 9/11 Commission revealed that the FBI built such restrictive policies

[70] Government Accounting Office. *Statement by Comptroller General of the United States David M. Walker, 9/11 Commission Report: Reorganization, Transformation, and Information Sharing*. (3 August 2004. Order No. GAO-04-1033T), 5.

internal to their own handling of information, that the sharing of information inside the FBI became anathema and possibly damaging to one's career:

> … pressure from the Office of Intelligence Policy Review, FBI leadership, and the FISA Court built barriers between agents—even agents serving on the same squads. FBI Deputy Director Bryant reinforced the Office's caution by informing agents that too much information sharing could be a career stopper. Agents in the field began to believe—incorrectly—that no FISA information could be shared with agents working on criminal investigations.
>
> This perception evolved into the still more exaggerated belief that the FBI could not share *any* intelligence information with criminal investigators, even if no FISA procedures had been used. Thus, relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators. [71]

Many of these overly restrictive interpretations of policy were driven by the stated desire to protect sources and methods. From the law enforcement perspective, the holders of information believed that the release or sharing of information would compromise a source that could help in the conviction of a case; divulging information too early (before a case is complete) could somehow damage the case, or make the prosecution lose the case. For intelligence community members, the protection of sources and methods may mean the loss of a technical capability; if a target knows that they can be tracked electronically, the target may chose to use other sources of communication, thus effectively rendering collection against him more difficult or impossible. This may make obsolete multi-million dollar investments in technical collection equipment. It may also mean the loss of a human source; a compromise of a HUMINT source most likely equates to their (and quite possibly their family's) death.

The initial attempts at sharing information following the 9/11 attacks consisted of increased use of "tearline" reporting, redacting specifics from the intelligence so that sources and methods could not be determined from the content of the report. This method of information sharing is important and has increased the dissemination of reporting to those agencies that would not ordinarily see the specific reports; however, the overuse of redacted information and "tearline" reports has, in many circumstances,

71 National Commission on Terrorist Attacks Upon the United States, 79.

restricted the ability of analytic units such as the USNORTHCOM J2 to effectively analyze the current threat environment. Redacting has become a crutch allowing the originator of the report to remove critical details; what is being decided to be redacted appears arbitrary and capricious with no apparent rhyme or reason as to why they are removing the information. There is no legal basis for the redacting of information, and no community policy for what or how to redact critical elements form original source information so there is no specific standard from one agency to the next or from one reporting unit to another within an agency as to what and how to redact sources and methods. This creates uneven reporting that hinders analysis.

B. RECENT CHANGES TO INFORMATION SHARING

There have been several changes in 2004 to increase information sharing and to help reform the Intelligence Community. These changes will have a great impact on the USNORTHCOM J2 and its ability to provide all-source, fused intelligence products.

The 9/11 Commission reported its findings in August 2004 and recommended several changes to increase the capabilities of both the Intelligence and Law Enforcement Communities in counterterrorism intelligence and operations. The White House, based on these recommendations, issued several Executive Orders in August 2004 to implement significant changes within the Intelligence Community.

1. Executive Order 13354: National Counterterrorism Center

EO 13354 directed the creation of the National Counterterrorism Center (NCTC), the follow-on organization to the Terrorist Threat Integration Center (TTIC). The TTIC was created in 2003 and was designated to merge and analyze all threat information in a single location under the direction of the Director of Central Intelligence, and encompasses elements of the CIA's Counter Terrorist Center (CTC) and the FBI's Counterterrorism Division, along with elements of other agencies, including DoD and the Department of Homeland Security (DHS). TTIC's stated responsibilities were to

"integrate terrorist-related information collected domestically and abroad" and to provide "terrorist threat assessments for our national leadership." [72]

The NCTC was established in December 2004 and took over where the TTIC began. The NCTC is to "serve as the primary organization … for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting purely domestic counterterrorism information." [73] Section 1 of the order set forth the governing policy for both the Law Enforcement and Intelligence Communities with regards to counterterrorism in that "to the greatest extent consistent with applicable law, agencies shall give the highest priority to …the interchange of terrorism information among agencies [and] the interchange of terrorism information between agencies and appropriate authorities of States and local governments…". [74]

2. Executive Order 13356: Strengthening the Sharing of Terrorism Information to Protect Americans

EO 13356 directed intelligence agencies to share terrorism information related to terrorism and counterterrorism and designated the NCTC to lead the effort. It directed that those agencies conducting counterterrorism analysis or retaining terrorism-related information to "…promptly give access to the terrorism information to the head of each such agency that has counterterrorism functions, and provide the terrorism information … in accordance with the standards and information sharing guidance pursuant to this order…". [75] EO 13356 stipulates that the community needs to standardize collection and sharing requirements and procedures and to set forth guidelines on how to share the information.

---

[72] Richard Best, Jr., *Homeland Security: Intelligence Support* (Washington, D.C.: Congressional Research Service Report for Congress, 23 February 2004. Library of Congress Congressional Research Service, Order Code RS21283), 5.

[73] U.S. President. *Executive Order*. "National Counterterrorism Center." (27 August 2004). Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-5.html [20 February 2005].

[74] U.S. President. *Executive Order*. "National Counterterrorism Center."

[75] U.S. President. *Executive Order*. "Strengthening the Sharing of Terrorism Information to Protect Americans." (27 August 2004). Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html [20 February 2005].

The 9/11 Commission highlighted overclassification of information as being an impediment to information sharing. Specifically, the Commission reported that,

> Current security requirements nurture overclassification and excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of overclassifying information, though these costs—even in literal financial terms—are substantial. There are no punishments for *not* sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration. [76]

One of the problems raised by EO 13356 is the issue of the use (or overuse) or the "Originator Controlled" caveat. Over-classification of intelligence products and reports limit their usefulness and inhibits the ability of USNORTHCOM J2 analysts from using the information properly or from disseminating the analysis based on that material more freely. Many products are marked with the classification caveat "Originator Controlled," or "ORCON." The ORCON caveat signifies "that the intelligence cannot be distributed further without the originator's approval. This insistence on control is due in part to the fear that without such control, the information will be leaked or inadvertently released and a critical source or method will be compromised." [77] The net affect of the use (or misuse/over use) of the ORCON caveat is the limited distribution of information, especially to those that may be able to use the analysis to prevent an attack or, at the least, to prepare against one. EO 13356 requires "terrorism information to be shared free of originator controls, including, for example, controls requiring the consent of the originating agency prior to the dissemination of the information outside any other agency to which it has been made available, the maximum extent permitted by applicable law, executive order, or presidential guidance". [78]

---

76 National Commission on Terrorist Attacks Upon the United States, 417.

77 National Commission on Terrorist Attacks Upon the United States, Appendix B, iv.

78 U.S. President. *Executive Order*. "Strengthening the Sharing of Terrorism Information to Protect Americans."

3. Intelligence Reform and Terrorism Prevention Act of 2004

The U.S. Congress passed the *Intelligence Reform and Terrorism Prevention Act* in December 2004. This legislation acted upon the recommendations set forth in the 9/11 Commission's report and put into law many of the facets contained in the Executive Orders mentioned above, with an emphasis on information sharing and the creation of the NCTC. The Act also creates the position of the Director of National Intelligence (DNI), responsible for "managing and directing the collection, analysis, production and dissemination of national intelligence." [79]

The Act amends the definition of National Intelligence from the National Security Act of 1947. According to the Act,

> The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and (B) that involves—(i) threats to the United States, its people, property, or interests;(ii) the development, proliferation, or use of weapons of mass destruction; or ''(iii) any other matter bearing on United States national or homeland security. [80]

This feature of the Act is very important because it emphasizes that domestic intelligence or information derived from law enforcement sources can be critical to national security, thus it is of importance to USNORTHCOM J2 analysts. Given the context of today's environment, there is no separation between intelligence for Homeland Security and intelligence in support of Homeland Defense; they should be viewed together, complimenting each other. For USNORTHCOM to effectively carry out its mission to "deter, prevent, and defeat threats and aggression aimed at the United States," and thus fulfilling the command's role as the Department of Defense's lead command in homeland defense and homeland security, its Intelligence Directorate must have a global perspective as well as one that looks at home. The new definition in the Act clearly states that national intelligence "refer[s] to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States" and "any

79 U.S. Congress, House. *Intelligence Reform and Terrorism Prevention Act of 2004* (December 7, 2004, 108th Cong, 2d sess,. House report No. 108-796).

80 *Intelligence Reform and Terrorism Prevention Act of 2004*, 27.

other matter bearing on United States national or homeland security." This key feature is an important point: for the USNORTHCOM J2 counterterrorism analyst to be able to "connect the dots," it must see all the dots, not just some of them.

C. COUNTERTERRORISM ANALYSTS AND ANALYSIS

The challenge for the USNORTHCOM J2 is to support its Commander and the forces assigned to him as they carry out the command mission (deter, prevent, and defeat threats to the homeland) and balance this against the need (and requirement) to follow the law and protect the constitutional rights of US Persons and information collected during the course of legal domestic investigations. There are important standards that have to be met to release or share domestic intelligence information to USNORTHCOM J2, but they are not so onerous as to make sharing impossible; once these standards are met, there should be no reason or excuse to not share the information.

If information collected by law enforcement agencies is on individuals that are not US Persons, there are no restrictions for the information to be shared with the Intelligence Community, including USNORTHCOM J2 analysts. This information is considered foreign intelligence since the individual is a representative of a foreign country, not the US. The calculus changes if the person the information pertains to is considered to be a US Person. The emphasis for the need to share domestic intelligence and law enforcement information with USNORTHCOM J2 is the determination of the nexus between the individual(s) and transnational terrorism. USNORTHCOM 2 analysts are, by law, able to receive and retain information if there is a reason to believe the US Person is connected to transnational terrorism, international narcotics activity, foreign intelligence, or is directly threatening DoD installations, property or personnel. If this nexus exists, there is no reason for law enforcement or other intelligence organizations not to share this data with USNORTHCOM J2 analysts. The norm should be to share the information, not fall back on an overly restrictive interpretation of the protection of sources and methods: "Such a system implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate. The culture of agencies feeling they own the information they

gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information—to repay the taxpayers' investment by making that information available." [81]

1. "Reason to Believe"

The key, then, is the definition of "reason to believe" a nexus exists between the US Person and transnational terrorism. The challenge exists in that there is no set standard definition for "reason to believe" applied across all intelligence agencies and organizations. The originators of information apply their own standards to determine if the information is to be shared, thus creating an uneven application of the definition and in essence creating barriers to increase information sharing.

USNORTHCOM J2 defines "reason to believe" in the following way:

> a reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the belief, and must rest on facts and circumstances that can be articulated; "hunches or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence and counterintelligence work applied to the facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion while someone unfamiliar with foreign intelligence or counterintelligence work might not share a similar belief. [82]

This definition takes into consideration all applicable laws and governing Intelligence Oversight instructions to set forth a sound definition to guide the sharing of domestic intelligence and law enforcement information to military counterterrorism analyst. The Intelligence and Law Enforcement Communities must agree to a single standard for "reason to believe" and apply it evenly across all intelligence agencies and organizations for all types of information. This includes the DoD intelligence organizations and the applications of their procedures and policies, including Intelligence Oversight policies. The USNORTHCOM J2 definition for "reason to believe" could be used for that standard for the two communities.

---

[81] National Commission on Terrorist Attacks Upon the United States, 417.

[82] U.S. Northern Command, *Intelligence Oversight: Summary of EO 12333, DoD 5240.1, and DoD 5240.1-R* (Colorado Springs, CO, December 2004).

2. Diffusion of Skills

Information Sharing is not the only challenge faced by the Intelligence and Law Enforcement Communities. Much has been discussed about being able to "connect the dots," the ability to make logical sense out of disparate information:

> The problem is broader than just collecting and sharing information. It is the challenge of using information effectively, linking collection with sound and imaginative analysis derived from multiple perspectives and employing cutting-edge technology to support end-users, from emergency responders to Presidents. In other words, we need to mobilize information for the new era of national security we have entered. 83

The 9/11 attacks significantly changed the analytic landscape in the Intelligence Community. Prior to the attack, the focus of the Intelligence Community was primarily on nation-states and traditional Cold War analytic perspectives. Military intelligence looked specifically at the militaries of other countries and their potential capabilities against the US. Even during the rise of state-sponsored terrorism in the 1980s, the Intelligence Community did not shift its focus completely away from the Soviet Union; although counterterrorism analysis began as a discipline, the analytic emphasis remained elsewhere. The attacks by al-Qa'ida changed this focus to counterterrorism and almost every intelligence element applied manpower and resources against this problem.

Before 9/11, there were limited numbers of experienced counterterrorism analysts across the community. Noted terrorism expert Bruce Hoffman wrote that "People often treat intelligence organizations like a bottomless resource, but they are not. There are only so many CIA analysts to go around, and they are already stretched supporting the global war on terrorism abroad, U.S. efforts to stabilize Iraq and Afghanistan, crises in the Levant, and simmering threats in Iran, North Korea, and elsewhere." 84 With the advent of this refocusing of effort against terrorism, there has been a high demand for analysts. This increased demand did not equate to increased capability; although there are more analysts doing counterterrorism analysis today, they are generally inexperienced and not trained specific to this analytic field. The community was throwing analysts at

83 "Protecting America's Freedom in the Information Age." *Report of the Markle Foundation Task Force on National Security in the Information Age.* By Zoe Baird and James L. Barksdale, co-chairmen. (New York : The Foundation, October 2002), 9.

84 Bruce Berkowitz, "Intelligence for the Homeland," *SAIS Review, Vol. XXIV* (Winter-Spring 2004), 6.

the problem, transferring people from other disciplines against the counterterrorism challenge and expecting them to be "counterterrorism analysts." The 9/11 Commission identified this problem, stating "[t]he limited pool of critical experts—for example, skilled counterterrorism analysts and linguists—is being depleted. Expanding these capabilities will require not just money, but time." [85]

Because of this diffusion of talent, the Intelligence and Law Enforcement Communities must take advantage of *all* available agencies and organizations that have counterterrorism analysts to leverage these capabilities. USNORTHCOM J2 is one such organization that is focused on counterterrorism analysis.

> Washington,D.C., is important. It is where foreign and domestic information can often come together, a place where varieties of domestic, foreign, law enforcement, and military information can readily be combined, and where central coordination of a national community can be organized. If anything goes wrong, the spotlight will be on the President. It is up to him to set the expectations for the strong but balanced system we will need. ***But such a system cannot be based in or directed just from Washington. The President needs to set an expectation and design a system that is truly national and decentralized. [Emphasis added]***[86]

The greatest likely threat to the US today is not from other nation-states but from the threat of attack by transnational terrorists and terrorist groups. The distinct homeland defense and homeland security mission of USNORTHCOM demands that its intelligence analysts focus on terrorism and counterterrorism analysis. USNORTHCOM J2 was designed and manned with this problem set in mind, focused foreign intelligence from around the world as well as domestic intelligence and law enforcement information generated in the US when a nexus with transnational terrorism is established. The organizational structure and manning of the USNORTHCOM J2 was developed with an eye toward the challenges inherent in counterterrorism analysis within both the Intelligence and Law Enforcement Communities that have been articulated in this thesis. The USNORTHCOM J2 has a good mix of experienced counterterrorism analysts (master level experience), personnel trained in other areas of expertise but knowledgeable of analysis skills (journeyman level experience), and individuals new to both

85 National Commission on Terrorist Attacks Upon the United States, 401.

86 "Protecting America's Freedom in the Information Age." *Report of the Markle Foundation Task Force on National Security in the Information Age*, 10.

counterterrorism and to analysis (apprentice level experience). This mix of analytic skills and experience ensures that the USNORTHCOM J2 can immediately provide quality counterterrorism analysis and support analysis at other organizations and agencies in both the Intelligence and Law Enforcement Communities today. At the same time, this mix of experienced analysts with apprentice level newcomers provides for the development of analytic skills for the new analysts, ensuring the continued training, education and mentoring of the next generation of counterterrorism analysts.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. *"A MORE PERFECT UNION…"* THE FUTURE FOR USNORTHCOM INTELLIGENCE

A. BRINGING LAW ENFORCEMENT INFORMATION TO USNORTHCOM J2

The tragedy of 9/11 forced the Intelligence and Law Enforcement Communities to reevaluate their information sharing practices. The nature of the threat today is such that there cannot be a dichotomy between the two communities with regard to information; all available relevant intelligence information from one community must be shared with the other in order to generate the most comprehensive analysis of the potential threat to our homeland. It is essential for all available information, whether it is from the Law Enforcement Community or the Intelligence Community, to be freely shared to every counterterrorism analyst. This has become the analytic imperative because "[i]ntelligence and law enforcement are becoming increasingly intertwined. Few doubt that valuable insights can derive from close correlation of information from differing intelligence and law enforcement sources." [87]

USNORTHCOM was created to provide the President and the Secretary of Defense a single point of contact to marshal military forces against threats to the homeland; to be the military's primary leader in homeland defense and lead when called upon for homeland security. As the DoD's (and the country's) leader in homeland defense, its intelligence unit, the USNORTHCOM J2, must have access to all available information to provide the Commander and his assigned forces the best analysis of the threat. Patrick Hughes, Under Secretary for Intelligence Analysis and Infrastructure Portection for the Department of Homeland Security and former Director of the Defense Intelligence Agency and stated in 2002, "The key to the success of the people that do the work of intelligence is access to information.

87 Best, *Intelligence to Counter Terrorism: Issues for Congress*, 19.

Intelligence sharing across the Intelligence Community, Federal, State, and local, is vital. Without open and expeditious sharing of intelligence, I believe this endeavor will fail." [88]

B. KEY POINTS FOR INFORMATION SHARING WITH USNORTHCOM J2

This thesis has tried to address several challenges to the sharing of information between the Law Enforcement Community and the Intelligence Community, and more importantly, to the counterterrorism analysts in the USNORTHCOM J2. These challenges, and in some cases misconceptions, need to be addressed and overcome so that *all* counterterrorism analysts in the Intelligence Community, and more specifically those in the USNORTHCOM J2, can have access to all available information, both foreign and domestic intelligence as it relates to transnational terrorism and threats to the homeland, so that all-source analysis can be produced and disseminated to senior decision makers.

1. Develop the "Need to Share"

The environment for sharing information across the two communities must be fostered. Cultural challenges must be overcome, engraining the spirit of "need to share" and not creating barriers based on an abstract and outdated concept of "need to know." The protection of sources of methods should be paramount and always considered when deciding what needs to be shared with all levels of government and across the communities, but it should not become a barrier for, or an excuse in not sharing intelligence.

2. Properly Define the "Reason to Believe"

Part of the two step process to determine what domestic intelligence and law enforcement information can be passed to military intelligence organization such as USNORTHCOM J2 is the determination of a nexus between a US Person and

88 U.S. Congress, Senate. Committee on Governmental Affairs. *Testimony of Lt. Gen Patrick M. Hughes, U.S. Army (Ret.), former Director (1996-1999), Defense Intelligence Agency (DIA), a review of the relationship between a Department of Homeland Security and the Intelligence Community Hearings*. (107th Cong., 2d sess., 2002).

transnational terrorism. The key to this determination is the definition of a "reason to believe" a US Person has a connection with terrorism. A uniform definition, such as the one used by USNORTHCOM J2, needs to be adopted across both the Intelligence and Law Enforcement Communities so that an evenly applied standard can be used to assist information sharing.

3. Stop the "Diffusion of Skills" by Incorporating USNORTHCOM J2

The refocusing of much of the Intelligence Community towards counterterrorism analysis has created a diffusion of analytic talent. This strain on available analytic resources may result in inaccurate and not well-developed analysis. The USNORTHCOM J2 brings to the Intelligence Community an established analytic capability. Analysis is the primary product of the organization and its primary contribution to both homeland security and homeland defense. The USNORTHCOM J2 can provide high quality and experienced counterterrorism analysts to support the analytic efforts of the rest of the Intelligence and Law Enforcement Communities today. It can only support these two communities, however, if it has access to all available information, including domestic intelligence and law enforcement information. Only then can a true all-source, fused intelligence product be created.

4. The Department of Homeland Security and the National Counterterrosim Center

This thesis has concentrated primarily on the need to share law enforcement information with counterterrorism intelligence analysts, focusing primarily on those analysts at USNORTHCOM. Although implied from the larger context for the need to share information with *all* organizations focused on counterterrorism, the thesis did not try to specifically address the information needs of the Department of Homeland Security (DHS). It must be mentioned, however, that DHS also needs to be able to receive both traditional and non-traditional intelligence information in order to fuse it into one coherent analytic product. DHS has a formal liaison relationship with USNORTHCOM, but has only informal analyst-to-analyst relationships each others intelligence directorates.

As was mentioned in Chapter V, the NCTC was created as a follow on organization to the TTIC to integrating and fusing all available counterterrorism intelligence in support of the President and the national leadership inside Washington, DC. USNORTHCOM J2 has developed direct informal relationships with the NCTC at senior leadership level as well as the analyst-to-analyst level. In addition, USNORTHCOM J2 has a direct liaison representative on the DIA's Joint Intelligence Task Force – Combating Terrorism (JITF-CT) Force Protection Unit which is a department within the NCTC.

The question remains unanswered: which agency should be the lead for homeland security intelligence for the entire country? DHS's Intelligence Analysis and Infrastructure Protection Division (IAIP) was conceived and chartered with that purpose in mind, but is the organization itself and the two communities that hold the information (Intelligence and Law Enforcement) structured to make this happen? Has the creation of first the TTIC, and now its successor the NCTC, made the concept of the IAIP obsolete before it has a chance to become established? Should the FBI retain domestic intelligence responsibilities in addition to its law enforcement roles and missions? These questions although worthy of in-depth analysis and research, are beyond the scope of this paper but remain important in future discussions of homeland security intelligence. Do we have it right or can we do it better? USNORTHCOM J2 remains engaged with each of these agencies at the analyst level, but it may need to establish more permanent positions to further the coordination and cooperation between USNORTHCOM and those agencies that have domestic intelligence analytic responsibilities.

C. FINAL THOUGHTS

Many changes and reforms have been implemented since the attacks 9/11, including changes made by specific agencies trying to create change of their own practices and procedures, reforms dictated to the two communities by the Executive Branch, and legislation passed by Congress instituting reforms. However, these changes will take time to develop and imbed themselves into the cultures of the two communities and the organizations that make them up. As the changes become an integral part of day-to-day activity and transform the Intelligence and Law Enforcement Community's culture

and relationships, it it stands to reason that the rest of the Intelligence Community take advantage of the creation and readily available pool of counterterrorism analysts at the USNORTHCOM J2 by increasing their access to non-traditional intelligence. The freeing up of more information and letting it flow out of the FBI and the rest of the Law Enforcement Community to USNORTHCOM J2 analysts will allow the critical job of all-source, fusion analysis to grow and continue while these changes to the FBI culture and organization take hold. This allows the most important mission of fused counterterrorism analysis of all available information to continue, to be able to detect, deter and prevent terrorist acts from happening, before they occur.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Berkowitz, Bruce. "Intelligence for the Homeland," SAIS Review, Vol. XXIV, Winter-Spring 2004: 1-6.

Best, Richard, Jr. *Homeland Security: Intelligence Support*. Washington, D.C.: Congressional Research Service Report for Congress, 23 February 2004. Library of Congress Congressional Research Service, Order Code RS21283.

Best, Richard, Jr. *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.* Washington, D.C.: Congressional Research Service Report for Congress, 3 December 2001. Library of Congress Congressional Research Service, Order Code RL30252.

Best, Richard, Jr. *Intelligence to Counter Terrorism: Issues for Congress*. Washington, D.C.: Congressional Research Service Report for Congress, 27 May 2003. Library of Congress Congressional Research Service, Order Code RL31292.

"Creating a Trusted Network for Homeland Security." *Second Report of the Markle Foundation Task Force on National Security in the Information Age.* By Zoe Baird and James L. Barksdale, co-chairmen. New York: The Markle Foundation, 2003.

Cumming, Alfred, and Todd Masse. *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress*. Washington, D.C.: Congressional Research Service Report for Congress, 6 April, 2004. Library of Congress Congressional Research Service, Order Code RL32336.

Diamond, John. "Panel Now Faces Difficult Task of Finding Fixes," *USA Today,* 15 April 2004.

Doyle, Charles. *The USA PATRIOT Act: A Sketch*. Washington, D.C.: Congressional Research Service Report for Congress, 18 April 2002. Library of Congress Congressional Research Service, Order Code RS21203.

Duffy, Michael. "How To Fix Our Intelligence," *Time,* 26 April 2004.

Gleghorn, Todd E. *Exposing the Seams: The Impetus for Reforming U.S. Counterintelligence.* Monterey, Naval Postgraduate School, 2003.

Government Accounting Office. *Statement by Comptroller General of the United States David M. Walker, 9/11 Commission Report: Reorganization, Transformation, and Information Sharing.* 3 August 2004. Order No. GAO-04-1033T.

Isaacson, Jeffrey A. and Kevin M. O'Connell. "Beyond Sharing Intelligence, We Must Generate Knowledge." *Rand Review* 26, No. 2 (Summer 2002): 48-50. Available online at http://www.rand.org/publications/randreview/issues/rr.08.02/intelligence.html [20 February 2005].

Ley, Michael P. "From the Editor," *Military Intelligence Professional Bulletin,* Jul-Sep 2002: 2.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy.* Washington, D.C.: CQ Press, 2003.

Moyer, Shawn P. *Creating a Mix of Spooks and Suits: A New Role for Intelligence.* Monterey, Naval Postgraduate School, 2003.

National Commission on Terrorist Attacks Upon the United States, Thomas H. Kean and Lee H. Hamilton. *The 9/11 Commission Report.* Washington, D.C.: 2004.

Office of Homeland Security, *National Strategy for Homeland Security*. Washington, D.C.: GPO, 2002.

"Protecting America's Freedom in the Information Age." *Report of the Markle Foundation Task Force on National Security in the Information Age.* By Zoe Baird and James L. Barksdale, co-chairmen. New York: The Markle Foundation, October 2002.

Senior Intelligence Official. 2004. Interview by author, October 2004.

Smith, Regan K. "Military Module," *Military Intelligence Professional Bulletin,* Jul-Sep 2002: 6.

Treverton, Gregory F. *Intelligence, Law Enforcement, and Homeland Security.* Washington, D.C.: The Century Foundation, 21 August, 2002.

Treverton, Gregory F. "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons," *Intelligence and National Security, Vol 18., No. 4 (Winter 2003)*: 121-140.

Treverton, Gregory F. *Reshaping National Intelligence for an Age of Information.* Cambridge, Cambridge University Press. 2001

U.S. Congress, House. *Intelligence Reform and Terrorism Prevention Act of 2004*, December 7, 2004, 108th Cong, 2d sess,. House report No. 108-796.

U.S. Congress, Senate and House. Permanent/Select Committees on Intelligence. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 with additional views.* 107th Cong., 2d sess., 2002.

U.S. Congress, Senate. Select Committees on Intelligence. *Statement by Director of Central Intelligence George J. Tenet before the Senate Select Committee on Intelligence on the "Worldwide Threat 2001: National Security in a Changing World" (as prepared for delivery)*, 107th Cong., 7 February 2001.

U.S. Congress, Senate. Committee on Governmental Affairs. *Testimony of Lt. Gen Patrick M. Hughes, U.S. Army (Ret.), former Director (1996-1999), Defense Intelligence Agency (DIA), a review of the relationship between a Department of Homeland Security and the Intelligence Community Hearings.* 107th Cong., 2d sess., 2002.

U.S. Department of Defense, DoD Instruction 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons.* Washington, D.C.: Government Printing Office, December 1982.

U.S. Northern Command, *Intelligence Oversight: Summary of EO 12333, DoD 5240.1, and DoD 5240.1-R.* Colorado Springs, CO, December 2004.

U.S. Northern Command, *U.S. Northern Command's Strategic Vision*, Colorado Springs, CO, 2003.

U.S. Northern Command, *Sustained Vigilance: Intelligence Support for North America's Homeland Defense.* Colorado Springs, CO, 2003.

U.S. President. *Executive Order*. "National Counterterrorism Center." (27 August 2004). Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-5.html [20 February 2005].

U.S. President. *Executive Order*. "Strengthening the Sharing of Terrorism Information to Protect Americans." (27 August 2004). Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html [20 February 2005].

U.S. President. *Executive Order*. "United States Intelligence Activities, Executive Order 12333," Federal Register 46, no. 59941 (4 December 1981). Available [Online]: http://www/fas.org/irp/offdocs/eo12333.htm [20 February 2005].

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Paul Stockton, Director
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

4. Michael Noll,
   Director of Intelligence
   NORAD/ U.S. Northern Command
   Colorado Springs, Colorado

5. John Schoch
   NORAD/ U.S. Northern Command
   Colorado Springs, Colorado