United States Military Intelligence Support to Homeland Security

A Monograph

by

Major James Lillard Wilmeth IV

United States Army

MENS EST CLAVIS VICTORIA

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

First Term AY 03-04

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major James Lillard Wilmeth IV

Title of Monograph: United States Army Military Intelligence Support to Homeland Security

Approved by:

_____   Monograph Director
COL Ramon Valle, IN

_____   Director,
Kevin C.M. Benson, COL, AR   School of Advanced
                                              Military Studies

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

Report Documentation Page			*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, 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. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **26 MAY 2004**	2. REPORT TYPE	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **United States military intelligence support to homeland security**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **James Wilmeth, IV**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army School for Advanced Military Studies,250 Gibbon Ave,Fort Leavenworth,KS,66027**	8. PERFORMING ORGANIZATION REPORT NUMBER **ATZL-SWV**

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

The terrorist attacks of September 11, 2001 identified a need for a better domestic intelligence capability. In order to prevent another attack on the homeland, one must first identify any failures in the current doctrine, theory, and practice regarding intelligence support to homeland security. This involves not only military intelligence, but also the various domestic and international intelligence organizations that maintain some degree of jurisdiction over intelligence collection, analysis, and dissemination. This monograph outlines how the new operational environment, current laws, regulations, and policies effecting domestic intelligence collection, and advocates establishing state level intelligence centers that rely heavily on the Reserve Component and which would enable better intelligence sharing between the law enforcement and intelligence communities at the local level.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**1**	**66**	

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

Abstract

UNITED STATES ARMY MILITARY INTELLIGENCE SUPPORT TO
HOMELAND SECURITY by Major James L. Wilmeth IV, United States Army, 61 pages.

       The terrorist attacks of September 11, 2001 identified a need for a better domestic
intelligence capability. In order to prevent another attack on the homeland, one must first identify
any failures in the current doctrine, theory, and practice regarding intelligence support to
homeland security. This involves not only military intelligence, but also the various domestic and
international intelligence organizations that maintain some degree of jurisdiction over intelligence
collection, analysis, and dissemination. This monograph outlines how the new operational
environment, which includes the establishment of a new combatant command and a significant
reorganization of the federal government, effects domestic intelligence collection. It also
addresses current laws, regulations, and policies effecting domestic intelligence collection, and
uses several case studies to outline current practice.

       This monograph advocates establishing state level intelligence centers that rely heavily
on the Reserve Component and which would enable better intelligence sharing between the law
enforcement and intelligence communities at the local level. The information collected at these
various facilities can be analyzed, deconflicted, and disseminated at a national level analytic
center that mirrors or even supplants existing INSCOM capabilities. Finally, this can be done
with little or no changes to existing laws, regulations, and policies. It will, however, require the
public and the intelligence community to reconsider how military intelligence supports to
domestic intelligence activities.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

The unprecedented terrorist attacks of September 11, 2001 forever changed many aspects of American life. Some of the changes were overt, visible, and subject to open and honest debate among politicians and the public. Other changes, however, were and continue to be less visible, either due to classification, a lack of interest, or simply an inability to understand how laws or regulations may affect United States citizens. One such change involves the intelligence community and how the Department of Defense (DoD) integrates within it with respect to homeland security.

Prior to September 11, 2001, the Army in general, and the military intelligence community in particular, were looking for ways to consolidate resources while maintaining efficiency. Part of this consolidation included centralizing strategic, or echelons above corps (EAC), intelligence capabilities at one or two domestic locations, vice maintaining an organic capability at every geographic combatant command. As an example, the 470th Military Intelligence (MI) Brigade, assigned to United States Army Southern Command (USARSO) was deactivated; its mission subsumed into the 513th MI Brigade, whose mission also included United States Army Central Command (USARCENT). There was a recognized risk, but given the strategic environment of the time, it was a risk that the Department of the Army was willing to accept.

That rationale disappeared after the devastating terrorist attacks on the United States homeland. The Major Army Command responsible for EAC MI, the Intelligence and Security

Command (INSCOM), recognized that since the Global War on Terrorism was global, each of the geographic combatant commands simultaneously required the unique capability provided by the EAC MI brigades (and groups).[1] As a result, the wheels were put in motion to re-establish the 470th MI Brigade capability at USARSO.

There was also a significant amount of discussion on how INSCOM could support a new combatant command, the United States Northern Command (NORTHCOM). In fact, INSCOM established the requirements necessary to provide intelligence support to NORTHCOM in the Army's Total Army Analysis (TAA) process in late 2001 (TAA 09).[2] However, the requirements levied for support to NORTHCOM went un-resourced. The feedback indicated that the requirements were not adequately justified. There was also an underlying concern reference army intelligence operating within the continental United States. This monograph will address both of these concerns, ultimately answering the question of whether EAC Intelligence, specifically counterintelligence, can support homeland security.

---

[1] The INSCOM Mission Statement reads, "Synchronize the operations of all INSCOM units to produce multi-disciplined, operationally relevant intelligence in support of the Department of the Army, Army Service Component Commander, and the intelligence community requirements. Current operational focus: Operation Iraqi Freedom, Phase IV support (hostile activity trend and pattern analysis), Global War on Terrorism, foreign intelligence services, and computer network operations." (on-line); available from www.inscom.army.mil; internet; accessed on January 13, 2004.

[2] Total Army Analysis (TAA) is "the acknowledged and proven method for explaining and defending Army force structure." It is further defined as "a multi-phased force structuring process, consisting of both qualitative and quantitative analysis designed to develop the Modification Table of Organization and Equipment and the Table of Distribution and Allowances 'generating' forces necessary to sustain and support the divisional and non-divisional combat forces delineated in the Defense Planning Guidance, the Illustrative Planning Scenario, and The Army Plan". Department of the Army, *How the Army Runs; A Senior Leader Reference Handbook 2001-2002*, Carlisle Barracks, PA: United States Army War College, 2001.

Research Question and Methodology

This monograph will answer the question of whether or not the mission of homeland security, which is largely a domestic mission, can and/or should be supported by EAC intelligence capabilities. First, it will examine EAC intelligence and how it relates to each geographic combatant command. Subsequently, the monograph will explore the new Department of Homeland Security (DHS) and how it fits into or even shapes the new operational environment. Additionally, it will explain how the new NORTHCOM relates (command and otherwise) to the DHS. This will be accomplished by relating doctrine and theory to the formerly disparate missions of homeland security and Army intelligence collection. Finally, the monograph will analyze the above information, contrasting it with several case studies, including the example of Joint Task Force 6, and will offer a conclusion.

As this topic is relatively new, most of the sources will be articles, research projects at various military and civilian colleges, and of course the quickly evolving national policies. The first group of sources is the laws, policies, regulations, and doctrine regarding the establishment of the DHS, the Patriot Act, and how these affect the National Security Strategy and the National Strategy for Homeland Security. This involves not only researching the actual documents (laws, regulations, etc.), but also any new interpretations of them. Closely related to these are the many policy statements and speeches made by the President and those within his administration. In many instances, these speeches fill the gap in the absence of written guidance. One is often forced to dissect these speeches, articles, or interviews for direction and intent. As such, they become very important to formulating strategy.

Certain criteria will be used in order to effectively address the question of using military intelligence within the construct of homeland security. These criteria include whether certain measures are feasible, acceptable, and suitable. In order to be feasible, the monograph will determine if present laws, policies, and regulations render it impossible to collect, analyze, and

disseminate intelligence for a predominantly domestic organization such as the DHS. To be acceptable, some policies, procedures, or laws might have to be changed. Finally, in order to be suitable, any negative perception of collecting domestic intelligence must be addressed. This monograph will discuss the benefits versus the risks of creating a domestic intelligence organization.

Chapter Two of this monograph will outline the newly evolving operational environment within which an intelligence construct will operate. Given the context of the new strategic environment, which, unlike past generations, has taken the form of a direct threat to the United States of America's homeland, this chapter will focus on the intelligence support to the mission of homeland security. In order to do so, the chapter will first provide a background on EAC intelligence and counterintelligence support to the geographic combatant commands, which will include how the commands are structured and how each has tailored and dedicated intelligence support. Chapter Two will also provide a brief history of the development of both the DHS and the new combatant command, NORTHCOM. The chapter will include the past and current relationships to other organizations within the ubiquitous 'Intelligence Community', such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA). It is important not only to understand how the DHS and NORTHCOM were born, but also to understand the unique national security environment within which they were proposed.

Chapter Three will outline the doctrinal application of any domestic intelligence and counterintelligence activities in support of NORTHCOM. It will accomplish this by first outlining current counterintelligence doctrine, focusing on support to existing geographic combatant commands, and highlighting some initiatives and organizations currently providing intelligence support for homeland security, albeit limited. Additionally, Chapter Three will outline the specific Executive Order and supporting DoD and Army regulations that impact any type of domestic military intelligence.

Chapter Four of this monograph will discuss theory, focusing on whether there is a shift towards the acceptance of domestic military intelligence support to NORTHCOM. The fact that the normally glacially slow process of transforming the structure of the Federal Government and the DoD was affected in an extremely rapid manner is important in and of itself. It displayed a singular sense of purpose that was forged through the lens of an unprecedented attack on the United States. The relatively strong support throughout the halls of Congress and in the public domain may not last. The American public, and therefore its Representatives on Capitol Hill, has an amazing ability to 'self-right' after a tragedy. This, while a laudable attribute, will make it more and more difficult to create and/or maintain a domestic intelligence capability, as the public has a healthy wariness of a central government, especially when it comes to possible or perceived infringements on personal privacy.

Specifically, Chapter Four will focus on the current paradigm of public perception; one that shuns any type of military involvement in domestic intelligence operations. It will subsequently use two case studies to outline that the public perception is just that; a perception. There are successful organizations, both predominantly military and government, which use military intelligence capabilities for domestic missions. Finally, Chapter Four will suggest a paradigm shift by citing two recommendations on how current organizations or capabilities can be augmented in order to adequately support homeland security.

Chapter Five contains conclusions and recommendations. It will summarize the analysis conducted throughout the monograph and present a cohesive argument responding to the research question of whether EAC Intelligence, specifically counterintelligence, can support homeland security. Chapter Five will also present several recommendations. It will do this by analyzing the viability of domestic military intelligence support to the mission of homeland security by using three criteria questions. First, given present laws, regulations, and policies, is it even possible to collect, analyze, and disseminate intelligence for a predominantly domestic organization such as the DHS or NORTHCOM? When discussing any type of intelligence

support to NORTHCOM, or any domestic military involvement, many blindly cite Posse

Comitatus as an impenetrable barrier, preventing any military involvement.[3] While the law

presents significant obstacles to domestic intelligence activities, it does have flexibility. In fact,

many of the restrictions on intelligence activities are found in Executive Orders and the

subsequent Army and DoD Regulations that implement those Executive Orders.[4] This chapter

will discuss some of the constraints, as well as how the new United States of America Patriot Act

affects them.[5] In answering the first question, the reader will have an idea of what the law was

designed to do, its actual restrictions, and the traditional restrictions by which the military has

abided for some time.

The second question asks what policies, procedures, or laws must be changed, if any, in

order for an effective EAC intelligence organization to support the DHS and NORTHCOM?

Finally, the third question addresses the fact that, despite the laws, policies, and regulations, there

---

[3] Posse Comitatus, or Title 18 of the United States Code, Section 1385, States, "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both." The Navy and the Marine Corps were subsequently included under this act. In other words, the Posse Comitatus Act prohibits the Department of Defense from conducting police work. United States NORTHCOM website; (on-line); available from http://www.northcom.mil/index.cfm?fuseaction=news.factsheets&factsheet=5; internet; accessed on February 10, 2004.

[4] Executive Order 12333, United States Intelligence Activities outlines intelligence activities with respect to United States Persons. Army Regulation 381-10, Department of Defense Directive 5240.1 and Department of Defense Regulation 5240.1R implement the Executive Order. These will be fully discussed in Chapter Five of this monograph. Smith, Regan K. *Homeland Security: An Intelligence Oversight Perspective*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, pp. 5-8.

[5] The United States of America Patriot Act of 2001, signed by President Bush on October 26, 2001, loosens certain law enforcement restrictions and allows the intelligence community and the law enforcement community to share certain information. This, too, will be discussed at length in Chapter Five. Ibid.

will be a major perception challenge with respect to collecting intelligence within the United

States. What might the benefits be versus the risks of creating such an organization?

Terms and Definitions

One of the challenges with any discussion regarding a relatively new concept such as

military intelligence support to homeland security is a common definition of terms. There are

many different definitions of 'intelligence', 'counterintelligence', 'homeland security', and even

'homeland defense'. This monograph will defer to the joint definition when possible. Joint Pub

1-02 defines intelligence as "information and knowledge about an adversary obtained through

observation, investigation, analysis or understanding."[6] It also defines intelligence as a "product

resulting from the collection, processing, integration, analysis, evaluation, and interpretation of

available information concerning foreign countries or areas."[7] The second definition connotes a

polished product vice raw information. It is also the Army definition out of FM 34-60,

Counterintelligence dated October 3, 1995.[8]

The Joint Pub defines the term 'information' as "facts, data, or instructions in any

medium or forum", or, "the meaning that a human assigns to data by means of the known

conventions used in their representation."[9] Neither of these definitions is very clear. The Army

better defines information, with respect to intelligence, as "unevaluated material of every

description that may be used in the production of intelligence".[10] In general terms, information is

---

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

[7] Ibid

[8] Department of the Army, FM 34-60, Counterintelligence. October 3, 1995.

[9] Ibid

[10] Department of the Army, Field Manuel 34-1, Intelligence and Electronic Warfare Operations, 27 September 1994.

comprised of the raw data that, when effectively analyzed, collated, and disseminated, becomes intelligence. It is the bedrock upon which good intelligence relies. Therefore, the key is to provide analysts, wherever they are, and whomever they work for, with accurate, reliable, and timely information. The analysts, in turn, produce the intelligence product.

Counterintelligence, on the other hand, is defined as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities."[11] The key in this definition is the caveat referencing international terrorist activities. This makes terrorism a specified function of counterintelligence.

Homeland defense and homeland security are two more crucial definitions important to understand, as they tend to be used interchangeably. They are, in fact, very different terms. Homeland defense is the "protection of United States territory, domestic population, and critical infrastructure against military attacks emanating from outside the United States."[12] In this regard, homeland defense represents no change from the military's so called traditional role of protecting the country. However, within the context of the new operational environment, which will be discussed at length in the following chapter, homeland defense takes on a slightly different

---

[11] Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 199

[12] As the definitions for both homeland defense and homeland security are not in Joint Pub 1-02, these definitions were taken from the United States Northern Command Homepage (on-line); available from http://www.northcom.mil/index.cfm?fuseaction=s.homeland; accessed on February 9, 2004.

connotation. Instead of the military attacks emanating from the likes of a monolithic Soviet Union, they can now come from trans-national, non-state terror organizations.

Homeland security, on the other hand, is the "prevention, preemption, and deterrence of, and defense against aggression targeted at the United States territory, sovereignty, domestic population and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies."[13] This does not necessarily fall within the traditional role of the military. When the military does participate in homeland security efforts, it is generally in a supporting role. In short, homeland security is prevention from within the United States and starts at the local and state level. Homeland defense seeks to address the threats before they can affect the homeland. Given the new operational environment, which will be explained in detail in the next chapter, perhaps a part of the prevention piece, no matter how it is classified, is an intelligence effort directed against some of these trans-national terrorist organizations, wherever they may be.

Summary

Chapter One has provided a series of important definitions required to address any intelligence support for homeland security. The next chapter will use these definitions and outline the new operational environment. It will do this by explaining how intelligence supports combatant commands around the world, as well as describing the important changes in the Federal Government that came about as a result of the September 11, 2001 terrorist attacks.

---

[13] Ibid.

CHAPTER TWO

OPERATIONAL ENVIRONMENT

The operational environment for and within which NORTHCOM will be responsible is singularly unique with respect to other combatant commands. First and foremost, a large portion of NORTHCOM's geographic responsibility is the United States itself.[14] Clearly, in an open and democratic society that values personal privacy and is traditionally extremely wary of domestic military and intelligence activities, there are obstacles, both actual and perceived, that must be overcome.

The previous chapter outlined the differences between homeland defense and homeland security. This construct is very useful against traditional threats to the United States. It becomes a bit more clouded when the threat is comprised of trans-national terror organizations that do not recognize or respect the border of the United States. These nebulous organizations are difficult to identify, locate, and track, hence their deadly effectiveness. When a military attack is coordinated between Hamburg, Germany, Boston, Massachusetts, and a cave in Afghanistan, the line between defense and security becomes vague. This monograph does not seek a revised definition of homeland defense or homeland security, but rather an enhanced understanding of these two terms. The first step towards ensuring the security of the homeland is to identify these murky and ambiguous terror groups, wherever they are.

---

[14] The United States NORTHCOM will be discussed at length later in this chapter. United States NORTHCOM website (on-line); available from www.northcom.mil/index.cfm?fuseaction=s.who_mission; internet; accessed on January 14, 2004.

Before any discussion of intelligence support to homeland security can occur, it is important to understand several concepts. First, one must understand how the current geographic combatant commands obtain intelligence support. Additionally, it is important to note that each of the commands has a slightly different structure and relationship, based upon the specific and unique requirements of that command. This, of course, connotes that an intelligence structure built for NORTHCOM may not resemble any of the existing organizations or have the same organizational relationships. Second, it is important to understand the short history of both the DHS and NORTHCOM, and how both have evolved since September 11, 2001. These relatively large federal government undertakings occurred in a remarkably short time; so short, in fact, that many people may not completely understand their mission or structure.

Intelligence Support to Combatant Commands

To understand how an EAC intelligence capability can support the new combatant command of NORTHCOM, it is first essential to understand how existing geographic combatant commands receive intelligence support. Currently, each geographic combatant command, through its Army Service Component Commander (ASCC), receives important intelligence support from either an INSCOM Theater Intelligence Brigade (TIB) or a Theater Intelligence Group (TIG).[15] Additionally, INSCOM is the Army's input, and therefore link, into and from the

[15] There are currently four TIB/Gs supporting the OCONUS Unified Commands through the respective ASCC. As indicated, the 470th MI Group supports USARSO, the 513th MI BDE supports USARCENT, the 66th MI Group supports United States Army Europe (USAREUR), and the 500th MI Group supports United States Army Pacific (USARPAC). Additionally, the 501st MI BDE supports the Eighth United States Army in Korea. (On-line); available from www.inscom.army.mil; accessed on January 13, 2004.

national intelligence architecture. For instance, the 704th MI Brigade at Ft. Meade, Maryland is

the plug into the National Security Agency (NSA). There are several Signals Intelligence

(SIGINT) units around the world that collect data that is fed into the NSA. The Intelligence and

Security Command also has the 902nd MI Group, a strategic level, worldwide counterintelligence

organization, also stationed at Ft. Meade, Maryland. The 902nd MI Group has two

counterintelligence battalions; one focused overseas and one focused domestically. The domestic

focus, however, is largely relegated to counterintelligence or counter-espionage cases involving

military personnel.[16]

Each worldwide INSCOM organization is structured differently, tailored to its specific

theater. They each collect, analyze, and disseminate intelligence to the ASCC and his decision

makers. More specifically, with respect to counterintelligence support when overseas, the

INSCOM units actively liaison with host nation authorities, from local, through state and

national, to international police and intelligence organizations in order to provide the commander

on the ground better situational awareness. For instance, if there were to be a large anti-American

rally in downtown Heidelberg, Germany, the counterintelligence detachment from the 66th MI

Group would receive that information from the local city authorities, the state police, or the

Militaerischer Abschirmdienst.[17] Depending on the source, this information may not be provided

---

[16] The mission statement for the 902nd MI Group reads, "The 902nd MI Group conducts
counterintelligence activities in support of Army Commanders and to protect Army forces, secrets, and
technologies by detecting, identifying, neutralizing and exploiting foreign intelligence services and
international terrorist threats." (On-line); available from www.inscom.army.mil/902nd/index.asp; accessed
on January 13, 2004.

[17] The Militaerischer Abschirmdienst, more commonly referred to as the MAD, is a
counterintelligence organization in the German Armed Forces that provides all Armed Services CI support.

to the Provost Marshal's office, despite the presence of a German police liaison officer. This

critical information is then used by the local commander in various ways, including adjusting the

threat condition (THREATCON) level or issuing a general security warning. [18]

In short, the INSCOM organizations in each of the geographic combatant commands

provide the ASCC with collection, analysis, and dissemination capabilities. These

brigades/groups serve as a two-way bridge between national level (strategic) intelligence and the

front line war fighter, providing the national decision making authorities with intelligence from

the theater using organic collection assets. Additionally, the INSCOM units incorporate national

level intelligence by virtue of unique access to interagency databases in the analysis they provide

to the local commanders.

Department of Homeland Security

On September 20, 2001, just nine days after the terrorist attacks on the United States,

President George Bush, in an address to Congress, announced the creation of an Office of

Homeland Security (OHS), and appointed the governor of Pennsylvania, Tom Ridge, as its first

Director. On October 8 of the same year the President signed the Executive Order creating the

OHS and swore in Governor Ridge as the Assistant to the President for Homeland Security. The

---

[18] The THREATCON program is a "progressive level of a terrorist threat to all military facilities
and personnel" that outlines recommended security measures for local commanders. The purpose of the
program is to provide a joint framework for anti-terrorism activities and is based upon threat information
provided to a commander. Department of Defense, Joint Publication 3-07.2, *Joint Tactics, Techniques, and
Procedures for Anti-Terrorism.* 17 March 1998. (On-line); available from http://www.dtic.mil/doctrine/
jel/new_pubs/jp3_07_2.pdf; internet; accessed on February 23, 2004.

mission of the OHS was to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks".[19]

In pursuance of the mission, in July of 2002, the OHS delivered the National Strategy for Homeland Security. In it, the prioritized strategic objectives are listed as preventing terror attacks within the United States, reducing the country's vulnerability to terrorism, and minimizing damage and the time it takes to recover from attacks if they do occur, commonly referred to as consequence management.[20] The document outlined a new DHS that would bring various, previously disparate federal organizations and responsibilities under one directorate. Until this time, the several federal agencies responsible for certain aspects of homeland security were hopelessly scattered in many different departments. The structure presented in Appendix 1 represents how widely spread the homeland security mission was prior to reorganization (see Appendix 1: Organizational structure prior to DHS).

The National Strategy for Homeland Security also outlined six critical mission areas; intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response.[21] This document, in conjunction with the *Homeland Security Act of*

---

[19] Department of Homeland Security website, (On-line); available from www.dhs.gov/dhspublic/display?theme=59&content=312; accessed on January 14, 2004.

[20] United States Government, *The National Strategy for Homeland Security of the United States of America*. Jul 2002.

[21] United States Government, *The National Strategy for Homeland Security of the United States of America*. Jul 2002

2002, dated January 23, 2002, and the President's *The Department of Homeland Security*, dated June 2002, culminated in an Executive Order establishing the DHS on January 24, 2003.

The DHS is organized in four major directorates; Border and Transportation Security (BTS), Emergency Preparedness and Response (EPR), Science and Technology (S&T), and Information Analysis and Information Protection (IAIP). Within these four directorates lie the 23 agencies that make up the Department. They are broken down as follows (with their previous Department in parentheses):

BTS Directorate

-United States Customs Service (Treasury)

-Immigration and Naturalization Service (elements of Justice)

-Federal Protective Service (General Services Administration)

-Transportation Security Administration (Transportation)

-Federal Law Enforcement Training Center (Treasury)

-Animal and Plant Health Inspection Service (elements of Agriculture)

-Office for Domestic Preparedness (Justice)

EPR Directorate

-Federal Emergency Management Agency (Federal Emergency Management Agency)

-Strategic National Stockpile and the National Disaster Medical System (Health and Human Services)

-Nuclear Incident Response Team (Energy)

-Domestic Energy Support Teams (Justice)

-National Domestic Preparedness Office (Federal Bureau of Investigation)

S&T Directorate

-Chemical, Biological, Radiological, and Nuclear Countermeasures Program (Energy)

-Environmental Measurements Laboratory (Energy)

-National Biological Warfare Defense Analysis Center (Defense)

-Plum Island Animal Disease Center (Agriculture)

IAIP Directorate

-Critical Infrastructure Assurance Office (Commerce)

-Federal Computer Incident Response Center (General Services Administration)

-National Communications System (Defense)

-National Infrastructure Protection Center (Federal Bureau of Investigation)

-Energy Security and Assurance Program (Energy)

There are two other organizations that fall under the DHS. The Coast Guard, which maintains its independent identity as a military organization under the Commandant of the Coast Guard, falls administratively under the Directorate of Border and Transportation Security. However, in times of war, it will revert to the DoD.[22] Additionally, the Secret Service is in the DHS, having transferred from the Treasury Department in March of 2003.[23] It answers directly to the Secretary of Homeland Security. The chart in Appendix 2 outlines administratively how the DHS is organized, breaking out the various directorates and their mission focus (see Appendix 2: Current DHS Organization).

This rather extensive reorganization is the largest such restructuring since the 1947 National Security Act, and it involves over 170,000 federal employees.[24] It was done during a

---

[22] United States Coast Guard website (on-line); available from http://www.uscg.mil/hq/g-cp/comrel/factfile/index.htm; internet; accessed on February 23, 2004.

[23] United States Secret Service website (on-line); available from http://www.secretservice.gov/history.shtml; internet; accessed on February 23, 2004.

[24] The National Security Act of 1947 (NSA of 1947) was an effort by then President Harry S. Truman to reorganize the United States Armed Forces and the government's foreign policy organizations to reflect the country's newly evolving role as a world leader following World War II. President Truman

crisis, perceived or otherwise, facing the United States. This will be discussed in detail in

Chapter Four, but suffice it to say that the window of opportunity for such wholesale change is

probably either gone or soon will be.

Intelligence will play a critical role in any aspect of homeland security. In order to

understand how intelligence fits into the DHS, one must read the legislation:

> "Except as otherwise directed by the President, the Secretary shall have such access as
> the Secretary considers necessary to all information, including reports, assessments,
> analyses, and unevaluated intelligence relating to threats of terrorism against the United
> States and to other areas of responsibility assigned to the Secretary, and to all information
> concerning infrastructures or other vulnerabilities of the United States to terrorism,
> whether or not such information has been analyzed, that may be collected, possessed, or
> prepared by any agency of the Federal Government."[25]

In short, the DHS is an intelligence consumer. It does not collect or produce intelligence.

However, there is a need for an analytic capability within the DHS, for even if it collects already

analyzed intelligence, it must collate it into a useable product that can be used by the appropriate

decision maker.

NORTHCOM

On October 1, 2002, President Bush established the newest Unified Command, the

NORTHCOM, representing the ninth such unified command.[26] The mission of NORTHCOM is

---

signed the bill on July 26, 1947. It created the Department of Defense by merging the Department of War
and the Department of the Navy. Additionally, it created the separate United States Air Force out of the
United States Army Air Corps, which, up until this act, was part of the United States Army. Before this
act, the separate departments (War and Navy) enjoyed cabinet like status. The NSA of 1947 created a
Department of Defense with a cabinet level secretary (the Secretary of Defense) and attempted to
streamline the military by creating a single department that would not work at crossed purposes from
another military department at the cabinet level. The NSA of 1947 also established the Central Intelligence
Agency and created the National Security Council. (On-line); available from http://www.worldhistory.
com; internet; accessed on February 23, 2004.

[25] Best, Richard. *Homeland Security: Intelligence Support* (Washington, D. C.: Congressional
Research Service Report for Congress, 18 November 2002), 2-3, Library of Congress Congressional
Research Service, Order Code RS21283.

[26] The commands that are considered geographic include NORTHCOM, The European Command,
the Pacific Command, the Central Command, and the Southern Command. The other commands are

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 the Secretary of Defense, provide military assistance to civil authorities including consequence management operations."[27] The assigned area of responsibility for NORTHCOM includes the continental United States, Alaska, Canada, Mexico, Puerto Rico, the United States Virgin Islands, the Gulf of Mexico, surrounding water out to approximately 500 nautical miles, and air, land, and sea approaches to the above mentioned area. Interestingly, Hawai'i and United States territories and possessions in the Pacific remain under the auspices of the Pacific Command.[28]

There are significant differences between NORTHCOM and its sister geographic Unified Commands. For example, there are few forces permanently assigned to NORTHCOM. While there are several standing Joint Force Headquarters and Joint Task Forces, there is no ASCC.[29] As such, there is no organic EAC Army intelligence capability. This monograph will determine the feasibility, acceptability, and suitability of establishing an EAC intelligence capability that mirrors the geographic combatant commands, as well as recommend a construct from which to operate.

---

considered functional commands. They include the United States Joint Forces Command, the United States Special Operations Command, the United States Strategic Command, and the United States Transportation Command. United States NORTHCOM website (on-line); available from www.northcom.mil; internet; accessed on January 14, 2004.

[27] United States NORTHCOM website (on-line); available from www.northcom.mil/index.cfm?fuseaction=s.who_mission; internet; accessed on January 14, 2004.

[28] United States NORTHCOM website (on-line); available from www.northcom.mil/index.cfm?fuseaction=s.who_homefron; internet; accessed on January14, 2004.

[29] The pre-existing joint task forces include the Joint Headquarters-Homeland Security, which coordinates the land and maritime defense of the continental United States, Joint Task Force-Civil Support, which coordinates the Department of Defense role in consequence management, and Joint Task Force-6, which provides counter-drug support to various agencies in the continental United States. United States NORTHCOM website (on-line); available from www.northcom.mil/index.cfm?fuseaction=s.who_team; internet; accessed on January 14, 2004.

Summary

With the understanding of how intelligence support to existing geographic combatant commands is organized, as well as a basic grasp of the evolution of both the DHS and the newest combatant command of NORTHCOM, it is now important to synthesize this within the context of the political machinations of domestic politics. This is critical and will shape any new intelligence organization and how it approaches its mission. The next chapter will address the doctrine of EAC intelligence support with a bit more fidelity by examining how a specific EAC intelligence organization conducts its mission. Additionally, it will discuss pertinent laws, policies, and regulations that can affect any intelligence support to homeland security. It will become apparent that many of the restrictions are not as constraining as people believe.

CHAPTER THREE

DOCTRINAL APPLICATION

The previous chapter outlined the new operational environment facing the country and it's military. What makes the new operational environment unique is the speed with which it has manifested itself. The new threats no longer come from a powerful, predictable superpower, but rather from a somewhat less powerful, and absolutely unpredictable foe. This recognition, however, does not automatically mean that the American people are willing to accept domestic intelligence activities as a matter of common practice. Before this can be analyzed, it is important to understand a doctrinal application of military intelligence that might provide support to homeland security, either through NORTHCOM, an ASCC attached to NORTHCOM, or a new organizational construct. This chapter will outline some of the ongoing efforts by army military intelligence organizations, namely the 902nd MI Group and the Army Counterintelligence Center (ACIC). Finally, it will explain some of the laws, regulations, and policies affecting Army intelligence.

Echelons Above Corps Intelligence Doctrine

The doctrine for EAC intelligence organizations is outlined in Field Manual (FM) 34-37, *Echelons Above Corps Intelligence and Electronic Warfare Operations*, dated January 1991. Although it is outdated, it provides a good, albeit generic, baseline for the doctrinal application of intelligence at the EAC level. It is important to note that the manual states in the first chapter that, by definition, EAC intelligence units perform their intelligence mission at the operational

level. Furthermore, the manual defines the operational level as the link between national and

military strategy.[30]

        Since FM 34-37 was written over ten years ago, it refers to outdated doctrinal concepts,

such as the Airland Battle Doctrine. Despite this, there are many important aspects of the manual

that transcend adjustments in strategy. For example, each EAC organization is significantly

different, especially the TIB/TIGs supporting the geographic commands. They are specifically

tailored according to the unique requirements in the theaters.

        The manual goes on to state that the EAC organizations "support unified, joint, and

combined commands; other United States Army EAC commands within the theater; and

Continental United States major Army commands."[31] Finally, the command relationship enjoyed

by the TIB/TIGs is outlined in FM 34-37. It states that the organizations fall under the command

of INSCOM and under the operational control of the theater commander during peacetime.[32]

During conflicts, command of the TIB/TIGs reverts to the theater commander.

        This could have some relevance to an EAC organization assigned to NORTHCOM.

There is enough built in ambiguity to make command of such an organization negotiable. In

---

[30] Department of the Army, Field Manual 34-37, *Echelons Above Corps Intelligence and Electronic Warfare Operations*. January 1991. Page 1-2.

[31] Ibid.

[32] Operational Control, as defined by Joint Publication 1-02 states, "Command authority that may be exercised by commanders at any echelon at or below the level of combatant command." It goes on to state that, "Operational control is the authority to perform those functions of command over subordinate forces involving organizing, and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command." Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. March 23, 1994.

other words, a homeland security command, for lack of a better term, may fall under command of the theater commander and not INSCOM. This would give the organization access to INSCOM's capabilities, but distance itself from a strictly Army, military intelligence organization.

Currently, however, the subordinate unit within INSCOM that is most involved in both homeland security and homeland defense is the 902nd MI Group. It is important to understand some of the counterintelligence group's initiatives.

902nd Military Intelligence Group

The army and its EAC intelligence capabilities have responded to the terrorist attacks on September 11, 2001 with its existing capabilities. In many cases, the focus of organizations that had previously been concerned with foreign intelligence services has been changed to address the threat of trans-national and non-state terror. One such organization is the 902nd MI Group. This unit, a part of INSCOM and located at Fort Meade, Maryland, was discussed earlier in this monograph. However, this chapter will go into detail concerning some of its new initiatives.

As discussed, the 902nd MI Group is the United States Army's primary strategic counterintelligence organization.[33] Traditionally, the Group's focus had been the detection, neutralization, and exploitation of Foreign Intelligence Services. This focus began to change after the fall of the Soviet Union and prior to September 11, 2001 to involve more of the terrorist

---

[33] The 902nd MI Group is not the only strategic counterintelligence organization in the United States Army. The 650th MI Group is also a strategic counterintelligence unit. It is headquartered at the Supreme Headquarters, Allied Powers Europe in Mons, Belgium, and has detachments and field offices across Europe. There are no offices or detachment within the United States. Its mission is to provide the Supreme Allied Commander, Europe with counterintelligence support.

threat. However, the attacks hastened the process, enabling the Group to focus its "core

competencies" against asymmetric approaches used by trans-national terrorist organizations.[34]

Counterintelligence Analysis and Control Element

An example of the 902nd MI Group's shift in focus is the establishment of the

Counterintelligence Analysis and Control Element (CI ACE). While the CI ACE was actually

planned prior to 2001 as a way to synchronize the Group's many activities, the terror attacks gave

new impetus to the project, enabling it to become more of a true analysis and control element. On

November 1, 2001, the CI ACE became operational. Its mission statement reads:

> "Conduct information fusion, achieve situational awareness, and conduct predictive
> analysis to protect United States Army installations, personnel, and technologies.
> Integrate with the 902nd Military Intelligence Group Operations Center to conduct
> operational synchronization to achieve situational dominance."[35]

The CI ACE will operate using the current, doctrinal intelligence cycle of planning and

directing, collection, processing, production, and dissemination. The CI ACE receives

information collected by its detachments and field offices located on select Army installations in

the United States. It integrates that information with information provided to it by other

intelligence and law enforcement agencies, but only those within the Department of Defense and

the Federal Government. Finally, it uses open source information. The CI ACE then processes,

---

[34] Pratt, Ginger T. *The 902nd Military Intelligence Group and Homeland Security*. Fort Huachuca,
AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, pp. 15-16.

[35] Palaganas, Arthur F. *The 902nd Military Intelligence Group's ACE – A Center for Information
Fusion and Situational Awareness*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-
Sep 2002, Vol. 28, Issue 3, pp. 15-16.

or analyzes the information, using the many tools and skilled analysts available to it. Once the information is turned into intelligence, the CI ACE creates products and disseminates them to commanders and Army decision makers, as well as to select DoD customers.

The CI ACE provides a good example for creating an analytical element that can obtain and analyze disparate pieces of information, turning them into actionable intelligence. It relies on an already established network of detachments and field offices, spread throughout the country at various Army bases. Another advantage enjoyed by the CI ACE is that by virtue of being in the 902nd MI Group, it is an EAC Army intelligence organization. That means it can tap into existing capabilities, such as databases or established liaison networks, of the national level intelligence community. This serves the Army, its installations, and personnel quite ably. What it does not do, at least not yet, is provide the same type of reporting and analytical network that engages what Robert D. Steele, in his book, "*Studies in Asymmetry, The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Non-Traditional Threats*", describes as the forward observers in the new war on terrorism: the American citizens. [36]

Army Counterintelligence Center

The ACIC is another organization that has changed its focus since the terror attacks. It, too, is part of the 902nd MI Group. The mission of the ACIC is to "provide timely, accurate, and effective multidiscipline counterintelligence and terrorism analysis in support of the Army,

---

[36] Robert Steele states that in this new war on terrorism, the "private sector is the primary actor in protecting our infrastructure here at home from individual actors." He goes on to say, "our own neighborhoods comprise the 'front line' and our citizens are the 'forward observers.'" Steele, Robert D. *Studies in Asymmetry, The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Non-Traditional Threat*s. Washington D.C.: Strategic Studies Institute, February 2002.

sustaining base commanders, continental United States based deploying forces, ground system technologies, and counterintelligence investigations and operations."[37] The ACIC is described as providing the 'big picture' support to the Army.[38]

The ACIC and the CI ACE work closely together, providing joint threat assessments, all the while ensuring that the two organizations do not duplicate their effort. In doing so, the ACIC and the CI ACE will strive to identify and fill any intelligence gaps with respect to Army force protection and counter-terrorism. The two organizations in the 902nd MI Group also coordinate for liaison officers that are exchanged between the Group and the Army's Criminal Investigations Command.[39] These liaison officers help with the exchange of information between the intelligence and law enforcement communities within the Army.[40] Much like the CI ACE, however, this does not address the bigger challenge of providing that same kind of support to homeland security. This intelligence sharing between the communities is essential not only within the Army, but within the law enforcement community writ large.

---

[37] Harlan, Charles. United States Counterintelligence Center Support to Homeland Security. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol 28, Issue 3, pp. 17-18.

[38] "The ACIC is the primary intelligence producer for intelligence and security threats to developmental United States ground systems and technologies." While the ACIC has shifted into the arena of identifying intelligence gaps with respect to counterterrorism and force protection as a result of the September 11, 2001 terrorist attacks, it maintains its focus on four basic functional areas; technology protection, force protection, information operations, and support to counterintelligence investigations and operations. Ibid.

[39] The Criminal Investigations Command is the Army's primary criminal investigative organization. It is responsible for investigations of crimes where the Army is or has an interest. They can conduct these investigations on or off military reservations, depending on coordination with local authorities. Global Security website; (on-line); available from http://www.globalsecurity.org/military/agency/army/cid.htm; internet; accessed on March 9, 2004.

[40] Harlan, Charles. United States Counterintelligence Center Support to Homeland Security. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol 28, Issue 3, pp. 17-18.

Joint Terrorism Task Force

The Joint Terrorism Task Force (JTTF) is a relatively new effort in which elements of the 902nd MI Group are participating. Established by the FBI, the JTTF comprises teams of local, state, and federal law enforcement personnel, along with FBI agents and elements of other federal agencies, who work together to both prevent terrorism and investigate any acts that do occur. While the first JTTF came into being in 1980, they have increased significantly since September 11, 2001. Today, there are 66 JTTF offices nationwide; several of which are augmented by military intelligence personnel from the 902nd MI Group.[41]

A typical mission statement of a JTTF office reads, "Prevent acts of terrorism, and investigate acts of terrorism in an effort to identify and prosecute those responsible."[42] The San Antonio office, as an example, enlists the support of several federal agencies, to include CIA, the Defense Intelligence Agency, and the United States Air Force Office of Investigation (USAF OSI).[43] The USAF OSI is the United States Air Forces' counterintelligence capability. The 902nd MI Group has soldiers posted at several other JTTF offices. While the military intelligence

---

[41] Columbia, South Carolina JTTF website (on-line); available from http://columbia.fbi.gov/jttf.htm; internet; accessed on March 9, 2004.

[42] Mission statement for the San Antonio JTTF website (on-line); available from http://sanantonio.fbi.gov/jttf.htm; internet; accessed on March 9, 2004.

[43] The United States Air Force Office of Special Investigations is the Air Force's major investigative service. Unlike the Army's Criminal Investigations Command, the USAF OSI is responsible for counterintelligence activities. The USAF OSI focuses on four priorities. They are to, "detect and provide early warning of worldwide threats to the Air Force; identify and resolve crime impacting Air Force readiness or good order and discipline; combat threats to Air Force information systems and technologies; and defeat and deter fraud in the acquisition of Air Force prioritized weapons systems." The USAF OSI website (on-line); available from http://www.dtic.mil/afosi/about.html; internet; accessed on March 9, 2004.

soldiers (or airmen, in the case of the San Antonio office) cannot participate in arrests or other law enforcement operations, due to Posse Comitatus, they can lend their expertise to analysis and interrogation techniques.

Laws, Regulations, and Policies

Any type of domestic intelligence support must occur within both the letter and spirit of the law. There are several laws, regulations, and policies that effect domestic military and intelligence activities within the United States. The most commonly heard obstacle to domestic intelligence activities is the often-misunderstood Posse Comitatus, discussed earlier in this monograph. The most relevant regulation, however, is Executive Order (EO) 12333, United States Intelligence Activities, as well as the various Army and DoD Regulations and Directives that implement EO 12333. These orders, regulations, and directives, often referred to collectively as intelligence oversight, provide guidance on how military intelligence collects intelligence with respect to United States citizens. Additionally, the United States of America Patriot Act, passed shortly after the September 11, 2001 terrorist attacks, affects domestic intelligence activities. The Act seeks to increase cross talk between the law enforcement and intelligence communities, as well as provide law enforcement agencies greater latitude on certain collection activities.

Executive Order 12333, United States Intelligence Activities and Associated Regulations and Directives

Executive Order (EO) 12333 stipulates how intelligence agencies can collect on United States citizens, referred to as United States Persons. A United States Person is defined as "a

United States Citizen; an alien known by the Department of Defense intelligence component considered to be a permanent resident alien; an unincorporated association substantially composed of United States' citizens or permanent resident aliens; or a corporation incorporated in the United States (except for a corporation owned by a foreign government or governments)".[44] The EO does not prohibit collection on United States Persons; rather it stipulates that the affected agencies (in this case the Army) create governing procedures, which must be approved by the Attorney General of the United States.

In pursuance to EO 12333, the DoD issued DoD Directive 5240.1-R, *Procedures Governing the Activities of DoD Components That Affect United States Citizens.* In turn, the Army issued Army Regulation 381-10, *Army Intelligence Activities.* The difficulty with respect to these various orders and regulations is that they seem to be very restrictive. Many well-intentioned Army military intelligence professionals will simply refuse to deal with any information that even hints of United States Persons.[45] But the fact is that intelligence components may collect on United States Persons.

----

[44] A person living outside the United States and an alien in the United States are presumed not to be United States Persons unless specific information indicates otherwise. Department of the Army, Army Regulation 381-10, *United States Army Intelligence Activities*. July 1, 1984.

[45] An anecdote personally experienced by the author serves to illustrate this problem. While serving as a Counterintelligence soldier in Europe, the local German police provided the author information regarding a demonstration. The demonstration was against an upcoming execution in the state of Pennsylvania. While the demonstration was legal and ostensibly non-violent, the local police thought it necessary to provide the information in order for Americans living in the vicinity to avoid the area. The difficulty came when the police provided a flyer produced by the German anti-death penalty organization. It had the name of the prisoner who was to be executed in Pennsylvania. In a subsequent intelligence oversight inspection, the well-meaning inspector implied that by having that flyer in the safe, it constituted collection against a United States Person (i.e. the prisoner). This story is simply meant to display the confusion, and to a certain degree, outright fear experienced by military intelligence professionals when it comes to collection on United States Persons.

Lieutenant General Robert Noonan, the then United States Army Deputy Chief of Staff, G2, recognized this confusion immediately after the September 11, 2001 attacks. He issued a memo on November 5, 2001 titled *Collecting Information on United States Persons*, in which he recounts several incidents after the terror attacks where well-intentioned military intelligence professionals in the United States refused information from local authorities for the sole reason that the reports contained information on United States Persons.[46] Lieutenant General Noonan wanted to remind the military intelligence community of its duties and responsibilities, and what can and does fall within the current guidelines. For example, he pointed out that intelligence components can indeed collect information on United States Persons when such a component has the mission (or function) to do so, and if the information falls within certain categories. Of the various categories, the two most pertinent, given the attacks, are "foreign intelligence" and "counterintelligence".[47] These categories allow collection if United States Persons are "reasonably believed to be engaged, or about to be engaged, in international terrorist activities. Within the United States, those activities must have a significant connection to a foreign power, organization, or person."[48]

The implication is that Army intelligence may receive information at any time from any source. If the information contains United States Person data, the Army can retain it if it pertains to counterintelligence or foreign intelligence as defined by Army Regulation (AR) 381-10. Additionally, Army intelligence may deliver the information to other DoD components or other

---

[46] Noonan, Robert W. LTG. *Collecting Information on United States Persons* (extract) Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, p. 9.

[47] The term 'counterintelligence' is the same as was outlined in Chapter One of this monograph. 'foreign intelligence' is defined as "information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities. Department of the Army, Army Regulation 381-10, *United States Army Intelligence Activities*. July 1, 1984.

[48] Noonan, Robert W. LTG. *Collecting Information on United States Persons* (extract) Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, p. 9.

agencies if the information pertains to them.[49] The bottom line is that receiving information does

not constitute collection. In fact, as Lieutenant General Noonan points out in his memo, it is the

Army's duty to receive all pertinent information "regarding international terrorists who threaten

the United States, and its interests, including those responsible for planning, authorizing,

committing, or aiding the terrorist attacks of 11 September 2001."[50]

The United States of America Patriot Act

The United States of America Patriot Act (referred to from now on as the Patriot Act)

was passed as a direct result of the terrorist attacks on September 11, 2001.[51] Like the

reorganization of the Federal Government, mentioned in Chapter Two of this monograph, this bill

was signed in an incredibly short time. It became law on October 26, 2001, just 45 days after the

attack. This is yet another example of an astute use of prevailing public opinion. It is likely that

had the bill remained bogged down in Congress, it would never have been signed.

In short, the Patriot Act provides federal officials greater latitude to track and intercept

communications; it seeks a more effective border control, denying foreign terrorists entry while

removing those already inside the country; it more fully defines terrorism, both foreign and

domestic, creating better definitions of terrorist crimes, more comprehensive penalties, and more

efficient procedural methods to use against terrorists; and it has provisions designed to crack

---

[49] This must be done under a Procedure 4, AR 381-10, Dissemination of Information About United States Persons, which outlines criteria necessary for transit of information. Department of the Army, Army Regulation 381-10, *United States Army Intelligence Activities*. July 1, 1984.

[50] Noonan, Robert W. LTG. *Collecting Information on United States Persons* (extract) Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, p. 9.

[51] The full name for the Patriot Act is Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Smith, Regan K. *Homeland Security: An Intelligence Oversight Perspective*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, pp. 5-8.

down on foreign money laundering, seen as a critical weapon against international and non-state terrorists.[52]

This act, while controversial, loosens some restrictions on foreign intelligence gathering. While many of the specific provisions outlined in the Patriot Act refer to procedural restrictions, such as allowing provisions for roving surveillance, it affords the United States intelligence community "greater access to information unearthed during a criminal investigation."[53] It also "encourages cooperation between law enforcement and foreign intelligence investigators" as well as "expands the Posse Comitatus Act exceptions."[54] These provisions, even if they seem more like statements of encouragement, indicate that Congress, at least in the days immediately following the terrorist attacks, was willing to codify into law an increased domestic intelligence capability. While the Patriot Act does not specifically mention military or Army intelligence, it also does not preclude them.

Summary

This chapter outlined current doctrine with respect to EAC intelligence organizations. More importantly, it discussed some of the initiatives already started by one of those EAC intelligence organizations, the 902nd MI Group. Finally, this chapter outlined the pertinent laws,

---

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

[53] According to the Congressional Research Report for Congress, the Patriot Act "permits roving surveillance (court orders omitting the identification of the particular instrument, facilities or place where the surveillance is to occur when the court finds the target is likely to thwart identification with particularity). Ibid.

regulations, and policies that most directly influence domestic military intelligence activities. It is apparent that the laws, regulations, and policies are not as restrictive as many may believe. Indeed, the initiatives outlined above serve to illustrate this fact. There are, however, some challenges when it comes to expanding or enhancing the projects started by the 902nd MI Group. The most visible is the public perception of such operations. By using several current case studies, as well as several possible proposals, the next chapter addresses the need for a paradigm shift in both the public domain and the Army intelligence community.

---

[54] Ibid.

CHAPTER FOUR

THEORY

Immediately after the attacks on September 11, 2001, there was a cry from virtually all segments of society for the government to identify and address the problems with national security, especially with respect to intelligence gathering directed at potential terrorists. This manifested itself in the relatively swift establishment of a new department of the Federal Government, as well as a new cabinet position. Without attributing any judgment, this was a very astute use of the prevailing political feeling immediately after the attacks. The President and his administration no doubt knew that, as is typical in America, the feeling of collective indignation would not last very long. The American public has a short memory, a label that is usually attributed in a pejorative sense. In many cases, and this is one of them, the public's ability to quickly distance itself from the emotional aspect of an event and address the root cause is a unique asset of a democratic society that helps the country 'self-right' itself. In other words, once the shock has worn off, the American public figures out the best way to address the causes and ensure that, in the meantime, the homeland is secure.

Public Perception or Current Paradigm

The perceived recent trend in the United States is to shy away from any military involvement in domestic intelligence activities. While this may be true, conducting both military and intelligence activity within the United States or its territories and possessions is not unprecedented. While a history of domestic military and intelligence activity within the country

is beyond the scope of this monograph, Joint Task Force 6 (JTF-6) is but one example of how the military, and its organic intelligence, has been employed within NORTHCOM's current operational environment.[55] Joint Task Force 6 will be discussed in greater depth later in this chapter. The perception is, however, that the military and its intelligence capability is strictly utilized against the foreign aspect of 'all enemies, foreign or domestic'.

The difficulty with the homeland security aspect of the larger Global War on Terror is that the line between foreign and domestic is fading as illustrated by the fact that many of the September 11 terrorists trained and lived within the United States for some time.   After the terrorist attacks, it became clear, through the various investigations and reports, that information regarding some of the terrorists was available prior to the attacks. For example, there were reports of suspicious individuals applying to aviation schools to learn to fly large jet aircraft, but only in level flight. They displayed no interest in how to take off or land. Unfortunately, these reports, which in the parlance of the intelligence community constitute raw 'information', never became intelligence. The reasons why this was the case will not be discussed at length in this monograph, but one of the primary reasons is that no organized structure existed within which the information could have been collected, analyzed, and disseminated, resulting in several disparate chunks of information simply floating around the intelligence and law enforcement communities.

This brings up another important failure prior to the September 11 attacks, which was lack of communication between the intelligence and law enforcement communities. After the

---

[55] JTF-6 is located at Fort Bliss, Texas. It is assigned to Joint Force Headquarters, Homeland Security, under NORTHCOM. Joint Task Force-6 website (on-line); available from http://www-jtf6.bliss.army.mil/html/mission/htm; internet; accessed on February 13, 2004.

terrorist attacks, the intelligence community was scrutinized, given its inability to take the pre-September 11 information and turn it into actionable intelligence. The American public was especially frustrated once it was determined that much of the information actually existed. Unfortunately, both the law enforcement and intelligence communities did what they were asked to do. The FBI, for example, was an organization designed to conduct investigations with an eye towards prosecution, as it is the investigative arm of the Department of Justice.[56] Contrast that with the primary purpose of Army counterintelligence, which is to "identify, neutralize, and exploit foreign intelligence attempts to conduct operations against the United States Army."[57] While this does not preclude prosecution, it lessens the inherent constraints. The priority is to neutralize foreign intelligence attempts vice arrest and prosecute them.

Case Studies

The American public faces a dichotomy. On the one hand, the public demonstrates a traditional unease concerning domestic Army intelligence activities. On the other, it shows a deep frustration with the failure of the intelligence community before September 11, 2001. This

---

[56] In the months leading up to the terrorist attacks on September 11, 2001, the FBI's priorities included "upgrading the Bureau's information technology infrastructure, addressing records management issues, and enhancing FBI's foreign counterintelligence analysis and security in the wake of the damage done by former special agent and convicted spy, Robert S. Hanssen." The current mission of the FBI has changed rather dramatically to reflect the current operational environment. It states, "the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners." This change of mission, with a focus on terrorism, is a direct result of the terrorist attacks, and is outlined in the United States Patriot Act signed into law by President Bush on October 26, 2001. The Federal Bureau of Investigation website; (on-line); available from http://www.fbi.gov/priorities/priorities.htm; internet; accessed on February 24, 2004.

[57] Department of the Army, FM 34-60, *Counterintelligence*. October 3, 1995.

paradox may seem insurmountable. There are, however, examples of successful organizations, both military and civilian, that currently conduct domestic intelligence activities. Two of these will be outlined in this monograph in order to understand how they work in the current operational environment, with an eye towards using them as a construct for future, increased domestic military intelligence support to homeland security.

Joint Task Force-6

As stated earlier, Army involvement in domestic issues is not unprecedented. Joint Task Force-6 has been conducting operations in the United States since 1989. As mentioned earlier, JTF-6 is located at Fort Bliss, Texas and it is assigned to Joint Force Headquarters, Homeland Security, under NORTHCOM. Its mission statement reads:

> "JTF-6 synchronizes and integrates Department of Defense operational, training and intelligence support to domestic law enforcement agency counter drug efforts in the continental United States to reduce the availability of illegal drugs in the United States; and when directed, provides operational, training, and intelligence support to domestic agencies' efforts in combating terrorism."[58]

The original area of responsibility (AOR) was the four states of California, Arizona, New Mexico, and Texas along the Mexican border. However, in 1995, the AOR expanded to include the entire continental United States, and again in 1997, to include Puerto Rico and the United States Virgin Islands.[59]

---

[58] Joint Task Force-6 website (on-line); available from http://www-jtf6.bliss.army.mil/html/mission/htm; internet; accessed on February 13, 2004.

[59] Ibid.

The JTF-6 has three areas of support -- operational, training, and intelligence support. These are subsequently divided into sub-categories.[60] Although only one of the categories is titled intelligence support, there are intelligence related sub-categories within each, demonstrating that there are, indeed, military and intelligence activities being conducted within the United States today, and which have been doing so, to some degree, since the late 1980's.

It is important to understand that all of the military support that JTF-6 provides is based upon a valid request from a Law Enforcement Agency (LEA). The JTF-6 is simply a force multiplier, assisting an LEA in accomplishing its mission. It is not the other way around. The military and its intelligence capabilities provide a supporting role, albeit a significant one. The resident capabilities within the construct of JTF-6 are unique; otherwise, why would it exist. These include intelligence analytical capability, as well as various assessment capabilities.

El Paso Intelligence Center

Another interesting case study differs significantly from the example of JTF-6. While JTF-6 is a military organization that supports LEAs, the El Paso Intelligence Center (EPIC) is a Department of Justice Drug Enforcement Agency organization. Additionally, the EPIC is more

---

[60] **Operational Support**: Aviation reconnaissance, aviation forward looking infrared, aviation support operations, air surveillance radar, unmanned aerial vehicle, ground transportation, dive operations, technology demonstrations and assistance, communications, engineer missions, *ground reconnaissance, ground surveillance radar, listening/observation post, and ground sensor operations*. Italics represent mission that require Secretary of Defense approval. **Training Support**: Mobile Training Teams, including language, first aid, military skills, interview and interrogation, intelligence link analysis, basic marksmanship, integrated planning, counterdrug investigations, working dog training and first aid, narco-terrorism personal protection, field tactical police operations, special reaction team, marksman/observer, and threat assessment training. **Intelligence Support**: Intelligence analysts, transcription/translation, topographic and imagery, intelligence architecture assessments, vulnerability assessments, special studies, intelligence threat assessment and targeting training. Ibid.

of an intelligence fusion center, concentrating on taking existing information and turning it into drug intelligence.[61]

The EPIC was created in 1974 as a Southwest Border Intelligence Service Center and was originally staffed with individuals from the Immigration and Naturalization Service, the United States Customs Service, and the Drug Enforcement Agency. The original mission was collecting and disseminating intelligence related to drug movement and immigration violations strictly on the United States / Mexico border. It has since evolved into a much larger and robust organization that focuses on the same issues, but covers the entire western hemisphere, where drug and immigration violations involve or are aimed towards the United States. Additionally, the staffing now includes individuals from over 15 federal agencies, as well as several state (Texas) agencies. Included in the EPIC's staffing are members of the Texas Air National Guard.[62]

A unique aspect of the EPIC is its information sharing agreements, which include agreements with other federal law enforcement agencies, international law enforcement agencies, such as the Royal Canadian Mounted Police, as well as law enforcement agencies in each state. They serve as a repository of information regarding drug intelligence. The EPIC maintains a robust analytical capability, including the development of the National Clandestine Laboratory Seizure Database, which enables the center to stay ahead of recent trends in drug trafficking.[63]

The two pertinent items of interest from studying the EPIC are the robust analytic ability that can transcend local, state, federal, and even international jurisdictions, as well as the

---

[61] Drug intelligence is simply intelligence related to drug trafficking. According to the National Drug Intelligence Center's website, one of its primary missions is to support the intelligence community's counterdrug efforts. National Drug Intelligence Center website; (on-line); available from http://www.usdoj.gov/ndic/about.htm#The; internet; accessed on February 24, 2004.

[62] El Paso Intelligence Center website (on-line); available from http://www.usdoj.gov/dea/programs/epic.htm; internet; accessed on February 24, 2004.

[63] Ibid.

participation of the Texas Air National Guard. The first item of interest simply demonstrates that it is possible to construct an intelligence organization that spans local, state, national, and international jurisdictions and, more importantly, creates the necessary agreements to make it work. The second item of interest involves the use of the Reserve Component. The Texas Air National Guard's participation in the EPIC demonstrates that a military capability is already being leveraged in a largely criminal intelligence organization.

Paradigm Shifts

There is discussion about the need for a paradigm shift by the American public; a shift accepting or at least allowing a greater degree of intelligence activities to be conducted within the United States. There is, however, a need for the intelligence community to shift as well. Several proposals have been drafted, the goals of which are to effect greater intelligence cooperation between the law enforcement and intelligence communities, and utilize all components of the military. The following represents but two of the many proposals. The first proposal is the creation of a Homefront Defense Analysis Center. The second advocates using various State Defense Forces, which are a variant of the state National Guard, in a homeland security type of role.

Homefront Defense Analysis Center

In his book, Robert D. Steele advocates the establishment of a Homefront Defense Analysis Center (HDAC), whose mission would be to "integrate national foreign intelligence, law enforcement intelligence, and corporate security intelligence."[64] The HDAC could be under the

---

[64] Mr. Steele's advocated mission statement goes on to include "legal access to credit card and travel industry databases for the purpose of checking all individuals on a new consolidated national watch list." Steele, Robert D. *Studies in Asymmetry, The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Non-Traditional Threat*s. Washington D.C.: Strategic Studies Institute, February 2002; p. 47.

command or direction (Mr. Steele calls it oversight) of INSCOM. He envisions the HDAC as a type of operations center, with 24-hour, seven days a week capability.

This capability, minus some of the corporate security intelligence, as well as full access to law enforcement intelligence, exists presently in the previously discussed CI ACE. In fact, the CI ACE can provide the catalyst upon which an HDAC can grow. The Army, as Steele states in his book, can take the lead in establishing an HDAC capability, if for no other reason than it already has a robust ability to take distributed intelligence and make it useable to a variety of customers.[65] The Army already does this when it provides EAC intelligence support to the Combatant Commands. The doctrine, training, and technical architecture exists. The HDAC can either replicate these existing capabilities, or integrate them into an expanded CI ACE.

State Defense Forces

It is always difficult to create new missions for the active component of the Army. This is especially true when it comes to a career field that, while not low density, certainly is in high demand, such as military intelligence. This is evidenced by the fact that the stop-loss program tends to focus on pilots, Special Operations, and Intelligence soldiers. In order to mitigate the impact on the active component, many of the military intelligence support missions conducted on behalf of the homeland security mission can be accomplished by the reserve component. The reserve component consists of the United States Army Reserve and the National Guard. One option resident within the National Guard is the State Defense Force.

---

[65] Ibid.

The State Defense Forces, also described as "Home Guards" or "Home Defense Forces" are military forces under the command of the state governor, through the Adjutant General. They are "created, funded, and controlled solely by the individual states."[66] Not all states have standing State Defense Forces (24 States and the Territory of Puerto Rico have standing State Defense Forces); however, they all have the authority to raise such forces.[67] These forces are composed of individuals who are paid only when activated by the individual states. The State Defense Forces are distinguished from the National Guard by the fact that they may not be called to federal service, although they are under the purview of the National Guard Bureau. The Bureau, through the state's Adjutant General, provides administrative, procedural, and organizational guidance to the State Defense Forces.[68]

The advantages of using the State Defense Forces are many. They include the simple fact that many of the states that have a standing State Defense Force, have already integrated it into

---

[66] The term State Defense Forces is generic. The title is different from state to state, ranging from the Alabama State Defense Force, the Massachusetts Military Reserve, to the Washington State Guard. For simplicity, however, they will collectively be referred to in this monograph as State Defense Forces. Tulak, Arthur N., Kraft, Robert W., & Silbaugh, Don. *State Defense Forces and Homeland Security*. Carlisle Barracks, PA: Parameters, United States Army War College Quarterly, Winter 2003-2004, Vol. XXXIII, No. 4, pp. 132-146.

[67] The State Defense Forces have different names in the various states. The 24 states and territory are listed as follows: Alabama State Defense Force, Alaska State Defense Force, California State Military Reserve, Connecticut State Militia, Florida State Defense Force, Georgia State Defense Force, Indiana Guard Reserve, Louisiana State Guard, Maryland Defense Force, Massachusetts Military Reserve, Michigan Emergency Volunteers, Mississippi State Guard, New Jersey Naval Militia, New Mexico State Defense Force, New York Guard and New York Naval Militia, North Carolina State Guard, Ohio Military Reserve, Oregon State Defense Force, Pennsylvania State Military Reserve, Puerto Rico State Guard, South Carolina State Guard, Tennessee State Guard, Texas State Guard, Virginia Defense Force, Washington State Guard. Ibid.

[68] Ibid.

their emergency management operations. In 28 states, the Adjutant General wears a second hat as the director of the state's emergency management agency or directorate.[69] This connotes that there is an existing relationship between the State Defense Forces and the law enforcement communities. If some of the State Defense Forces are utilized in a military intelligence capacity, there will be a natural flow of information, resulting in communication between the intelligence and law enforcement communities. Again, in many cases, these are actually the same people.

Another advantage the State Defense Forces have is the fact that they may not be called to federal service, as they belong exclusively to the state. As such, they are not required to train for combat roles. Their training, in fact, can reflect the needs and priorities of the governor, through the Adjutant General. Additionally, this is all done within the auspices of the National Guard Bureau. This means that, unlike the National Guard, which can be called to federal service at any time, the State Defense Forces will always be available to the governor, and will have trained according to the articulated requirements. These articulated requirements can be military intelligence support to homeland security.

The State Defense Forces could be used to create State Intelligence Centers. These intelligence centers, which would operate much like an operations center (i.e. 24-hour a day manning), could either mirror or be a part of the existing JTTFs, mentioned in Chapter Three. They could provide intelligence to the JTTF after collecting or receiving information from a variety of sources, including local and state law enforcement agencies. An HDAC type of organization that would ensure deconfliction and coordination between states could coordinate these intelligence centers.

---

[69] Ibid.

In this respect, the individual states and territories could provide organic Army intelligence capability in the realm of homeland security. The challenge would be to coordinate them so that there is a common purpose. Additionally, the fact that the State Defense Forces are independent from the active component may make it difficult to ensure unity of effort across the country.

Summary

Through a theoretical approach, this chapter addressed the current paradigm, with respect to both the military and the American people. This paradigm tends to preclude the use of military intelligence within the United States. For the military, it is a paradigm created through a generation of intelligence soldiers having been inculcated with the fact that domestic operations are not possible. For the American people, the thought of the United States Army or any of its organic military intelligence capabilities operating within the country is simply not palatable. Using several case studies, however, this chapter showed that not only can the Army conduct intelligence activities within the country, but also that it is currently doing so.

This chapter concluded with two possible constructs that may cause a paradigm shift, both in the Army and with the American people. These proposals, along with others addressed throughout this monograph, will be analyzed for viability in the next chapter.

CHAPTER FIVE

RECOMMENDATIONS, ANALYSIS, AND CONCLUSION

The mission of protecting the United States of America from all enemies, both foreign and domestic, is the reason the Army exists. The Army has evolved over its 229-year history, but its mission remains the same. In order to effectively accomplish its mission, the Army's intelligence community has developed tactics, techniques, and procedures that tend to be pro-active, vice reactive. In other words, the intelligence community is chartered with providing predictive intelligence. Contrasted with that pro-active mandate is the traditional mission of the law enforcement community. Many law enforcement agencies, judicial organizations, and even military consequence management programs are designed to react to an attack. The challenge is how to apply Army intelligence capabilities within the United States in order to help prevent future attacks on the country.

Theoretically, it is not only possible for the United States Army to provide EAC intelligence support to a domestic entity, it is happening right now. Additionally, as outlined in Chapter Three, the EAC doctrine is sufficient to provide guidelines within which to utilize the intelligence capabilities. The doctrine remains valid whether the intelligence is provided by the active or reserve component. Given these two facts, there are several recommendations that may make Army intelligence support to homeland security more efficient than it already is. These recommendations will include organizational changes, as well as changes to traditional command and control relationships. This chapter will outline recommendations, and then will analyze the viability of each by asking three questions; are the recommendations feasible, acceptable, and suitable?

Recommendations

It is clear that the mission of homeland security relies heavily on timely and accurate intelligence. What is not as clear is who provides that intelligence and how it is collected,

analyzed, and disseminated. As outlined earlier in this monograph, there are many agencies,

including Army organizations, which have invested a great deal of time and resources to address

this challenge. There are, however, several things that can be done to increase the efficiency and

effectiveness of intelligence support to homeland security. They include, but are not restricted to

creating State Intelligence Centers that are empowered to share information and even intelligence

at the lowest (i.e. local) possible level. Representatives from different organizations, including

members of the State Defense Forces, can staff these centers. These State Intelligence Centers

can be coordinated by a HDAC. Finally, a traditional command and control relationship with

NORTHCOM and the DHS may not be possible. Therefore, a non-traditional command

relationship is necessary in order to ensure this intelligence apparatus will be effective.

The first step in any effective intelligence organization is the collection of information. If

the appropriate information remains uncollected, intelligence will not exist. This was the

problem in the wake of the September 11, 2001 attacks. The disparate pieces of information

existed; however, there was no means by which it could be collected, analyzed, and rendered in a

useable format. As such, this requires an organizational fix, rather than a wholesale overhaul of

intelligence tactics, techniques, and procedures. If, as was the case before the terror attacks, the

information exists, there simply needs to be a method by which it is distributed to organizations

and analysts who can create intelligence. This intelligence, in turn, must be disseminated to the

appropriate decision maker. If any of these steps is omitted, the intelligence is useless.

The second step is to integrate this domestic intelligence, regardless of how it was

collected, into the larger, worldwide threat picture. In this global war on terror, the area of

interest is the planet Earth. Terrorists operate in many countries, including the United States.

Therefore, intelligence collected in the state of Florida may be relevant to, or made relevant by

intelligence collected by an intercepted telephone call from Pakistan to Afghanistan. In other

words, there must be a method to integrate national level, or strategic, intelligence with the

intelligence gathered at local and state levels by those local and state level organizations, whether they are civilian or military.

These two steps can be accomplished with the establishment of State Intelligence Centers. These centers can mirror or be a part of the existing JTTF concept by becoming its analytical control element. They will operate 24 hours a day, seven days a week and be manned by members of the individual State Defense Forces, agents from the local FBI office, and representatives from local and state police agencies. This does several things. First, it provides a local and organic intelligence capability that is capable of using the information collected by the "forward observers" on the new "front line".[70] This represents the type of information that an EAC intelligence organization, even without the present laws, policies, and regulations in place, would not be able to collect. Secondly, creating a State Intelligence Center and manning it with members of the State Defense Force who, in many of the states are already integrated into the state's emergency management agency, effectively taps into an already existing liaison network. Finally, this reduces the requirements currently levied on the active duty intelligence soldiers, primarily out of the 902nd MI Group, to man the JTTFs. Instead of sending soldiers to various centers around the nation, they can return to their primary mission, that of conducting counterintelligence activities in support of Army Commanders to protect Army forces, secrets, and technologies. The 902nd MI Group expertise can be used to help train the State Defense Forces in current tactics, techniques, and procedures through a mobile training team concept.

---

[70] As Robert Steele states in his book, the citizens of the United States are the forward observers in the new war on terror, and the neighborhoods are the new front line. Steele, Robert D. *Studies in Asymmetry, The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Non-Traditional Threat*s. Washington D.C.: Strategic Studies Institute, February 2002; p. 18.

In order to ensure the State Intelligence Centers are not working at crossed purposes, there must be a capability to coordinate and deconflict collection and analysis. This is addressed in a HDAC. This organization can mirror the structure of the 902nd MI Group's CI ACE. It would be a part of INSCOM, but not necessarily a command. This provides room to explore different command relationship options. The HDAC serves many purposes. First, it is a centralized analytical center that can take the intelligence produced at the State Intelligence Centers, integrate it, and provide decision makers at NORTHCOM or the DHS with a nationwide intelligence product. Secondly, it can act as the 'traffic cop' with respect to collection from the many State Intelligence Centers, much like the current G2X concept. A G2X, and his Counterintelligence Coordinating Authority are the Human Intelligence (HUMINT) resident experts on a Division G2 staff. They ensure that all HUMINT, which includes all counterintelligence work, is coordinated and deconflicted within a Division's AOR.

Finally, an HDAC can serve as the bridge between which the local, or tactical intelligence, is integrated with the national, or strategic intelligence. For example, a policeman during his usual patrols might see something out of the ordinary, for example, a vehicle parked in a restricted area near an airport. This information seems insignificant, and in the past might have resulted in nothing more than a traffic ticket. If that van had contained an individual conducting pre-operational reconnaissance in preparation for a terrorist attack on an airplane, he received nothing more than a scare and a ticket. By integrating national level intelligence, that policeman would have been made aware of recent intercepted phone conversations detailing a planned attack, for instance. In this notional exercise, the policeman would have had many more options, including arrest or exploitation.

There are several obstacles to this concept, many of which will be addressed in the viability analysis section of this chapter. One common difficulty that can be mitigated by a recommendation is that regarding command relationships. As stated earlier, the State Defense Forces work for the state governors, through the Adjutant General. The National Guard Bureau,

however, is the executive agent. If the DHS, through NORTHCOM, looks at the states as individual entities, it can create memorandums of agreement and/or understandings, creating "security cooperation plans for homeland security contingency operations with each of the states and territories."[71] These agreements must address NORTHCOM's tasking authority, through the HDAC and the Adjutant General, to the states forces. This does not imply a command relationship, as the State Defense Forces would remain under the command of the state Adjutant General; rather it implies an ability, through tasking authority, to ensure a unity of effort.[72]

Since NORTHCOM does not have an ASCC in the traditional sense, the HDAC, through its unique command and control relationships with the State Intelligence Centers, can assume the role of an EAC intelligence organization that answers directly to NORTHCOM and is in close coordination with the DHS. It is significantly different from other INSCOM organizations, in that it must coordinate with over fifty different intelligence centers rather than command them.

Finally, the culture within the military intelligence community must change. This monograph does not advocate a loosening of restrictions or oversight on intelligence gathering, but rather an honest look at how the current policy and guidance is implemented. There are built in procedures for virtually every scenario. In the past, however, with the threat as it was, the Army did not need to be heavily involved in domestic intelligence work. That paradigm has

---

[71] Tulak, Arthur N., Kraft, Robert W., & Silbaugh, Don. *State Defense Forces and Homeland Security*. Carlisle Barracks, PA: Parameters, United States Army War College Quarterly, Winter 2003-2004, Vol. XXXIII, No. 4, p. 133.

[72] This is not unprecedented. During the 2002 Olympic Games in Salt Lake City, Utah, a Combined Joint Task Force-Olympics (CJTF-O) was established. There were a series of agreements established, giving the Commander of the CJTF-O tasking authority over the state forces in his area of operation.

changed. The Army, by virtue of its mission of protecting the country against all enemies, must now become involved, domestically, in homeland security.

Viability Analysis

The next hurdle is to determine whether or not the idea of domestic intelligence in support of homeland security is viable. There are three questions that must be answered in order to establish the viability of this proposal; whether it is feasible, acceptable, and suitable.

Feasibility

The question of whether domestic military intelligence can feasibly support homeland security can be distilled into one, basic question. That is, given present laws, policies, and regulations, is it even possible to collect, analyze, and disseminate intelligence for a predominantly domestic organization such as the DHS or NORTHCOM? The short answer to this question, as outlined previously in this monograph, is simply, yes.

The previous chapters, specifically Chapter Three, discussed many of the laws, regulations, and policies effecting domestic military intelligence. Executive Order 12333 is the most relevant of those. The Army implements the guidance in EO 12333 through AR 381-10. These regulations and policies outline in specific detail how Army intelligence can collect information on United States Persons. The bottom line is that these are not as restrictive as many believe. They simply outline the procedures and responsibilities with respect to domestic collection. If these procedures and responsibilities are met, then the Army can assist in homeland security.

The Patriot Act, regardless of its controversies, indicates that Congress recognized the disconnect between the law enforcement and intelligence communities. The truth is that many of the restrictions placed upon law enforcement organizations and Army intelligence had not been updated to reflect current technology. Cellular phones and the invention of the Internet are but

two examples of technological advances that rendered many collection techniques obsolete. Additionally, the Army had little requirement to conduct domestic intelligence collection within the United States. This is evidenced by the fact that a specific combatant command responsible for the North American continent was not established until after the attacks on September 11, 2001.

Domestic Army intelligence support to homeland security, especially with the passage of the Patriot Act, is feasible. Additionally, the State Intelligence Centers, the HDAC, and the rather unique command and control methods outlined in this chapter are all feasible. They are all capable of being accomplished. To some degree or another, they all have precedent.

Acceptability

Since it has been determined that, strictly speaking, domestic military intelligence support to homeland security is feasible, the next question is whether it is acceptable. In order to be acceptable, domestic intelligence conducted by the Army must be adequate to satisfy the articulated requirement of increased intelligence support to homeland security in order to protect the country. More specifically, what policies, procedures, or laws must be changed, if any, in order for an effective EAC intelligence organization to support the DHS and NORTHCOM?

First, as stipulated in the previous feasibility test, there need not be any significant changes to current policies, procedures, or laws. By and large, they provide adequate guidance for the Army to provide intelligence support to homeland security. The Army is already providing limited support through the 902nd MI Group with the CI ACE, the ACIC, and its participation in the JTTFs.

However, there are changes necessary in several other aspects of intelligence support to homeland security. The first, with respect to the military in general and Army intelligence in particular, concerns the aforementioned paradigm shift that is needed. The Army intelligence community, especially the current generation, has grown up in an era of strict, almost over-

adherence to Executive Order 12333 and Army Regulation 381-10, as well as other pertinent policies and regulations. The memo released by the United States Army Deputy Chief of Staff for Intelligence immediately after the September 11, 2001 terrorist attacks, outlining the duties and responsibilities of the Army's intelligence collectors, highlights this. The culture within the military intelligence community must change to reflect the current operational environment. Currently, the Army and its intelligence apparatus is built to protect, and therefore collect against, a monolithic threat, such as the Soviet Union. The Cold War threat was significant, but rarely did the enemy plan the mass murder of innocent civilians within the United States, using the very freedoms guaranteed to all citizens as cover, nuclear war notwithstanding.

Another change necessary within the Army intelligence establishment is the relationship between the active and reserve components, as well as the relationship within the components themselves. The State Defense Forces are a resource that has not been efficiently leveraged in the search for homeland security. If they have been leveraged at all, they are uncoordinated and depend upon the individual states. The National Guard Bureau, which is the Executive Agent over the State Defense Forces within the DoD, must coordinate with the states in order to more efficiently address homeland security concerns at the local level. [73] At the same time, the individual states must change how they utilize the National Guard, and more specifically, the State Defense Forces.

---

[73] Tulak, Arthur N., Kraft, Robert W., & Silbaugh, Don. *State Defense Forces and Homeland Security*. Carlisle Barracks, PA: Parameters, United States Army War College Quarterly, Winter 2003-2004, Vol. XXXIII, No. 4, pp. 132-146.

These changes imply that a new or adjusted command and control methodology be adapted. The individual State Defense Forces may not be part of INSCOM or a particular EAC intelligence organization in a traditional command and control type of way. Rather, there may be over fifty different memorandums of agreement or understanding between INSCOM and the State Intelligence Centers, with the HDAC providing a strategic direction, as well as deconfliction of the various centers.

The second paradigm shift concerns the citizenry of the country. The American public is not especially amenable to domestic intelligence activities. This despite the several case studies pointing out current examples of Army intelligence participating in what can only be characterized as domestic missions. Upon close examination of the laws, policies, and regulations regarding domestic military intelligence activities, however, it becomes apparent that there are significant safeguards in place. So significant, in fact, that they lead directly to the first paradigm experienced by Army intelligence professionals, mentioned above. Having said this, however, there are no recommendations in this or any other monograph that can change public perception. The best the Army can do is to mitigate existing concerns and ensure the current laws, policies, and regulations are strictly enforced.

One way to mitigate the public's concern is to involve the reserve component, specifically the National Guard and State Defense Forces. In this way, the communities across the United States have a vested interest. The State Intelligence Centers will not be manned by active duty soldiers who arrive for a short tour and move away; rather, local residents who represent the local community will staff them. The fact that this community familiarity will only serve to enhance their mission is a bonus.

A second way to mitigate the public's concern over domestic intelligence activities is to highlight the relationship of the State Intelligence Centers with NORTHCOM and, more importantly, the DHS. This, and the significant participation of other agencies in the State

Intelligence Centers other than the DoD can allay some fears that the ubiquitous 'pentagon' is operating in local communities.

The recommended changes to Army intelligence support to homeland security are acceptable. They demand no radical changes in current laws, policies, or regulations, but rather a change in the Army mindset and the public's perception. These are the paradigms that must shift. Fortunately, the first paradigm and any necessary adjustments can be affected relatively easily within the Army. The second paradigm, however, is much more difficult, and in the end, much more important.

Given the history of the United States, its freedoms, and traditional wariness of domestic military operations, the possible negative perceptions that many of her citizens may possess with respect to a domestic military intelligence capability must be addressed. Despite laws, policies, and regulations that may allow or even direct domestic intelligence activities, there will be a major perception challenge with respect to collecting intelligence within the United States.

Suitability

Suitability is defined as something that is appropriate to a purpose or an occasion. The suitability test is the most difficult of the three tests used to analyze the recommendations outlined in this monograph. The benefits of creating a domestic Army intelligence capability to support homeland security have been outlined at length during the course of this monograph. They include, but are not limited to using Army intelligence tactics, techniques, and procedures that have been honed during the course of many operations and conditions to build a similar capability, but focused on a new type of target in a new operational environment. The training, personnel, and doctrine, not to mention the assets (to include money), are unique in the military and are not resident in organizations that tend to be on the front lines of this new war. Instead of creating a national police force that replicates Army intelligence capabilities, it seems more efficient and much less expensive to create a requirement for the Army to provide the necessary

support to homeland security. This, of course, connotes an increase in resources for Army

intelligence, both in manpower and funding, but that is beyond the scope of this monograph.

Yet another benefit of leveraging Army intelligence to support homeland security is the

immediate and existing access to national level intelligence. This access is already resident in

INSCOM. It is facilitated by technology, such as data mining techniques, analysis software, and

database systems. The various INSCOM subordinate commands have been acting as the bridge

between national and tactical intelligence for the Combatant Commanders since at least the

inception of INSCOM in 1977.[74] This is not a new concept; however, applying it to homeland

security is. The bottom line is that Army intelligence has a long history of supplying different

commanders and customers, which are often geographically separated from the intelligence

center, with pre-emptive, analytical products with which decision makers can act.

It is rather difficult to gauge whether or not these recommendations will be perceived as

suitable by the public, but the benefits significantly outweigh the risks accrued by not creating

some type of domestic intelligence organization that can support homeland security. There must

be a bridge between the law enforcement and intelligence communities. Additionally, there must

be a bridge between local, state, and national level information gathering organizations, be they

police, military, customs, or border patrol. Currently, if there are those bridges, it tends to be ad

hoc. This is unacceptable, as the terrorists can find and then exploit any gaps in coverage and

capabilities.

---

[74] Gilbert, James L. *In '77, Command Created New Identity*. Fort Belvoir, VA: INSCOM
Journal, Summer 2002, Vol. 25, No. 2, pp. 14-16.

Conclusion

In hindsight, if anything might have helped stop 9/11, it would have been better information about threats inside the United States – something made difficult by structural and legal impediments that prevented the collection and sharing of information by our law enforcement and intelligence agencies.[75]

> Doctor Condoleezza Rice, National Security Advisor
> Congressional Testimony to the 9/11 Panel
> 8 April 2004

The attacks on September 11, 2001 were horrific. The United States of America and all her citizens were affected. Unlike Pearl Harbor in December of 1941, where the target was predominantly military, this attack was purposely aimed at so-called 'soft targets'. The enemy used the freedoms that America has struggled to obtain and protect as cover for their murderous actions. Part of the terrorists' plan was no doubt to change and curtail many of those freedoms. As such, this monograph does not advocate in any way an abrogation of American citizens' personal freedoms, rights, or privileges. Rather, it simply points out that resident in the very organization charged with protecting and defending this country is a capability that, even within current guidelines, can contribute much more to the security of the homeland. It requires a shift in how Army intelligence approaches the new operational environment, and it requires patience and understanding on the part of the American citizens, but it can be accomplished. It must be accomplished.

---

[75] Quoted by Doctor Condoleezza Rice, National Security Advisor, on 8 April 2004 during congressional testimony in front of the 9/11 Panel, United States Congress, Washington, D.C.

APPENDICES

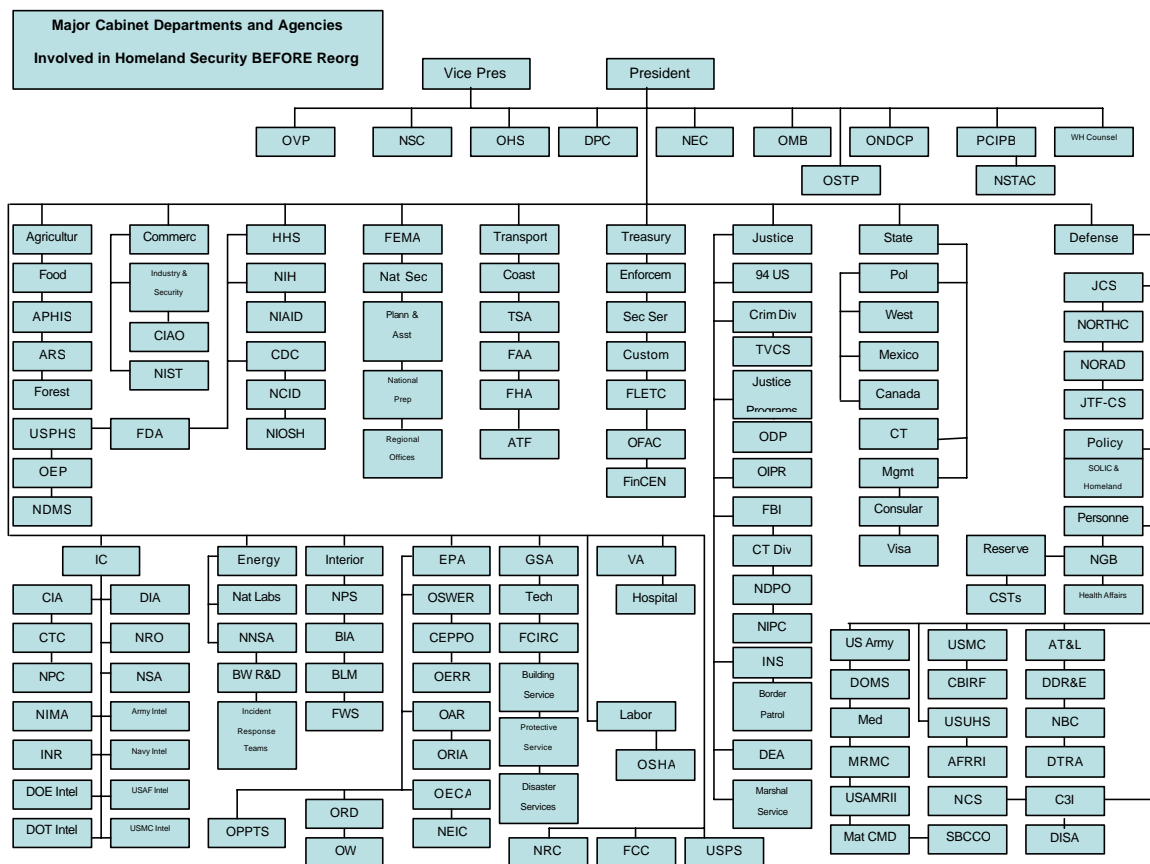## Appendix 1: Organizational Structure Prior to DHS

Figure 1.   Organizational structure before the creation of the DHS.[76]

Appendix 2: Current DHS Organization

Department of Homeland Security

Note (1): Effective March 1st, 2003

Figure 2   Organizational Structure of the new Department of Homeland Security.[77]

---

[77]The Department of Homeland Security website (on-line); available from www.dhs.gov/dhspublic/display?theme=13; internet; accessed on February 9, 2004

BIBLIOGRAPHY

United States Government Documents, Manuals, Policies, and Speeches

Chizek, Judy G. *Military Transformation: Intelligence, Surveillance, and Reconnaissance.* Washington D.C.: Report for United States Congress, January 17, 2003.

Best, Richard. *Homeland Security: Intelligence Support* (Washington D.C.: Congressional Research Service Report for Congress, November 18, 2002), Library of Congress Congressional Research Service, Order Code RS21283.

Dacey, Robert F. *Critical Infrastructure Protection: Significant Challenges Need to be Addressed.* Washington D.C: Congressional Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, the United States House of Representatives, Washington D.C., 24 July 2002.

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

Department of the Air Force, *The United States Air Force and Homeland Civil Support (White Paper) Draft.* No date.

_____, *The United States Air Force and the Security of the Homeland (White Paper) Draft.* No date.

Department of the Army, AR 381-10, *United States Army Intelligence Activities.* 1 July 1984

_____, AR 381-12, *Subversion and Espionage Directed Against the United States Army (SAEDA).* 15 January 1993.

_____, AR 381-20, *The Army Counterintelligence Program.* 15 November 1993.

_____, FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process (MRCP 3-1.6.14).* 8 May 1996.

_____, FM 34-1, *Intelligence and Electronic Warfare Operations.* 27 September 1994

_____, FM 34-7, *Intelligence and Electronic Warfare Support to Low Intensity Conflict Operations.* 18 May 1993

_____, FM 34-36, *Special Operations Forces Intelligence and Electronic Warfare Operations.* 30 September 1991.

_____, FM 34-37, *Echelons Above Corps Intelligence and Electronic Warfare Operations.* January 1991.

_____, FM 34-52, *Intelligence Interrogation.* 28 September 1992.

_____, FM 34-60, *Counterintelligence.* 3 October 1995.

_____, FM 101-5-1, *Operational Terms and Graphics.* 30 September 1997.

_____, *How the Army Runs; A Senior Leader Reference Handbook 2001-2002,* Carlisle Barracks, PA: United States Army War College, 2001.

Department of Defense, Defense Intelligence Agency Manual 58-12 (S), *The DoD HUMINT Management System, (U)*. 30 June 1997.

_____, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. 23 March 1994.

_____, Joint Publication 3-07.2, *Joint Tactics, Techniques, and Procedures for Anti-Terrorism*. 17 March 1998.

House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*. Washington D.C.: United States Congress, December 2002.

Rice, Condoleezza. Testimony before Congressional 9/11 Panel. Washington D.C.: 8 April 2004.

United States Government, *Executive Order No. 12333*, United States Intelligence Activities.

_____, *The Department of Homeland Security*. June 2002.

_____, *The National Security Strategy of the United States of America*. September 2002.

_____, *The National Strategy for Homeland Security of the United States of America*. July 2002.

Articles and Briefings

Andrew, Brad T. *Army Intelligence Support to Homeland Security*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28 Issue 3, pp.48-51.

Cordesman, Anthony H. *Defending America: Redefining the Conceptual Borders of Homeland Defense*. Washington D.C.: Center for Strategic and International Studies, Revision, December 12, 2000.

Duncklee, Elizabeth M. & McKnight, Jeremy J. *Counterintelligence Technical Capabilities for Homeland Security*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, p 21.

Fuller, Brian. *Military Intelligence in Need of Overhaul*. Electronic Engineering Times, 17 September, 2001, Issue 1184, pp. 1-2.

Gilbert, James L. *In '77, Command Created New Identity*. Fort Belvoir, VA: INSCOM Journal, Summer 2002, Vol. 25, No.2, p. 14-16.

Harlan, Charles. *United States Army Counterintelligence Center Support to Homeland Security*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, pp. 17-18.

Harper, James. *Personnel for the United States Northern Command*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, p. 43.

Harris, Bernadette. *United States Department of Homeland Security*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Apr-Jun 2003, Vol. 29, Issue 2, pp. 27-29.

Ikle, Fred C. *Defending the United States Homeland: Strategic and Legal Issues for DoD and the Armed Services*. Washington D.C.: Center for Strategic and International Studies, January 1999.

Jones, Jerry W. *ISR Support to Force Protection*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Apr-Jun 2003, Vol. 29, Issue 2, pp. 5-12.

Luikart, Kenneth A. *Transforming Homeland Security*. Washington D.C.: Air & Space Power Journal, Summer 2003, Vol. 17, Issue 2, pp. 69-77.

Noonan, Robert W. *Collecting Information on United States Persons*. (extract) Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol.28, Issue 3, p. 9.

Palaganas, Arthur F. *The 902ⁿᵈ Military Intelligence Group's ACE-A Center for Information Fusion and Situational Awareness*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol.28, Issue 3, pp. 19-20.

Peters, Katherine M. *Troops on the Beat*. Washington D.C.: Government Executive, April 2003, Vol. 35, Issue 5, pp. 56-60.

Pratt, Ginger T. *The 902ⁿᵈ Military Intelligence Group and Homeland Security*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, pp. 15-16.

Smith, Regan K. *Homeland Security: An Intelligence Oversight Perspective*. Fort Huachuca, AZ: Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3, pp. 5-8.

Steele, Robert D. *Studies in Asymmetry, The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Non-Traditional Threats*. Washington D.C.: Strategic Studies Institute, Feb 2002.

Tulak, Arthur N., Kraft, Robert W., & Silbaugh, Don. *State Defense Forces and Homeland Security*. Carlisle Barracks, PA: Parameters, United States Army War College Quarterly, Winter 2003-2004, Vol. XXXIII, No. 4, pp. 132-146.

Monographs, Theses, and Reports

Baker, Donald L. *Terrorism-A New Age of War: Is the United States up to the Challenge?* Carlisle Barracks, PA: United States Army War College, April 9, 2003.

Jackson, Mark A. *Domestic Threat Intelligence Management*. Fort Leavenworth, KS: United States Army Command and General Staff College, June 2001.

Kelly III, Patrick. *Intelligence Support to Homeland Security: Supporting the Supporting Effort*. Carlisle Barracks, PA: United States Army War College, April 9, 2003.

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

Schalch, Margaret E. *Intelligence Reform: The Phoenix of 9/11?* Carlisle Barracks, PA: United States Army War College, April 7, 2003.

Valle, Ramon. *Is a Deployable Joint Task Force Augmentation Cell (DJTFAC) a Viable Tool for US Northern Command During Consequence Management Operations?* United States Army Advanced Operational Arts Studies Fellowship, Fort Leavenworth, KS 2003.

Vandaveer, Joan B. *Revamping the Operations Center Concept in the Intelligence Community for the 21ˢᵗ Century*. Carlisle Barracks, PA: United States Army War College, August 2002.

Books

Berkowitz, Bruce D. & Goodman, Allan E. *Strategic Intelligence for American National Security*. Princeton, New Jersey: Princeton University Press, 1989.

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations*. 6ᵗʰ ed. Chicago: University of Chicago Press, 1996.

Websites

"Army Intelligence and Security Doctrine." Federation of American Scientists. Available from http://www.fas.org/irp/doddir/army. Internet. Accessed on August 27, 2003.

Department of Homeland Security. Available from http://www.dhs.gov. Internet. Accessed on January 13, 2004.

El Paso Intelligence Center. Available from http://www.usdoj.gov/dea/programs/epic.htm. Internet. Accessed on February 24, 2004.

Global Security. Available from http://www.globalsecurity.org. Internet. Accessed on March 9, 2004.

Headquarters, United States Army Intelligence and Security Command. Available from http://www.inscom.army.mil. Internet. Accessed on January 13, 2004.

Headquarters, United States Northern Command. Available from http://www.northcom.mil. Internet. Accessed on January 13, 2004.

Joint Terrorism Task Force, Columbia. Available from http://columbia.fbi.gov/jttf.htm. Internet. Accessed on March 9, 2004.

Joint Terrorism Task Force, San Antonio. Available from http://sanantonio.fbi.gov/jttf.htm. Internet. Accessed on March 9, 2004.

National Drug Intelligence Center. Available from http://www.usdoj.gov/ndic/about/htm#The. Internet. Accessed on February 24, 2004.

United States Air Force Office of Special Investigations. Available from http://www.dtic.mil/afosi/about.html. Internet. Accessed on March 9, 2004.

World History Encyclopedia. Available from http://www.worldhistory.com. Internet. Accessed on February 23, 2004.

902nd Military Intelligence Group. Available from http://www.inscom.army.mil/902nd/index.asp. Internet. Accessed on January 13, 2004.