NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE EVOLUTION OF REGIONAL COUNTERTERRORISM CENTERS WITHIN A NATIONAL COUNTERTERRORISM NETWORK:

IS IT TIME TO FUSE MORE THAN INFORMATION?

by

Ron Leavell

March 2007

Thesis Advisor:	Robert Simeral
Second Reader:	Chris Bellavita

~~**Distribution Authorized to U.S. Government Agencies and their Contractors; (Operational Use); (March 2007). Other requests for this document must be referred to President, Code 261, Naval Postgraduate School, Monterey, CA 93943-5000 (or the Commander of Criminal Intelligence Section, Seattle Police Department) via the Defense Technical Information Center, 8725 John J. Kingman Rd. STE 0944, Ft. Belvoir, VA 22060-6218.**~~

Approved for public release; Distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

September 12, 2008

SUBJECT: Change in distribution statement for *Evolution of Regional Counterterrorism Centers within a National Counterterrorism Network* – March 2007.

1. Reference: Leavell, Ron. *The Evolution of Regional Counterterrorism Centers within a National Counterterrorism Network: Is It Time To Fuse More Than Information?* Monterey, CA: Naval Postgraduate School, March 2007. UNCLASSIFIED [Distribution Authorized to U.S. Government Agencies and their Contractors]

2. Upon consultation with NPS faculty, the School has determined that this sanitized thesis (pp. 114-117 marked out) may be released to the public and that its distribution is unlimited, effective September 8, 2008.

University Librarian
Naval Postgraduate School

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2007	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE The Evolution of Regional Counterterrorism Centers Within a National Counterterrorism Network: ***Is It Time To Fuse More Than Information?***	5. FUNDING NUMBERS
6. AUTHOR (S) Ron Leavell	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
~~Distribution Authorized to U.S. Government Agencies and their Contractors; (Operational Use); (March 2007). Other requests for this document must be referred to President, Code 261, Naval Postgraduate School, Monterey, CA 93943-5000 (or the Commander of Criminal Intelligence Section, Seattle Police Department) via the Defense Technical Information Center, 8725 John J. Kingman Rd. STE 0944, Ft. Belvoir, VA 22060-6218.~~ Approved for public release; Distribution is unlimited	~~C~~ A

13. ABSTRACT (maximum 200 words)

There is widespread consensus among both policymakers and intelligence professionals that domestic counterterrorism efforts remain hampered by the lack of an effective national intelligence network that fully integrates the Homeland's entire intelligence assets and other related Homeland Security capabilities into one national counterterrorism system. The failure to unify our domestic counterterrorism efforts inhibits timely and complete information sharing and the evolution of a more robust Homeland Security prevention and response capacity.

To achieve counterterrorism synergy we need a holistic approach that removes the intelligence element from its vacuum and fuses it in the counterterrorism crucible, along with the investigations element and related Homeland Security prevention and response operational elements, in **R**egional **A**ll-Hazards, **D**isaster and **A**nti-Terrorism **R**esource (**R.A.D.A.R.**) centers. These regional and super-regional **R.A.D.A.R.** centers can then be united into a National Counterterrorism Network under the auspices of the National Counterterrorism Center and the National Operations Center. Fusing this multi-government level, multi-disciplinary collaboration of intelligence, investigative and operational assets, along with the resources of key private sector groups into one unified organism would eliminate information sharing barriers, and will ensure the most efficient and effective use of Homeland Security resources to prevent and respond to terrorist attacks and natural disasters.

14. SUBJECT TERMS Anti-Terrorism; Investigations; Operations; Fusion Center; Counterterrorism; Domestic Counterterrorism; Multi-Disciplinary; National Counterterrorism Network; Regional Counterterrorism Centers; Intelligence Centers; Collaboration, Intelligence; All-Crimes; All-Hazards	15. NUMBER OF PAGES 155
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL ~~UL~~

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

THIS PAGE INTENTIONALLY LEFT BLANK

~~**Distribution Authorized to U.S. Government Agencies and their Contractors; (Operational Use); (March 2007). Other requests for this document must be referred to President, Code 261, Naval Postgraduate School, Monterey, CA 93943-5000 (or the Commander of Criminal Intelligence Section, Seattle Police Department) via the Defense Technical Information Center, 8725 John J. Kingman Rd. STE 0944, Ft. Belvoir, VA 22060-6218.**~~

Approved for public release; Distribution is unlimited

THE EVOLUTION OF REGIONAL COUNTERTERRORISM CENTERS WITHIN A NATIONAL COUNTERTERRORISM NETWORK:

IS IT TIME TO FUSE MORE THAN INFORMATION?

Ron Leavell
Lieutenant, Seattle Police Department
B.A., St. Johns University, 1980
J.D., Seattle University Law School, 1990

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
March 2007

Author: Ron Leavell

Approved by: Robert Simeral
Thesis Advisor

Chris Bellavita
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

There is widespread consensus among both policymakers and intelligence professionals that domestic counterterrorism efforts remain hampered by the lack of an effective national intelligence network that fully integrates the Homeland's entire intelligence assets and other related Homeland Security capabilities into one national counterterrorism system. The failure to unify our domestic counterterrorism efforts inhibits timely and complete information sharing and the evolution of a more robust Homeland Security prevention and response capacity.

To achieve counterterrorism synergy we need a holistic approach that removes the intelligence element from its vacuum and fuses it in the counterterrorism crucible, along with the investigations element and related Homeland Security prevention and response operational elements, in **R**egional **A**ll-Hazards, **D**isaster and **A**nti-Terrorism **R**esource (**R.A.D.A.R.**) centers. These regional and super-regional **R.A.D.A.R.** centers can then be united into a National Counterterrorism Network under the auspices of the National Counterterrorism Center and the National Operations Center. Fusing this multi-government level, multi-disciplinary collaboration of intelligence, investigative and operational assets, along with the resources of key private sector groups into one unified organism would eliminate information sharing barriers, and will ensure the most efficient and effective use of Homeland Security resources to prevent and respond to terrorist attacks and natural disasters.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. PROBLEM STATEMENT....1
- B. RESEARCH QUESTIONS....2
- C. OBJECTIVES....2
- D. AUDIENCE....2
- E. SIGNIFICANCE OF RESEARCH....3
- F. HYPOTHESES....3

II. METHODOLOGY....7

III. THE COUNTERTERRORISM CHALLENGE....9
- A. AN OVERVIEW OF THE STATE OF THE AMERICAN INTELLIGENCE AND COUNTERTERRORISM COMMUNITY....10
  - 1. The Definitional Struggle....11
  - 2. The "Intelligence Cycle"....13
  - 3. The Intelligence Community....17
  - 4. Federal Intelligence Community....17
  - 5. The Domestic Intelligence Community....18
- B. THE COUNTERTERRORISM TRIAD....20

IV. EFFORTS AT REFORMING THE NATION'S DOMESTIC COUNTERTERRORISM STRUCTURE....23
- A. THE IMPETUS FOR REFORM....24
- B. A COMMUNITY IN NAME ONLY....27
  - 1. Coordinating the Federal Intelligence Community....28
  - 2. Intelligence Reform and Terrorism Prevention Act Reform Efforts....28
  - 3. National Counterterrorism Center....31
- C. REFORMING THE DOMESTIC COUNTERTERRORISM COMMUNITY....31
  - 1. Defining Mission Spaces....32
  - 2. Remaking the Federal Bureau of Investigation....33
  - 3. Where's A Cop When You Need One? The Role of State, Local and Tribal Authorities in Counterterrorism....39

V. EVOLUTIONARY ROADBLOCKS - THE STRUGGLE TO COLLABORATE....43
- A. COLLABORATION....43
- B. FEDERAL CENTRIC ISSUES....45
- C. INTEGRATION OF STATE, LOCAL AND TRIBAL RESOURCES INTO THE COUNTERTERRORISM COMMUNITY....47
  - 1. All Terrorism Is Local....48
  - 2. Prevention Is Paramount....49
  - 3. Hometown Security Is Homeland Security....49

4. Homeland Security Strategies Must Be Coordinated Nationally, Not Federally 50
5. The Importance of Bottom Up Engineering, the Diversity of the State, Tribal and Local Public Safety Community and Non-Competitive Collaboration 50
D. DISSEMINATION ISSUES 51
E. CIVIL LIBERTY AND PRIVACY CONCERNS 56
F. MILITARY –CIVIL INTELLIGENCE SHARING 60

VI. EMERGING FROM THE PRIMORDIAL SOUP-THE ROAD TO COLLABORATION 61
A. EARLY COLLABORATIVE EFFORTS 63
1. Joint Terrorism Task Forces 63
2. Terrorism Early Warning Groups 64
3. Field Intelligence Groups 65
B. THE EMERGENCE OF FUSION CENTERS 66
C. THE INFORMATION SHARING ENVIRONMENT 71
1. Interagency Threat Assessment and Coordination Group 73
2. Fusion Center Focus 75
3. Integrated National Fusion Center Network 76
D. PUBLIC-PRIVATE PARTNERSHIPS 78

VII. EVALUATING EVOLUTIONARY PROGRESS 81

VIII. RECOMMENDATIONS- WINNING THE CO-EVOLUTION RACE 91
A. FROM REDUCTIONISM TO HOLISM –ACHIEVING SYNERGY 92
B. HYBRIDIZING A COLLABORATIVE COUNTERTERRORISM MODEL- FUSING MORE THAN INFORMATION 93
C. R.A.D.A.R. CENTERS 94
1. Regionalism and Collaboration 94
2. Governance 96
3. Multi-disciplinary -- Terrorism Early Warning 98
4. Co-location and Collaboration 100
5. Subject Matter Coverage 103
a. The "All Crimes" Approach 103
b. "All Hazards" 104
6. Component Groups 104
a. Intelligence and Investigations Components 105
b. Operations Component 106
7. "Primary" versus "Secondary" Centers 107
D. A NATIONAL COUNTER TERRORISM NETWORK 108
E. PERSONAL PRIVACY AND CIVIL LIBERTIES PROTECTION 112
F. ~~PROPOSED PILOT PROJECT~~ 114

IX. RECOMMENDATIONS FOR FURTHER RESEARCH 119

X. CONCLUSIONS 121

LIST OF REFERENCES **125**
INITIAL DISTRIBUTION LIST **135**

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. The Intelligence Cycle 13
Figure 2. Pre and Post-9/11 Federal Intelligence Community Structure 30
Figure 3. FBI National Security Branch- FBI 38
Figure 4. Classification/Declassification Historical View 52
Figure 5. Figure-Information Sharing Environment as Proposed in 2006 Implementation Plan 77
Figure 6. Length of Jail Sentences for Terrorism Related Crimes – TRAC 84
Figure 7. Number of Terrorism Related Prosecution - TRAC 85
Figure 8. **RADAR** Center Component Groups 105
Figure 9. Potential RADAR center cluster within a National Counterterrorism Network.....109
Figure 10. FEMA Regional Offices 111
Figure 11. Proposed National Counterterrorism Network 112

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. The "INT's" from FBI's Directorate of Intelligence 15
Table 2. Federal Intelligence Community and associated missions 18
Table 3. Law Enforcement Agencies and Officers 48
Table 4. Operating ISAC's, as of July 2006 80

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

CIA	Central Intelligence Agency
CRS	Congressional Research Service
COMINT	Communications Intelligence
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
ELINT	Electronic Intelligence
EPB	Emergency Preparedness Bureau
FIG	Field Intelligence Group (FBI)
FBI	Federal Bureau of Investigation
FOUO	For official use only
GEOINT	Geospatial intelligence
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HUMINT	Human intelligence
IALEIA	International Association of Law Enforcement Intelligence Analysts
IMINT	Imagery intelligence
ITACG	Interagency Threat Assessment and Coordination Group (NCTC)
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAC	Information Sharing and Analysis Center
ISC	Information Sharing Council
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LEIU	Law Enforcement Intelligence Unit
MASINT	Measurement and signatures intelligence

NCISP	National Criminal Intelligence Sharing Plan
NCN	National Counterterrorism Network
NRCC	National Response Coordination Center
NCTC	National Counterterrorism Center
NIC	National Intelligence Council
NIP	National Intelligence Program
NIS	National Intelligence Strategy
NOC	National Operations Center (DHS)
NORTHCOM	Northern Command
NSA	National Security Agency
NSB	National Security Branch (FBI)
NSC	National Security Council
NSS	National Security Strategy
OSINT	Open-source intelligence
PCII	Protected Critical Infrastructure Information
PHOTINT	Photo intelligence
RADAR	Regional All-hazards, Disaster and Anti-terrorism Resource
SIGNIT	Signals intelligence
TECHINT	Technical intelligence
TEW	Terrorism Early Warning
TLO	Terrorism Liaison Officer
TTIC	Terrorist Threat Integration Center
WMD	Weapons of Mass Destruction
WTC	World Trade Center

ACKNOWLEDGMENTS

I would like first to acknowledge the Department of Homeland Security for its generous support and funding of the Masters in Security program, and the Naval Postgraduate School, Center for Homeland Defense and Security, for the creation and administration of this program. Both entities have collaborated to create the nation's premier Homeland Security program, without which, working professionals like me would be unable to develop and share expertise in such an effective manner.

Of course, behind these entities are the people that make a successful program possible and determine the quality of the program. From the tremendous support staff of Heather Issvoran, Mark Fish, Debby Miller and Tom Mastre, to the academic staff of instructors--bright, dedicated and committed to our success--to the "quality control guru," Bill Pelfrey, I have not worked with a more pleasant and talented group. In particular, I want to thank my thesis team for their encouragement and guidance: Captain Robert Simeral for sharing his invaluable insights from his career as an intelligence professional, Doctor Chris Bellavita for teaching me that critical thinking about Homeland Security is more important than knowledge of technical details, and Doctor Lauren Wollman for guiding me through the writing labyrinth when I floundered. Finally, Greta Marlatt deserves special recognition for her outstanding research support and her status as my footnote savior.

My classmates in both cohorts were a welcome oasis of intellectual talent, passion, and humor that left me optimistic about the future of Homeland Security. My greatest progress as a Homeland Security student came from listening to their insights and perspectives.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In the immediate aftermath of September 11, it is understandable that we would experiment with a myriad of new counterterrorism architecture designed to overcome the defects in our national framework that led to the successful attacks. It is also understandable that much of the new structures would be hastily constructed because the exigency of the situation demanded we quickly develop solutions to shelter the Homeland. Nonetheless, almost six years later, in the rush to solve the problems identified by the 9/11 Commission and others, not enough time and other resources have been devoted to an inspection of the effectiveness of the pre and post 9/11 counter-terrorism structures to ensure that our counterterrorism and Homeland Security organisms have adapted and evolved to where they need to be.

There is a consensus that, while we have improved information sharing and intelligence analysis, there are still enormous gaps in these and other aspects of our national counterterrorism strategy. Moreover, the ever-growing number of new counterterrorism organizations, such as fusion centers, is consuming an ever-increasing amount of likely decreasing Homeland Security dollars and resources. In terms of counterterrorism, we are also well beyond the "alarmed discovery and euphoric enthusiasm" stage of the issue-attention cycle. We have been through the shock and awe of "realizing the cost of significant progress." We have felt the "gradual decline of public interest," and we are now firmly settled into the prolonged limbo of the "post-problem stage," where counterterrorism only sporadically captures the national interest.[1] This environment thus cries out for a retrospective examination. It is now time to take stock of the strengths and weaknesses of what has evolved, including the newest counterterrorism progeny, fusion centers.

[1] For an explanation of the issue attention cycle by its author, see Anthony Downs, *Political Theory and Public Choice* (Northampton, MA: Edward Elgar, 1998), 100-112.

B. RESEARCH QUESTIONS

The research will attempt to answer several questions: What is the current state of our domestic counterterrorism efforts? Are the Joint Terrorism Task Force and Fusion Center models fine-tuned enough for the domestic threat environment? Alternatively, is there something still missing in the gene pool of our Homeland Security organisms? Is future development of a unified model feasible or desirable? Intertwined with this question, how well are we addressing the subsets of intelligence, investigations, and operations?

The research questions are further focused on finding out what entities should be included in a potential National Counterterrorism Network (NCN), and how such a network would be constructed. For example, would "regionalizing" our approach produce better results? If so, how might "a region" best be defined in geographical terms? Which disciplines or entities should be included, and how would the difficult task of governance be addressed? What are the implications for civil liberties and privacy?

C. OBJECTIVES

In studying current and proposed collaborative and single entity counterterrorism structures and networks, I will identify the positive and negative aspects that should lead to a "best practices" approach. This best, or at least "smart," practices approach will present policy options that can be applied to both improve existing entities and to aid in the creation of a National Counterterrorism Network.

D. AUDIENCE

The audience for this research includes the entities currently funding, overseeing or participating in domestic counterterrorism intelligence, investigations or operations, as well as those contemplating participating in or creating such organizations. This research will be applicable to all levels of government, federal, state, local and tribal, as well as a broad array of Homeland Security disciplines, including law enforcement, public health, fire, emergency management, private sector security and interested members of the

public. In particular, the Department of Homeland Security and others are searching for ways to vertically and horizontally integrate our disparate national counterterrorism resources, and this research will be especially relevant to that effort.

E. SIGNIFICANCE OF RESEARCH

The significance of this research is that while we have made substantial progress since 9/11, there is a consensus that we are still not sharing information effectively, and there is considerable question as to the best model for conducting counterterrorism intelligence, investigations and operations. Since there is limited evidence that al Qaeda or any "organized serious group" has attempted further attacks against the United States on American soil, we don't know if we have undertaken effective anti-terrorism measures, or if our systems simply have not been tested. Since it is a "pass-fail" system, we ought not to defer to al Qaeda to do the examination. We need to ensure we are not simply following a "check box" approach in having each state create a "fusion center," and agencies participate in "joint terrorism task forces." There is a need to identify remaining issues and potential solutions to ensure that these and other counterterrorism structures are maximizing our counterterrorism capacity.

F. HYPOTHESES

This thesis will explore the following five central hypotheses in researching current and proposed domestic counterterrorism structures and systems.

1) <u>Despite progress since 9/11, we have to continue to critically examine the efficacy of our current strategies in order to conclude whether there is evidence that our new domestic counterterrorism strategy is effective in preventing and responding to terrorism, or simply untested.</u>

When considering potential policy options that we can apply to our counterterrorism efforts, one of those options will be to maintain the status quo. One can argue that since there have been no further attacks, our current systems are effective. Therefore, whether the lack of attacks is due to successful interdictions, or simply because al Qaeda has not decided to launch attacks is an important consideration. To the extent that we can answer this question, it would help determine to what extent our current structures are effective in preventing attacks.

On the other hand, if, if there is no evidence of an organized effort to launch serious attacks accompanying this time of domestic "tranquility," we don't know if our newly evolved counterterrorism structures to detect, prevent and interdict such attacks have the right adaptations. Because of the potential catastrophic consequences of a successful attack, e.g., a WMD attack, a critical examination of the strengths and successes, along with the weaknesses and vulnerabilities of our current efforts is imperative. To aid this examination, we need to consider both quantitative and qualitative approaches.

2) The integration of Intelligence with related Homeland Security components such as Investigations and Operations may have a synergistic effect on counterterrorism efforts that maximizes our nation's prevention and response capacity

Most of our current counterterrorism structures isolate the intelligence function in intelligence or fusion centers, separating intelligence from investigative components and operational elements. For example, a Joint Terrorism Task Force (JTTF) is primarily an *investigative* group, operating under a different command structure and organization than most fusion centers, which focus primarily on *intelligence*. Both fusion centers and JTTF's are separated physically and organizationally from most *operational* components, such as first responders. If we combine these three counterterrorism elements, the resulting synergy should provide substantial benefits such as timelier sharing of information from intelligence components to operational components, more efficient targeting of investigative and operational resources based on intelligence needs and vice-versa, etc.

3) Our counterterrorism effectiveness will increase by adoption of a fully collaborative multi-level, multi-discipline effort.

Even though nearly all participants and organizations pay homage at the altar of collaboration, the design of our counterterrorism structures may inhibit achieving the full benefits of a fully collaborative approach. A fully collaborative approach entails controversial concepts such as joint governance, joint decision-making, and resource sharing. Collaborations that are more fulsome will produce the necessary trust and relationships for more timely and complete information and resource sharing, and enable operational responses that are more effective. The research associated with this thesis will ascertain to what extent Homeland Security stakeholders feel their participation

comprises a true and effective collaboration, and identify barriers to more effective efforts among the various Homeland Security disciplines and levels of government. We will explore options that overcome these barriers.

4) Regionalism within an "all-hazards" framework is a cornerstone to establishing effective counterterrorism centers.

America has tens of thousands of political subdivisions, many of which have their own separate police, fire, health and other Homeland Security structures. Overlaying this morass is an increasing amount of disparate intelligence and counterterrorism structures such as fusion centers. As a prerequisite to forming a National Counterterrorism Network, we need to organize the multitude of counterterrorism entities that exist, and continue to proliferate. This is integral in order to share information and resources in a timely and complete fashion. It is also central to the successful application of every step of a national intelligence cycle.[2]

Because of declining funding levels, a ubiquitous shortage of personnel, and desirable economies of scale and efficiencies, a *regional*, rather than a local or state approach, will likely be necessary to form the foundation of an effective national counterterrorism effort. Furthermore, we might best form and strengthen the partnerships and relationships integral to counterterrorism within the sandbox of "all-hazards" where Homeland Security stakeholders more commonly interact with each other. It is also more efficient to use existing structures, relationships and resources for both terrorism and other hazards when feasible. This thesis research will assist in defining considerations for identifying regional boundaries, regional partners, and potential organizational structures.

5) Our "regionalized" structures need to be horizontally and vertically integrated under the auspices of a national counterterrorism network to ensure more effective information sharing, intelligence analysis, and coordination of investigations and operations.

Despite progress in improving information sharing since 9/11, there are still enormous battles over turf, funding, and control. This results in information silos, inefficient use of our limited counterterrorism resources, and a lack of coordination of investigative, intelligence and operational resources. Without some kind of national system or network, there is unlikely to be an effective way to overcome the long history

[2] See Chapter III A.2.

of collaboration problems among legacy groups, such as the CIA, FBI, etc., as well as newcomers such as the DHS. The sovereign struggle between federal, state, tribal and local officials will also likely remain problematic without a structure to unite efforts into a national system. Moreover, even if a utopian vision of collaboration and harmony reigns in our regions, there will still be a need for a network structure to connect and coordinate the various regions.

II. METHODOLOGY

Homeland Security is a young enough field that it remains more art than science so I will assess the research hypotheses by several methods. One will be by interviews of subject matter experts, augmented with my informed observation from several years as a Homeland Security and intelligence professional. There is also a wealth of published research and commentary on the various components of Homeland Security and counterterrorism to dissect and review. Additionally, there is available empirical data to determine the nature and extent of finished intelligence products we are producing. Finally, surveys of stakeholders, such as Homeland Security practitioners and consumers of intelligence, exist that will also help to measure effectiveness of current systems by metrics such as work products received from various entities, satisfaction scales, and significant operational or investigative successes.

To narrow the scope to a manageable level, this paper will also focus on the prevention side of the counterterrorism house, as compared with a preparation and response focus. In doing so, I will review intelligence and related anti-terrorism disciplines, such as operations and investigations, that appear to have a synergistic potential. There is a substantial amount of scholarly literature, as well as editorial and policymaker analysis on this subject. I will supplement this written research with on-site visits and/or interviews of multiple counterterrorism (CT) entities and participants, including the Arizona Counter Terrorism Information Center (ACTIC), the National Capital Region Intelligence Center, Illinois Statewide Terrorism Intelligence Center (STIC), and the Los Angeles Joint Regional Intelligence Center (LAJRIC).

I expect this approach to produce an understanding of and insight into the beneficial and detrimental aspects of our nation's current counterterrorism efforts. The primary goal is to develop a smart/best practices foundation in order to provide the basis for policy recommendations to improve our domestic Homeland Security position. This will necessitate presenting an analysis of the primary problems identified in the post 9/11 reviews, the major efforts initiated because of the attacks, and potential options that remain.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE COUNTERTERRORISM CHALLENGE

The nature of Homeland Security and its offspring of counterterrorism will likely always remain more an art than a science, but we still need to be rigorous in our examination of the domestic counterterrorism challenge. One of the difficulties is the ad hoc nature of much of the counterterrorism process, where many parts have developed in isolation for specialized purposes without any coordinated policy or effort, e.g., the myriad of stand-alone intelligence groups in various jurisdictions. Other aspects of reform reflect a systemic effort, such as creating a Homeland Security Information Network. The objectives and appropriate metrics of each approach are very different.

Another challenge in examining domestic counterterrorism efforts is that legacy effects of the larger counterterrorism arena, especially long-standing difficulties in the intelligence field, still impact newly created counterterrorism structures. Therefore, in attempting to discern the strengths and weaknesses of our embryonic Homeland Security counterterrorism efforts, our examination can benefit from borrowing an analytical tool from the science of biology and applying an "evo-devo" approach to studying the effectiveness of our current Homeland Security efforts. "Evo-devo" (or "evolutionary developmental biology") emerged as a discipline in the late 1990's and involves the scientific study of both the individual organism's development and the evolution of the organism's lineage to gain new insights. Evo-devo identifies the origin *and* evolution of embryonic development and describes how modifications of developmental processes lead to the production of new features and sometimes new organisms.

Since our domestic counterterrorism effort is at an embryonic stage, still developing new features, but also carries the "genes" of previous structures and systems, that impact those new features, an "evo-devo" approach is well-suited for our examination. An "evo-devo" approach to Homeland Security would involve studying the evolution of key counterterrorism fields, such as intelligence, investigations and operations as well as the development of specific key "organisms," such as the fusion centers and JTTF's. This approach would ideally provide the necessary insight to identify

not only the beneficial and detrimental traits in our current national, regional, and local counterterrorism efforts, but also the causes behind the development of these traits so that we can develop a model that corrects the flaws and replicates the strengths.

Accordingly, our examination will include a review of the foundational elements or "genetic code" of the counterterrorism process, especially focused on intelligence and its cousin--information sharing. This will be followed by an assessment of how well counterterrorism organisms have adapted to their new environment, dissecting perceived strengths and weaknesses of our current reform efforts, particularly the nascent fusion center effort. Finally, we will scrutinize some possible evolutionary paths that may develop an even stronger domestic counterterrorism organism.

A. AN OVERVIEW OF THE STATE OF THE AMERICAN INTELLIGENCE AND COUNTERTERRORISM COMMUNITY

Though the outward appearances vary, nearly all counterterrorism efforts share some common genetic material integral to understanding their resulting characteristics and potential. Highlighting and defining certain key aspects of intelligence and related anti-terrorism components is necessary for a thorough analysis in later chapters of how well America has adapted to the "new normalcy" as the Gilmore Commission describes our national threat environment after 9/11.[3] This new normalcy acknowledges that the threat of terrorism will not disappear, and thus a critical examination is called for to ascertain the strengths and weaknesses of our domestic intelligence and counterterrorism community.

It is beyond the scope of this thesis to present an exhaustive review of the entire national intelligence effort, or even to be a primer on intelligence.[4] Instead, we will focus on examining the elements of the intelligence branch of the family counterterrorism tree that explain specific issues of controversy, or that lay a foundation for discussions in subsequent chapters regarding perceived weaknesses and gaps in our current reform efforts. For example, when we examine "information-sharing" problems, we need to

[3] Gilmore Commission Report, *Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty* (Washington, DC: RAND, 2003).

[4] For an excellent in depth study of intelligence see Mark Lowenthal's book *Intelligence, From Secrets to Policy* (Washington, DC: CQ Press, 2006).

understand the essential difference between "information" and "intelligence," and we need to understand how privacy and civil liberties concerns have evolved along with the collection of intelligence and sharing of information.

1. The Definitional Struggle

There is no one definition of "counterterrorism," or "anti-terrorism" as some observers refer to it. Counterterrorism forms one of the six critical mission areas of Homeland Security, and the term encompass a broad array of practices, tactics, and strategies that all levels of government and the public and private sector undertake to combat terrorism.[5] Though some argue that "counterterrorism" implies a more aggressive posture, i.e., *offensive* measures taken to prevent, deter, and respond in combating terrorism, than "anti-terrorism," which can be thought of as *defensive* measures used to reduce the vulnerability of people and property to terrorist acts, the literature generally treats the terms synonymously, and they will be so used in this thesis

What is "intelligence?" Definitions abound. The National Criminal Intelligence Sharing Plan (NCISP) defines it as "information that has been analyzed to determine its meaning and relevance."[6] Former Assistant Director of Central Intelligence, Mark Lowenthal, makes some important points in this somewhat cumbersome but illuminating definition:

> Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.[7]

Notice that this definition makes the salient point that intelligence includes "the carrying out of operations…." This reinforces the discussion in the preceding sections in which the integration of intelligence components with operational components is posited

---

[5] *National Strategy for Homeland Security* (Washington, DC: Office of Homeland Security, July 2002) viii–x, at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (accessed December 14, 2006).

[6] United States. Department of Justice. *National Criminal Intelligence Sharing Plan* (Washington, DC: Bureau of Justice Assistance, October 2003), 28. Available at http://www.iir.com/global/products/NCISP_Plan.pdf (accessed January 19, 2007).

[7] Mark M. Lowenthal, *Intelligence, From Secrets to Policy* (Washington, DC: Congressional Quarterly Press, 2002 [second edition]), 8.

as an essential aspect of the counterterrorism effort. This definition also makes clear that intelligence is both *a product* and *a process*. This process, discussed below, is known as the "intelligence cycle." A basic understanding of the intelligence cycle is critical, as this cycle is what distinguishes two terms that are often mistakenly used interchangeably: "information" and "intelligence."

The distinction between "information" and "intelligence" is significant. Post-9/11, the mantra calling for "information-sharing" has led to distributing what Lisa M. Palmieri, President of the International Association of Law Enforcement Intelligence Analysts (IALEIA), calls "uncorroborated, unevaluated, 'white noise,'" that can derail counterterrorism efforts by drowning out significant intelligence.[8] Former Secretary of State Colin Powell is quoted as saying, "I don't need news. I don't need facts. I have a television. I have the Internet. I have a telephone. People tell me lots of facts. I need to know what it means, how important it is, what you think about it."[9]

Confusing information with intelligence can also lead to the phenomenon known as "circular reporting." Circular reporting occurs when two or more collectors get information from the same source but report the information independently. This leads to the false confirming of information, or the false conclusion that there is a "pattern" of certain suspicious behaviors.

The problem of circular reporting is particularly relevant to our discussion of the need for a National Counterterrorism Network that connects our ever-growing number of disparate fusion and intelligence centers, including the hypothesis that regionalizing our efforts within a national network is an important evolution. It is also pertinent to the call for integration of a multi-disciplinary, multi-agency, collaborative approach in order to develop a more united and coordinated intelligence cycle.

---

[8] Lisa M. Palmieri, Information vs. Intelligence: What Police Executives Need to Know, paper for IACP Annual Meeting, 2005.

[9] Thomas Fingar, quoting Colin Powell, conference presentation during The DNI's Information Sharing Conference and Technology Exposition, Denver, CO, August 21, 2006.

2. The "Intelligence Cycle"

The process of producing intelligence is commonly referred to as the "intelligence cycle." The intelligence cycle is the method by which raw information is converted into intelligence and made available to the targeted consumers, including policymakers, military planners, and, in the case of criminal intelligence, investigators.

There are six primary steps in the intelligence cycle: identifying needs and priorities, collecting information based on the identified needs, analysis, producing a finished intelligence product, disseminating that product, and getting feedback.

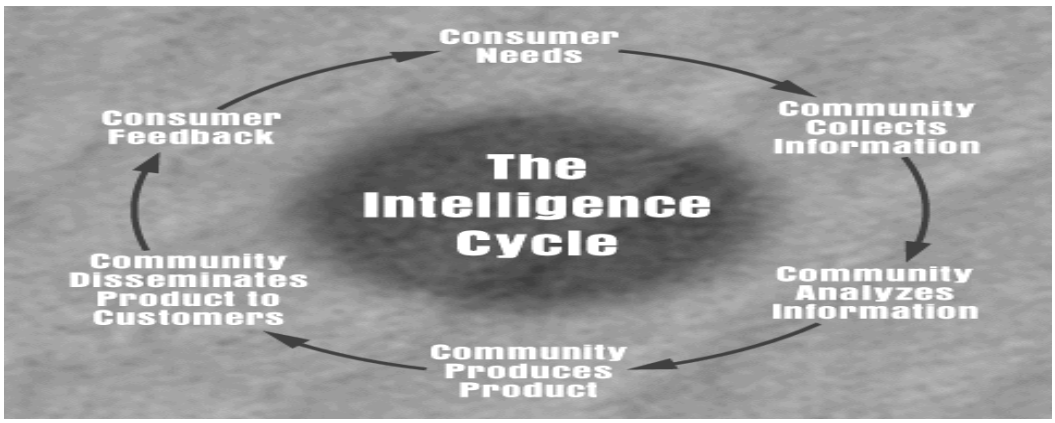


Figure 1. The Intelligence Cycle[10]

I. Needs assessment: This is where the intelligence cycle both begins and is usually renewed. The intelligence cycle begins here because it involves determination of the intended consumers' intelligence requirements, preparation of a collection plan, and direction to the collectors and collection system of what to collect.[11] It is also where the cycle begins anew because finished intelligence usually generates new requirements from the consumers who may have found the intelligence provided was insufficient. Alternatively, the finished intelligence product may have been useful, but further

[10] Commission on the Roles and Capabilities of the United States Intelligence Community. "An Overview of the Intelligence Community" in the *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. (Washington, DC: US Government Printing Office, 2000). Available at http://www.access.gpo.gov/intelligence/int/int023.html (accessed January 17, 2007).

[11] These are also commonly referred to as Identified Intelligence Needs (IIN's) or Identified Intelligence Requirements (IIR's).

intelligence needs have been identified. This needs/requirements stage focuses the next step--the collection of information. The consumers who drive this stage range from policymakers to individual investigators or operational users. As an example, the Director of National Intelligence (see below) issues the National Intelligence Priorities Framework (NIPF) to the federal intelligence community (IC)[12] to provide guidance on the national intelligence priorities approved by the President. The NIPF is updated twice a year with input from the federal IC and is a classified document.

There has been a post-9/11 epiphany that we need to move beyond a Cold War mentality regarding intelligence. In her upcoming book on intelligence reform, UCLA Professor Amy Zegart writes, "the U.S. intelligence community showed a stunning inability to adapt to the rise of terrorism after the Cold War ended"… "The Cold War had dominated both the thinking and operation of the CIA and the 13 other agencies of the U.S. intelligence community."[13]

In changing the Cold War mentality and adapting to our new threat environment, the nation's intelligence needs and requirements need to be driven by not only the traditional federal intelligence community, the military and high level policymakers, but by the broader Homeland Security community. The Homeland Security community is larger than just federal law enforcement officials and the military. It includes state, local, and tribal law enforcement, as well as such disciplines as Public Health, Fire Services, Utilities, Transportation, Emergency Management and Private Security. Changing our mentality therefore requires "opening the club" to groups and individuals that previously were locked out, since they were previously not seen as significant stakeholders, as either consumers or collectors of intelligence. As discussed in the next chapter, we are still struggling to move from the conceptual to the concrete in this arena.

II. Collection: This step involves collection of raw information and transfer to analytical components for production of finished intelligence products. It is at this stage

[12] The term "Intelligence Community" is generally used to refer to the group of sixteen federal government agencies that have a recognized role in national intelligence, e.g., the CIA and FBI, and the term is used in this manner here; however, who or what should actually comprise the "Intelligence Community" is discussed throughout this thesis as a central point of concern.

[13] Amy Zegart, excerpt from an upcoming book to be published, *Intelligence in Wonderland: 9/11 and the Roots of Failure,* from an online article available at http://www.international.ucla.edu/article.asp?parentid=31370 (accessed on December 4, 2006).

that civil liberty or privacy concerns are usually raised concerning whether a particular collection technique, e.g., surveillance of international telephone calls, is constitutionally sound or is violative of a right such as the Fourth Amendment warrant requirement or the First Amendment's protection of freedoms of expression.[14] These concerns are explored further in subsequent chapters. There are five main ways of collecting intelligence, often collectively referred to as "intelligence collection disciplines" or the "INT's."

Human Intelligence (HUMINT) is the collection of information from human sources. The collection may be done openly, as when FBI agents interview witnesses or suspects, or it may be done through clandestine or covert means (espionage). Within the United States, HUMINT collection is the responsibility of federal, state, and local law enforcement. Beyond U.S. borders, HUMINT is generally collected by the CIA, but also by other U.S. components abroad.

Signals Intelligence (SIGINT) refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites. Communications Intelligence (COMINT) is a type of SIGINT and refers to the interception of communications between two parties. U.S. SIGINT satellites are designed and built by the National Reconnaissance Office, although conducting U.S. signals intelligence activities is primarily the responsibility of the National Security Agency (NSA). The FBI collects SIGINT through authorized wiretaps and other electronic intercepts of information. Telemetry Intelligence (TELINT) is sometimes used to indicate data relayed by weapons during tests, while electronic intelligence (ELINT) can indicate electronic emissions picked up from modern weapons and tracking systems. Both TELINT and ELINT can be types of SIGINT and contribute to MASINT.

Measurement and Signatures Intelligence (MASINT) is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities. MASINT includes the advanced processing and use of data gathered from overhead and airborne IMINT and SIGINT collection systems.

Geospatial Intelligence (GEOINT) comprises the exploitation and analysis of satellite information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. GEOINT sources include imagery and is sometimes also referred to as imagery intelligence or IMINT or photo intelligence (PHOTINT). One of the earliest forms of IMINT took place during the Civil War, when soldiers were sent up in balloons to gather intelligence about their surroundings. It was practiced largely in World Wars I and II when both sides took photographs from airplanes. Today, the National Reconnaissance Office designs, builds, and operates imagery satellites, while the National Geospatial-Intelligence Agency is largely responsible for processing and using the imagery

Open-Source Intelligence (OSINT) refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).

Table 1. The "INT's" from FBI's Directorate of Intelligence[15]

[14] For a review of principal changes since 9/11 and the dangers they may pose, see Stephen J. Schulhofer. *The Enemy Within: Intelligence Gathering, Law Enforcement and Civil Liberties in the Wake of September 11* (Washington, DC: Century Foundation Press, 2002).

[15] "'INT's' – The Intelligence Collection Disciplines" Available at http://www.fbi.gov/intelligence/di_ints.htm (accessed November 12, 2006).

When it comes to collection, more is not necessarily better. At a recent intelligence conference, Thomas Fingar, Deputy Director of National Intelligence, called for systemic change in intelligence gathering and posited that U.S. intelligence collectors "have become vacuum cleaners on steroids," resulting in enormous amounts of unanalyzed data.[16] What's more, another speaker remarked that simply "placing more hay on the haystack doesn't make finding the needles any easier"[17]

III. Analysis: Analysis is perhaps the most critical phase in the intelligence cycle as this stage involves taking the raw data or basic information and converting it into intelligence. This "value added" process places the information in context, adds perspective, verification and corroboration. Finally, when it has been reviewed and correlated with information available from other sources, it is called "finished intelligence."

The explosion of new intelligence and analytical centers post 9/11 has fueled a huge demand for analysts, with the FBI alone adding over a thousand. This demand, coupled with the high skill level needed for competent analysis, has created a significant shortage of qualified analysts, and this shortage is recognized as one of our major problems in addressing counterterrorism gaps.[18]

IV. Production: Information has to be produced in a form useful to the consumer. Accordingly, this step includes preparation of a variety of finished intelligence products defined by the consumer's needs, including single-source, event-oriented reports, such as intelligence bulletins, and longer term, all-source, finished intelligence studies, such as strategic intelligence assessments.

V. Dissemination: Dissemination is the process of actually distributing a finished intelligence product to the intended consumers. This process involves both the technical means to distribute the product, such as using secure web based networks, faxes, telephones, etc., as well as the restrictions placed on who can receive the intelligence. Intelligence agencies must balance the need to share sensitive information,

---

[16] Bruce Finley, "Intelligence Fixes Floated at Conference" *Denver Post,* August 22, 2006.

[17] Ibid.

[18] "Intelligence Agencies Face Staff Shortage" *USA Today,* December 27, 2004.

including terrorism-related information, with the need to protect it from too widespread of an audience that might endanger sources, expose methods, or otherwise inhibit a counterterrorism operation or investigation.

To protect sensitive sources and methods, intelligence is distributed according to two basic tenets: the "need to know" (Does the recipient have a legitimate reason to receive the information?) and the "right to know" (Does the law allow the recipient to receive the information?). Additionally, legal restrictions involving the "classifying" of information may require a special security clearance to receive certain information. Dissemination issues are explored more fully in Chapter V.

VI. Feedback: This step is frequently omitted from discussion but it is essential in ascertaining whether the product disseminated met the identified needs or whether gaps or new needs were identified. These gaps or new needs stimulate new requirements, thus continuing the process or "cycle." Feedback also serves an important role in quality control. Consequently, the FBI and other agencies have begun sending customer surveys along with intelligence products to receive feedback.

3. The Intelligence Community

We often hear the term "intelligence community" used as though it was a monolithic entity, but more accurately, there are three intelligence communities.

- The military intelligence community centered on the Department of Defense,
- A foreign intelligence community centered on the CIA, and
- A domestic intelligence community centered on the Departments of Justice (the FBI) and Homeland Security, but also including state, local and tribal law enforcement, and arguably, the broad group of Homeland Security disciplines, such as Public Health, Fire, Transportation, Private Security, etc.

4. Federal Intelligence Community

The sixteen federal intelligence agencies are the ones that most of us think of when we hear the term "intelligence community." In fact, the federal intelligence

community, or "IC," is actually prescribed by law, first starting with the National Security Act of 1947, which established the CIA, and since modified by various presidential orders.

Agency	Mission
Air Force Intelligence	Intelligence related to military mission
Army Intelligence	Intelligence related to military mission
Central Intelligence Agency	Foreign intelligence and counterintelligence
Coast Guard Intelligence	Information related to maritime security and HLD
Defense Intelligence Agency	Defense attaches and overall defense issues for DOD
Department of Energy	Analyzes foreign nuclear weapons and non-proliferation, energy security
Department of Homeland Security	Fuses law enforcement and intelligence information and HLS threats
Department of State	Intelligence related to foreign relations
Department of the Treasury	Collects and process information that affects fiscal and monetary issues, including terrorism financing
Drug Enforcement Administration	Information and enforcement of controlled substance laws
Federal Bureau of Investigation	Domestic counterterrorism and counterintelligence
Marine Corps Intelligence	Information related to military mission
Nat'l Geo-Spatial Intelligence	Geo-spatial data including maps and other targeting data
National Reconnaissance Office	Operates our nation's reconnaissance satellites
National Security Agency	Signals collection and analysis
Navy Intelligence	Information related to military missions

Table 2. Federal Intelligence Community and associated missions

5. The Domestic Intelligence Community

Determining the proper composition of the domestic intelligence community is a central question to resolve to improve the nation's intelligence capacity. This section discusses the historical development of the domestic counterterrorism community at the time of 9/11.

The FBI has a unique role in that it is part of both the *federal* intelligence community as described previously, as well as the *domestic* intelligence community. The latter role arises since the Bureau has the primary responsibility for counterterrorism within the United States per presidential order.[19] Conventionally, the domestic intelligence community primarily consisted of solely the FBI.

Prior to 9/11, the Department of Homeland Security did not exist, and state, local and tribal law enforcement intelligence was generally not a significant part of the counterterrorism or national security effort. Rather, law enforcement intelligence was focused on intelligence as it related to criminal investigation aspects, not national security concerns. This absence of non-federal law enforcement involvement in national security developed when state and local law enforcement curtailed much of their intelligence activity in the 1970's in a backlash against real and perceived abuses. So called "red squads" had been formed in many major police departments to root out communists, but grand jury investigations and lawsuits uncovered illegal spying, illegal searches, and disinformation campaigns. According to research by David E. Kaplan:

> Americans engaged in constitutionally protected free speech were routinely photographed, wiretapped, and harassed--all in the name of national security. In Memphis, the police department spied on the National Association for the Advancement of Colored People and gathered data on political activists' bank accounts, phone records, and close associates. In New Haven, Conn., police wiretapped over a thousand people. In Philadelphia, then police chief Frank Rizzo boasted of holding files on 18,000 people. The list of "subversives" grew to include the League of Woman Voters, civil rights groups, religious figures, and politicians running for office.[20]

As a result, many law enforcement agencies shut their intelligence units down, or operated under onerous legislative restrictions. This exclusion of state, local and tribal police from the national security intelligence effort in the 1970's formed the stage for their absence from the counterterrorism arena when al Qaeda decided to strike the United

---

[19] George W. Bush, "United States Intelligence Activities" Executive Order 12333, December 4, 1981 at § 1.14(a).

[20] David E. Kaplan, "When the Cops Saw Only Red" *U.S. News and World Report,* May 8, 2006.

States in 2001. Much of our nation's reform efforts after 9/11 have been devoted to figuring out how best to reintegrate these forces back into the domestic arsenal.[21]

B. THE COUNTERTERRORISM TRIAD

While 9/11 may be primarily perceived as an intelligence failure and discussed as such, it is important to place the intelligence failures in the larger context of "counterterrorism." This is essential because, as the Joint Inquiry of Congress noted, the failure *to act* on the available intelligence was as important as the failure *to gather* intelligence.[22] Similarly, the Gilmore Commission noted the need for our national strategy to combat terrorism to include not only intelligence, but also "all key functional domains," and "it must be comprehensive, encompassing the full spectrum of deterrence, prevention, preparedness and response."[23]

The 9/11 Commission agreed with the conclusions of the Gilmore Commission regarding the need for a comprehensive approach encompassing more than just the intelligence domain.[24] Drawing on the conclusions of these commissions, and in analyzing the missions of the principal players in the various Homeland Security disciplines, three central components of counterterrorism emerge: intelligence, investigations and operations.

The anti-terrorism aspects of these three components are discussed in detail in the following chapters, but it is useful at this point to summarize them as follows:

---

[21] Though it will be discussed at length in following chapter on reforms, it's worthwhile to note at this juncture that while our nation's nearly 800,000 state, local, and tribal police were largely omitted from the intelligence community prior to 9/11, the membership chasm extended to a broad range of what we would now refer to as "Homeland Security disciplines," including Public Health, Fire, Private Security, and so on.

[22] Richard A. Best, Jr., *The Intelligence Community and 9/11: Congressional Hearings and the Status of the Investigation* (Washington, DC: Library of Congress, Congressional Research Service, January 16, 2003).

[23] Gilmore Commission, *Fourth Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Washington, DC: White House Office of the Press Secretary, December 15, 2002), 2.

[24] National Commission on Terrorist Attacks, *9 /11 Commission Report* (New York: W.W. Norton & Company, First Edition, 2004).

- "Intelligence" refers to the entire intelligence cycle, including identifying requirements or needs, collection, analysis, reporting, dissemination, and hopefully, feedback.
- "Investigations" are law enforcement authorities' attempts to solve crimes or attempted crime by investigation with the goal of arrest and prosecution. And,
- "Operations" comprises those concrete operational counterterrorism missions, such as interdiction or prevention by deploying operational forces, as well as response and recovery operations, such as a hazardous material clean up from a biological or chemical attack.

Thus, "counter" or "anti" terrorism can be thought of as a three-legged table that supports Homeland Security, with investigations, operations and intelligence forming the legs. Each leg of Homeland Security is interdependent. If one is missing, the table will fall. Likewise, if the table is of insufficient height or size to meet our needs, we cannot simply focus on raising or reshaping one of the legs—intelligence; the legs need to be coordinated with each other. Another useful analogy is to think of the trio synergistically and holistically, as three strands of a rope. The separate strands are by themselves insufficient to lift much weight, but combined as a whole, they have a much greater capacity.

To illustrate the interrelated and synergistic nature of the counterterrorism triad, the 9/11 context provides a classic, though tragic, example. In 9/11, even though salient and actionable intelligence existed, since it was not shared or coordinated with investigative or operational components, such as law enforcement agents, airport security or border patrol officers, it proved worthless. As a result, the opportunity to prevent the attack via a criminal investigation and or interdiction operation was lost.

This is not to diminish the importance of the intelligence component; indeed, it may be the most important part of the triad. Homeland Security Secretary Michael Chertoff has fittingly referred to intelligence as critical to the "all hazards mission" and the "radar of the 21st century,"[25] (a metaphor we will return to later in the Recommendations chapter). Additionally, the Commission on the Intelligence

[25] Remarks by the Secretary of Homeland Security Michael Chertoff *2006 Bureau of Justice Assistance, U.S. Department of Justice and SEARCH Symposium on Justice and Public Safety Information Sharing*, March 14, 2006. http://www.dhs.gov/xnews/speeches/speech_0273.shtm (accessed December 12, 2006).

Capabilities of the United States Regarding Weapons of Mass Destruction (also known as the WMD Commission) further remarked, "Every person with whom we spoke was unanimous on one point: there is nothing more important than having the best possible intelligence to combat the world's deadliest weapons and most dangerous actors."[26] Nonetheless, it remains that "intelligence" is a *necessary*, but not a *sufficient* condition for effective counterterrorism.

[26] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction *Report to the President of the United States* (Washington, DC: The Commission, March 31, 2005), 540.

IV. EFFORTS AT REFORMING THE NATION'S DOMESTIC COUNTERTERRORISM STRUCTURE

> *"The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew, and act anew. We must disenthrall ourselves, and then we shall save our country."*[27]
>
> Abraham Lincoln

In contrast to the bitterly divided America President Lincoln faced, our leaders have dealt with an America largely united in the righteousness of the anti-terrorism cause and in the belief that serious reform was necessary to protect the Homeland. Where parties differ, and sometimes appreciably, is their view of the nature and extent of the changes that are needed. Exacerbating the intellectual divide is that over five years have elapsed since the attacks, diminishing the sense of urgency, if not common purpose. On the positive side, the passage of time has brought perspective to apply to our reform efforts. What seemed useful or necessary may no longer be wise or there may be a better mousetrap.

In following Lincoln's admonition, this chapter will present the principal schools of thought on reforming the nation's counterterrorism architecture, including areas of concurrence and divergence. This will entail examining the primary problems that were identified as contributing to our collective failure to prevent the attacks on September 11, the strengths and weaknesses of the reforms that were initiated as a result, and the problems that remain. In particular, we will focus on the effectiveness of organisms, pre and post September 11, which employ a multi-agency approach to counter-terrorism efforts.

According to 9/11 Commission Chairman Thomas Kean, 9/11 "was a failure of policy, management, capability and, above all, a failure of imagination." The four components in this quadrant of failure will form the framework for the analysis in this chapter.

---

[27] Abraham Lincoln, *Annual Message to Congress -- Concluding Remarks*, Washington, D.C. December 1, 1862. http://showcase.netins.net/web/creative/lincoln/speeches/quotes.htm (accessed December 4, 2006).

A. THE IMPETUS FOR REFORM

As with many problems, unfortunately often a major calamity is needed as a catalyst before reform takes place. Regrettably, it turns out the longstanding problems in our domestic counterterrorism community were not immune from this need. In particular, the intelligence discipline and information-sharing processes had significant, long-standing, and apparently obvious, shortcomings.

At a high-level meeting on September 11, 1998, the federal intelligence community (IC) prophetically concluded that the "failure to improve operations management, resource allocation, and other key issues within the [IC], including making substantial and sweeping changes in the way the nation collects, analyzes, and produces intelligence, will likely result in a catastrophic systemic intelligence failure."[28]

When this prophecy was tragically fulfilled exactly three years later, the post-9/11 scrutiny produced unanimity that our previous domestic counterterrorism efforts were indeed grossly deficient, and the maxim, "9/11 was an intelligence failure," was created. In particular, the 9/11 Commission and others have recognized that there was a general intelligence failure of information sharing and cooperation among all levels of the government, and a specific intelligence failure to "connect the dots" in order to prevent the attacks.[29]

Reinforcing what the 9/11 Commission Report found, a US Senate Intelligence Committee reported that**:**

> Serious problems in information sharing…persisted, prior to September 11, between the Intelligence Community and relevant non-Intelligence Community agencies. This included other federal agencies as well as state and local authorities. This lack of communication and collaboration

[28] *Counterterrorism Intelligence Capabilities and Performance Prior to 9-11*: A Report to the Speaker of the House of Representatives and the Minority Leader from the Subcommittee on Terrorism and Homeland Security House Permanent Select Committee on Intelligence July 17, 2002. Note also the inclusion of "operations" as an essential component with intelligence. Available at http://www.house.gov/harman/terrorism/071702_Report.html (accessed March 7, 2007).

[29] National Commission on Terrorist Attacks, *9 /11 Commission Report* (New York: W.W. Norton & Company, First Edition, 2004).

deprived those other entities, as well as the Intelligence Community, of access to potentially valuable information in the 'war' against Bin Ladin.[30]

Because of these acknowledged intelligence debacles, immediately after the 9/11 attacks there was a consensus that we needed to revamp the American domestic intelligence structure to combat the threat of terrorism on our soil. On the organizational side, billions of dollars have been spent reorganizing existing structures and countless new information sharing groups and mechanisms have been established. These dollars, coupled with public and political pressure have brought a myriad of new counterterrorism architecture such as multi-agency fusion centers, regional intelligence centers, a doubling of the number of Joint Terrorism Task Forces (JTTF's), and so on.

On the legislative front, Congress has passed the Intelligence Reform and Terrorism Prevention Act (IRTPA),[31] and the executive branch has issued its own multiple executive orders and strategies. We will discuss the IRTPA at length in the next section, but there are three interrelated executive documents that bear introducing now as they set out a foundation for the reform efforts-- the National Security Strategy, the National Intelligence Strategy of the United States and the National Criminal Intelligence Sharing Plan.

The National Security Strategy lays out the President's vision of how to protect America and end tyranny elsewhere in the world. It has five main themes that center around defeating terrorism by a strong America that promotes freedom and democracy throughout the world. Most relevant to our focus is the strategic objective and mandate to "Transform America's National Security Institutions to Meet the Challenges and Opportunities of the 21st Century."[32] To bring life to this charge, the National Intelligence Strategy (NIS) attempts to tailor US national intelligence to 21st century threats by identifying ten principle objectives:

---

[30] United States. Senate. Select Committee on Intelligence and House Permanent Select Committee on Intelligence. *Joint Inquiry into the Terrorist Attacks of September 11, 2001, Final Report - Part 1* (Washington, DC: GPO, December 10, 2002).

[31] *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),* PL108-408 (December 17, 2004).

[32] United States. President. *The National Security Strategy of the United States of America* (Washington, DC: White House, 2006). Available at http://www.whitehouse.gov/nsc/nss.html (accessed on February 12, 2007).

- Build an integrated intelligence capability to address threats to the homeland.
- Strengthen analytic expertise, methods and practices.
- Rebalance, integrate and optimize collection capabilities.
- Attract, engage and unify an innovative and results-focused work force.
- Ensure that decision-makers can access the intelligence they need when they need it.
- Establish new and strengthen existing foreign intelligence relationships.
- Create clear, uniform security practices and rules.
- Exploit path breaking scientific and research advances.
- Learn from our successes and mistakes.
- Eliminate redundancy[33]

The National Criminal Intelligence Sharing Plan (NCISP), developed by the Global Intelligence Working Group (GIWG) and endorsed by the U.S. Department of Justice (DOJ), particularly addresses domestic intelligence reform needs. The NCISP's overarching goal is to link together all levels of law enforcement, including officers on the street, intelligence analysts, unit commanders, and police executives via a nationwide communications capability for sharing critical data.

The Plan makes twenty-eight recommendations that outline model policies, standards, and guidelines for developing a local law enforcement intelligence function. It makes recommendations regarding key implementation issues and barriers; and identifies methods for developing and sharing critical data. The recommendations attempt to promote:

- A model intelligence-sharing plan.
- A mechanism to promote intelligence-led policing.
- A blueprint for law enforcement administrators to follow when enhancing or building an intelligence system.
- A model for intelligence process principles and policies.
- A plan that respects and protects individuals' privacy and civil rights.

[33] United States. Office of the Director of National Intelligence. *National Intelligence Strategy of the United States of America: Transformation Through Integration and Innovation* (Washington, DC: Office of the Director of National Intelligence, 2005). Available at http://www.globalsecurity.org/intell/library/news/2005/intell-051026-dni01.htm (accessed on October 21, 2006).

- Technology architecture to provide secure, seamless sharing of information among systems.
- A national model for intelligence training.
- An outreach plan to promote timely and credible intelligence sharing.
- A plan that leverages existing systems and networks, yet allows flexibility for technology and process enhancements.[34]

Most of these reform efforts are aimed at improving our intelligence capacity; however, as discussed in Chapter III, 9/11 reviews have made it clear that the intelligence failures did not occur in a vacuum. A joint inquiry of Congress summarized the intelligence failures in the larger context of counterterrorism in an extensive review of our nation's intelligence system:

> The findings further suggested systemic weaknesses of intelligence and law enforcement communities: an absence of emphasis on the counterterrorist mission, a decline in funding, limited use of information technology, poor inter-agency coordination, insufficient analytic focus and quality, and inadequate human intelligence. Above all, there was a lack of a government-wide strategy for acquiring and analyzing intelligence and for acting on it to eliminate or reduce terrorist threat.[35]

Our discussion begins at the identified problem of a disconnected and dysfunctional intelligence "community" extant prior to the attacks on September 11.

B. A COMMUNITY IN NAME ONLY

Ambassador John Negroponte laid out the organizational reform challenge during his confirmation hearings to become our nation's first Director of National Intelligence (DNI). In order to overcome problems such as the failure of the FBI and CIA to share information about the 9/11 terrorists before the attack, Ambassador Negroponte explained that America needed to create "a single intelligence community that cooperates seamlessly, that moves quickly, and that spends more time thinking about the future than the past."[36] This unity was needed to overcome problems identified in the 9/11 review,

---

[34] United States. Department of Justice. *National Criminal Intelligence Sharing Plan* (Washington, DC: Department of Justice, October 2003), iv. Available at http://www.iir.com/global/products/NCISP_Plan.pdf (accessed January 19, 2007).

[35] Best, 16.

[36] John Negroponte, US Senate Confirmation Hearings Testimony, April 12, 2005. Available at http://usinfo.state.gov/usinfo/Archive/2005/Apr/12-450912.html (accessed on December 12, 2006).

including the failure to share warnings between FBI field offices and other agencies and the CIA's failure to pass the names of suspected terrorists to other agencies, such as the Federal Aviation Administration and Customs agencies.[37]

Perhaps understandably, since traditionally the intelligence community had been considered largely the province of only federal agencies, and since it was the federal government conducting the reviews of 9/11, the initial integration and reform efforts focused primarily on the federal intelligence community.

1. Coordinating the Federal Intelligence Community

The WMD Commission pointed out that since the federal intelligence community lacked centralized direction and coordination, it was a "community" in name only. "The 15 intelligence agencies rarely act with a unity of purpose," the Commission said in its overview of the report.[38] In response, Congress and the executive branch have adopted three major reforms: creation of the position of Director of National Intelligence (DNI), who ostensibly oversees the sixteen-member federal intelligence community[39] and is responsible for resolving the internecine squabbles between the FBI, CIA and DHS, creation of a center to co-locate key components of each of these agencies, and the demand to create an environment in which vital information will be shared effectively.

2. Intelligence Reform and Terrorism Prevention Act Reform Efforts

Under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Congress codified into law the three reforms that are important to our analysis: the position of intelligence "czar" the DNI, to oversee the intelligence community, the establishment of the National Counterterrorism Center (NCTC) to coordinate counterterrorism intelligence and operations, and the formation of an Information Sharing

---

[37] 9/11 Commission Report, 258.

[38] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction *Report to the President of the United States* (Washington, DC: The Commission, March 31, 2005), 5.

[39] At the time of the 9/11 Commission Report, the Office of National Security Intelligence had not been created within the DEA, thus it became the 16th.

Environment (ISE) to facilitate sharing of information.[40] The NCTC and ISE are discussed more fully later in Section C of this chapter in connection with fusion centers; this section focuses on the DNI.

Under IRTPA, management of the federal IC is by the Office of the Director of National Intelligence (ODNI). The IRTPA grants the DNI the authority to integrate the IC's functioning according to the management principle of "centralized oversight, decentralized execution."[41] Even though the ODNI leads the federal intelligence community, and ODNI components produce finished intelligence, the ODNI does not run day-to-day operations in the federal intelligence agencies. The entire core functions that each member of the federal IC traditionally performed, including, collection of information, analysis, operations, technology development, dissemination of intelligence, and internal management are all still performed by the various intelligence agencies.

According to many reviewers, the DNI position has thus far fallen short of its mandate to ensure effective intelligence collection and sharing. A recent Senate Intelligence Committee report concluded, "The Committee is extremely frustrated that four years after the terrorist attacks of September 11, 2001, and after Intelligence Community promises to improve information sharing, the Community appears to have made little progress in this regard."[42] Additionally, at a recent intelligence sharing conference for the federal IC, sponsored by the Director of National Intelligence, a variety of intelligence experts acknowledged major barriers to effective information sharing remain. One speaker compared the 16-agency U.S. intelligence community to 8-year-old soccer players bunching around the ball leaving the remainder of the field uncovered.[43]

---

[40] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) at § 1011.

[41] Ibid.

42 United States. Senate. *Intelligence Authorization Act for Fiscal Year 2006.* S. Rpt. 109-142. (Washington, DC: GPO, September 29, 2005).

[43] Finley.

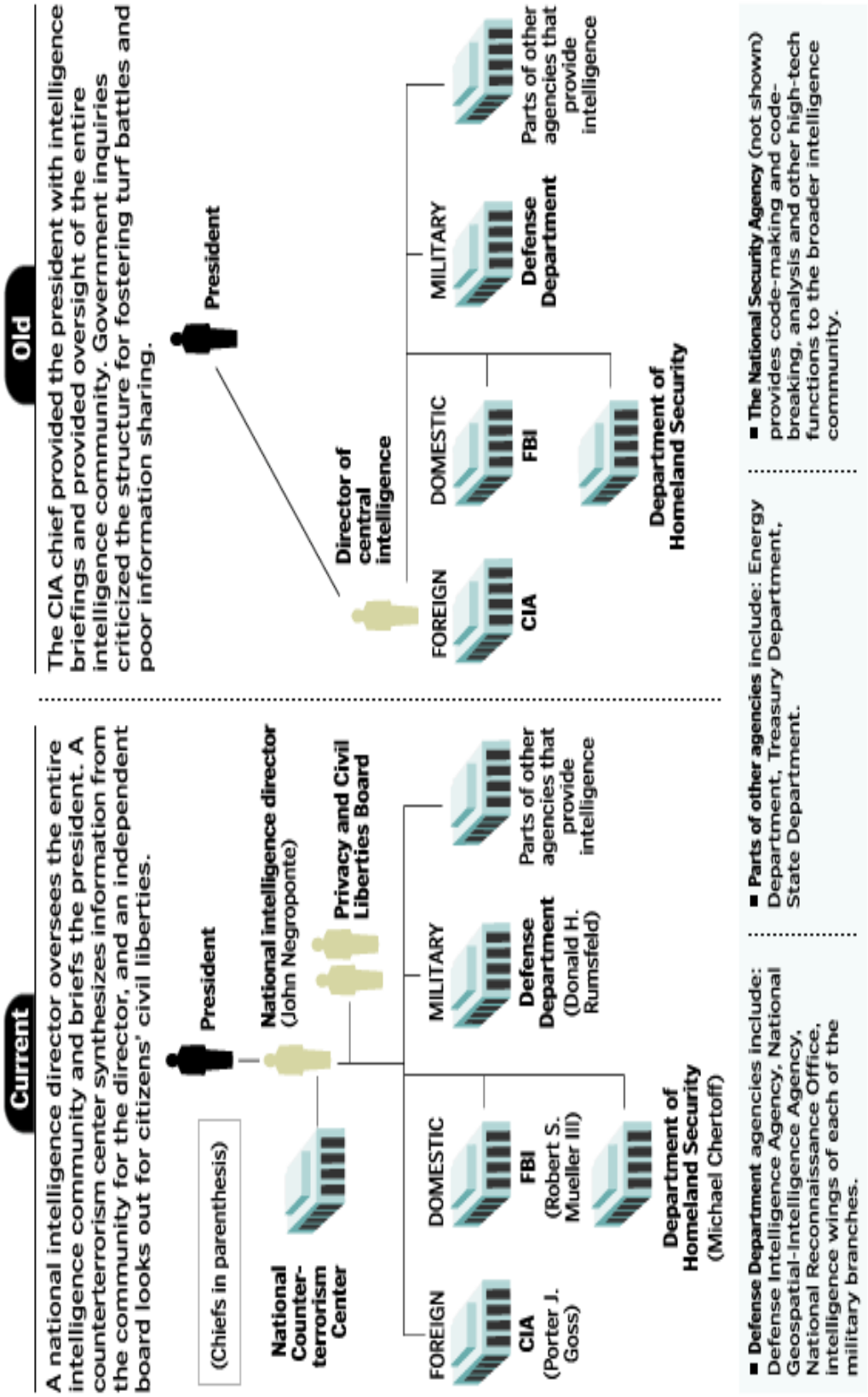


Figure 2. Pre and Post-9/11 Federal Intelligence Community Structure

3. National Counterterrorism Center

In a further attempt to resolve ongoing information sharing problems, President Bush established the National Counterterrorism Center (NCTC) by executive order in September 2004. Congress, in the IRTPA, later codified it in December 2004.[44] The Presidential and Congressional intent is that the NCTC will serve as the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism.

The IRTPA places the NCTC under the Office of the DNI with a mandate to:

- Serve as the federal government's multi-agency center analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, including threats to U.S. interests at home and abroad.
- Conduct strategic operational planning for counterterrorism activities
- Assign operational responsibilities to lead agencies for counterterrorism activities
- Function as a shared knowledge bank for the counterterrorism community, making information available to the intelligence, law enforcement, Homeland Security, diplomatic, and military communities across the United States Government.[45]

The NCTC operates as a partnership of federal organizations including the CIA, FBI, and Departments of State, Defense, and Homeland Security. Representatives from the IC meet, many via videoconference, and update the nation's threat matrix three times a day at the NCTC. We will discuss more about the NCTC in the next chapter in the discussion of collaboration challenges.

C. REFORMING THE DOMESTIC COUNTERTERRORISM COMMUNITY

As a starting point of analysis, there is concurrence in the literature that the very nature of the American political system is at the core of the problem of developing effective counter-terrorism architecture. The American system consists of a vast number of political units, including an immense federal bureaucracy of competing agencies with overlapping and redundant counter-terrorism responsibilities, along with over twenty

[44] IRTPA, Section 1012, PL 108-458, Executive Order 13354, "National Counterterrorism Center," 69 *Federal Register* 53589, September 1, 2004.

[45] Ibid.

thousand cities, counties and states, and a multitude of other political sub-divisions. Just in the law enforcement arena, there are nearly 800,000 officers spread among some 18,000 police departments and some 3000 sheriff offices.[46] This morass confounds information sharing on a basic level, let alone achieving integration of efforts.[47] The Police Executive Research Foundation (PERF) has concurred that one result of this complex system of government is ineffective communication and confusion over roles and responsibilities for counter-terrorism.[48]

1. Defining Mission Spaces

Homeland Security involves six critical mission areas as defined by the federal government:[49]

- Intelligence and warning,
- Emergency preparedness and response,
- Domestic counterterrorism,
- Critical infrastructure and key asset protection,
- Defense against catastrophic threats, and
- Securing the borders and transportation system

The federal role in these critical mission areas is fairly clear; much of it is defined by presidential decree or Congress. For example, Congress and the executive branch have designated the primary mission of the Department of Homeland Security (DHS) as securing the homeland and protecting it against conventional and unconventional attacks in the United States. President Bush, via presidential directive, has also designated the Attorney General of the United States as the lead federal agency responsible for criminal investigations of terrorist acts or terrorist threats by individuals or groups within the

---

[46] Brian A. Reaves and Matthew J. Hickman, *Census of State and Local Law Enforcement Agencies, 2000* (Washington, DC: Department of Justice, October 2002, NCJ 194066), 1. http://www.ojp.usdoj.gov/bjs/pub/pdf/csllea00.pdf (accessed December 14, 2006).

[47] According to the US Census Bureau, there are approximately 23,000 cities and counties.

[48] Martha Blockin and Gerald Murphy, *Protecting Your Communities From Terrorism, Strategies for Local Law Enforcement Series*. (Washington DC: PERF, 2003).

[49] *National Strategy for Homeland Security*, viii–x.

United States, as well as related domestic intelligence collection efforts.[50] The Attorney General generally acts through the Federal Bureau of Investigation (FBI), but many other federal agencies, in particular the Department of Homeland Security (DHS), have central roles in the counter-terrorism arena.

2. Remaking the Federal Bureau of Investigation

As chronicled previously, as the lead for domestic counterterrorism, the Federal Bureau of Investigation has shouldered the greatest share of the criticism regarding the failure to prevent the 9/11 attacks. Those criticisms have centered on the discovery that the FBI failed to integrate and analyze information within its own field offices and among its own agents, as well as integrate information that was available in other agencies, such as state and local law enforcement, departments of motor vehicles, etc.

However, the FBI argues its efforts were constrained by shortages of key personnel, in addition to technological and legal limitations. For example, before September 11, executive branch interpretations of laws intended to protect privacy also served to inhibit information sharing within the FBI. The building of a "wall" between intelligence gatherers and criminal investigators to protect privacy also served to prohibit information sharing between these two critical counterterrorism components. After 9/11, Congress amended these laws to remove any barriers between intelligence agents and criminal investigators. In testifying in support of the PATRIOT Act legislation that removed this metaphorical wall, CIA Director Porter Goss said, "The wall was a barrier against full and discerning dialogue and greatly impinged on the effective use of critical tools necessary to fight terrorism."[51]

Nonetheless, despite the proposition that there is a synergy between this two vital counterterrorism components, some observers remain convinced that the very nature of intelligence and investigations make these critical functions ill suited to be housed within the same agency. The argument is that it is unreasonable to expect that a law enforcement

---

[50] George W. Bush *Management of Domestic Incidents*, Homeland Security Presidential Directive (HSPD): 5 (Washington DC: The White House, February 2003), 2. Available at http://knxup2.hsdl.org/homesec/docs/dhs/HSPD5.pdf (accessed March 7, 2007).

[51] Porter J. Goss, testimony before the Select Committee on Intelligence United States Senate, April 27, 2005.

agency, such as the FBI, can effectively conduct domestic security intelligence since it also has to remain focused on law enforcement and criminal investigations. Consequently, some have argued for the United States to create a new domestic intelligence agency without law enforcement responsibilities, modeled on the British MI-5. Federal Judge Pozner, for example, has argued that an intelligence focus is inconsistent with an investigative focus because of the differing mindsets. He advocates creation of a domestic intelligence agency, a model that Great Britain and most of the major world democracies have chosen.[52]

Pozner and other advocates of separate law enforcement and domestic intelligence agencies argue the intelligence and law enforcement cultures are very different and placing intelligence within a primarily investigative agency invariably leads to a de-emphasis of intelligence. They believe a nation benefits by having an administrative and personnel structure focused solely on intelligence, especially counterterrorism. Judge Pozner recently elaborated on this "investigative case" versus "intelligence gathering" problem:

> A law-enforcement approach to terrorism can cause intelligence data to be evaluated from the too-narrow perspective of its utility in building a criminal case; retard the sharing of information lest full credit for a successful prosecution be denied the field office that began the investigation; and discourage the collection and retention of information. This last point is related to the difference between collecting information for the sake of knowledge and collecting it for the sake of building a case. Criminal investigators want to collect enough information to prove their case but not enough to give defense counsel information that may be usable to exculpate the defendant. Intelligence officers don't have that inhibition.[53]

Additionally, Senator Shelby from the Senate Intelligence Committee has similarly observed an intrinsic problem in housing intelligence within a law enforcement agency. In commenting on the negative impact on housing intelligence within the FBI, he observed:

---

[52] Richard A Pozner, *Remaking Domestic Intelligence* (Stanford, CA: Hoover Institution Press, 2005).

[53] Ibid., 58-59.

> . . . Its agents are trained and acculturated, rewarded and promoted within an institutional culture the primary purpose of which is the prosecution of criminals. ... Information is stored, retrieved, and simply understood principally through the conceptual prism of a "case"—a discrete bundle of information the fundamental purpose of which is to prove elements of crimes against specific potential defendants in a court of law.
>
> The FBI's reification of "the case" pervades the entire organization, and is reflected at every level and in every area: in the autonomous, decentralized authority and traditions of the Field Offices; in the priorities and preference given in individual career paths, in resource allocation, and within the Bureau's status hierarchy to criminal investigative work and post hoc investigations as opposed to long-term analysis; in the lack of understanding of and concern with modern information management technologies and processes; and in deeply-entrenched individual mindsets that prize the production of evidence-supported narratives of defendant wrongdoing over the drawing of probabilistic inferences based upon incomplete and fragmentary information in order to support decision making…
>
> Far from embracing probabilistic inference, "knowledge" in a law enforcement context aspires—in its ideal form at least—not only to certainty but also to admissibility, the two essential conceptual elements of being able to prove someone guilty beyond a reasonable doubt in a court of law. Within such a paradigm, information exists to be segregated and ultimately employed under carefully managed circumstances for the single specific purpose for which it was gathered.[54]

Major democracies, such as France, Germany, Canada, and Australia generally follow Great Britain's MI5 model, separating police powers of investigation and arrest from intelligence collectors. A primary reason these democracies have separated intelligence from criminal investigations is for the stated purpose of protecting of civil liberties.[55] These democracies subscribe to the belief that removing the coercive power of arrest and prosecution from the intelligence collectors lessens the opportunity to curtail essential liberties such as the expression of free speech. However, in perhaps an ironic twist, many civil libertarians in America have *opposed* the creation of a separate domestic

---

[54] *Final Report of the Congressional Joint Inquiry Into September 11* "September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence," December 20, 2002, 52–53, http://www.fas.org/irp/congress/2002_rpt/shelby.pdf (accessed November 14, 2006).

[55] In regards to the French model, this is true to a lesser extent, as the domestic intelligence agency is a directorate under the national police agency.

intelligence agency for the same reason. Gregory Najeimi of the ACLU argues, "Creating a domestic agency would be bad for civil liberties and bad for security, we haven't had a domestic CIA since the country was founded. We went through all the years of the Cold War without a domestic CIA, we don't need one now."[56]

Current FBI Director Robert Mueller has argued against removing domestic intelligence from the Bureau for reasons of effectiveness, stating that splitting the law enforcement and intelligence functions into separate agencies "would leave both agencies fighting the war on terrorism with one hand tied behind their backs."[57]

In considering this issue, the 9/11 Commission ultimately agreed with Director Mueller and specifically recommended against creation of a new domestic intelligence agency at this time, urging instead that the FBI be given an opportunity to reform. The Commission outlined its concerns:

- If a new domestic intelligence agency were outside of the Department of Justice, the process of legal oversight—never easy—could become even more difficult. Abuses of civil liberties could create a backlash that would impair the collection of needed intelligence
- Creating a new domestic intelligence agency would divert attention of the officials most responsible for current counterterrorism efforts while the threat remains high. Putting a new player into the mix of federal agencies with counterterrorism responsibilities would exacerbate existing information-sharing problems.
- A new domestic intelligence agency would need to acquire assets and personnel. The FBI already has employees, facilities and relationships with state and local law enforcement, the CIA, and foreign intelligence and law enforcement agencies.
- Counterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action. Because the FBI can have agents working criminal matters and agents working intelligence investigations concerning the same international terrorism target, the full range of investigative tools against a suspected terrorist can be considered within one agency. [58]

---

[56] Gregory Najeimi, quoted in "MI5-Style Intel Agency Could Be Hard Sell in U.S." *FOX News Website* (April 21, 2004), http://www.foxnews.com/story/0,2933,117677,00.html (accessed January 5, 2007)

[57] Robert Mueller, Ibid.

[58] *9/11 Commission Report*, 423-425.

Congress and the Executive Branch have to date agreed with the 9/11 Commission's recommendation to focus on reforming the Bureau, adding 7000 employees and doubling the FBI's budget to six billion dollars since 2001. Director Mueller has thus set out to remake the Bureau into a more effective counterterrorism agency, addressing both law enforcement *and* intelligence.

On the investigative side, because of the increased resources and renewed focus, counterterrorism investigations now account for half of the investigations conducted by the FBI.[59] However, the most significant changes have been in the area of intelligence reform. In response to new resources and the mandate to focus more on intelligence, the FBI has undertaken significant organizational reform with the stated goal to create an Intelligence Program on par with its investigative programs. According to the FBI, "now that the Intelligence Program is established and developing, we are turning to the next stage of transforming the Bureau into an intelligence agency."[60]

Director Mueller describes these reforms as including new enhanced analytical capabilities, state-of-the-art information technology, and an integrated intelligence structure at headquarters and in the field. The FBI has also created new Field Intelligence Groups (FIG's), discussed in Chapter VI, in each of its field offices, and has added many more Joint Terrorism Task Forces (JTTF's), also discussed in Chapter VI.

Despite these changes, some concern remained as to whether the FBI had sufficiently transformed from largely an investigative agency, to also become an intelligence agency. Because of this concern, the President directed the FBI to go further in its reforms and create a National Security Branch within the Bureau. The new National Security Branch (NSB) consolidates three previously separate programs—counterterrorism, counterintelligence and intelligence. Even more significantly, the DNI was given budget authority over the FBI's national intelligence activities, i.e., the NSB, and the DNI was given specified authority to concur in the appointment of the executive assistant director (EAD) of the NSB.

---

[59] Karen DeYoung, "A Fight Against Terrorism—and Disorganization" *Washington Post* (August 9, 2006).

[60] United States. Federal Bureau of Investigation. *Report to the Commission on Terrorist Attacks Upon the United States: The FBI's Counterterrorism Program* (Washington, DC: FBI, April 14, 2004), 31. http://www.fbi.gov/publications/commission/9-11commissionrep.pdf (accessed November 20, 2006).

To some this is seen as a possible portent of a future new domestic intelligence agency argued for by Pozner and others, should efforts to reform the Bureau be judged inadequate. By consolidating counterterrorism and intelligence in one branch, with funding controlled outside of the Bureau, some view this as a possible transition stage in preparation for moving these responsibilities outside of the FBI.

Figure 3. FBI National Security Branch- FBI[61]

[61] The NSB was established by authority of a June 28, 2005, White House memorandum "Strengthening the Ability of the Department of Justice to Meet Challenges of the Security of the Nation" directing the Attorney General to implement the WMD Commission's recommendation for the FBI to establish a "National Security Service." see *FBI Foreign Terrorist Tracking Task Force (FTTTF).* Available at http://www.usdoj.gov/jmd/2008justification/exhibit300/fbi_ftttf.pdf (accessed March 7, 2007).

3. Where's A Cop When You Need One? The Role of State, Local and Tribal Authorities in Counterterrorism

In contrast to the federal government, the role of state, local and tribal (SLT) government in Homeland Security and counterterrorism is not well defined.[62] This applies to how the federal government views the state, local and tribal role, and how SLT governments view their own role.

The federal government has traditionally had a narrow view of the role of SLT governments, especially the local role, in the six critical mission areas of Homeland Security. The prevailing view was that local government was essentially limited to a "first responder," role, responsible for responding to and mitigating the impacts of an attack, but having only a supporting role regarding "intelligence and warning" and "domestic counterterrorism." This is reflected in the above-mentioned presidential directives, which recognize the first responder role but omit mention of local participation in the others.

Lest this be interpreted as the federal government running roughshod over the wishes of the states, and particularly "the locals," it needs to be made clear that local governments have generally taken a similarly narrow view regarding their appropriate role in Homeland Security. Though there are some exceptions, the research reveals that, with the exception of New York City, most cities have not developed any significant counterterrorism capacity.[63] Although not universally true, in general, most cities have focused on the first responder role, i.e., mitigation and response, and they have deferred to the federal government in the intelligence, investigations and operations domains, playing primarily a supporting role when the FBI requests assistance on a particular investigation or identified intelligence need.

---

[62] The term "state, local, and tribal," or more commonly "state and local," is commonly used to connote the combined body of non-federal government players in Homeland Security. Despite this common usage, there is recognition that in many respects, "State" government has a distinctly different role in dealing with terrorism than does "local" government. It is, however, beyond the scope of this document to analyze the distinctions between the non-federal entities.

[63] Michael O'Hanlon, "The Role of State and Local Governments in Homeland Security: Written Testimony for the Senate Committee on Homeland Security and Governmental Affairs" (Washington, DC: Brookings Institution, July 14, 2005. http://www.brookings.edu/views/testimony/ohanlon/20050714.pdf (accessed December 2, 2006).

The previous chapter described the diminished role of non-federal law enforcement in national security intelligence starting in the 1970's because of real and perceived civil rights abuses. When the nation awoke to the need for Homeland Security after the 9/11 attacks, only sixteen percent of state and local agencies reported having a specialized unit or individual assigned responsibility for addressing terrorism, and only about ten percent of police agencies had an intelligence unit, largely found only in the larger departments.[64]

The advantages of deferring the responsibility for counterterrorism to the federal government, primarily the FBI, are substantial. Immediately before 9/11, much of the country was entering into a period of severe financial and budgetary limitations, which culminated in a loss of law enforcement and other first responder positions. By avoiding a principal role in counterterrorism, SLT governments have avoided the tremendous personnel costs associated with this mission.

Further, this diminished role for local government has lessened their liability exposure considerably. Counterterrorism activities carry with them considerable political risk. By definition, counterterrorism will necessarily involve political and religious considerations. Accusations of racial and religious profiling, and "Patriot Act blowback" are the norm. Many cities and states have laws regulating intelligence collection involving religious and political groups, and a long tradition of emphasizing the promotion of First Amendment rights. Because the federal government has taken the lead on counterterrorism, local governments have been freed to concentrate on the largely non-controversial areas of emergency response and preparedness. They have been spared the negative publicity and criticism that agencies, such as the United States Attorney's Office, the FBI, DHS and Immigrations and Customs Enforcement (ICE) have had to endure.

There is also the very real problem that high-profile crime problems other than terrorism exist. Local government officials are pressured to use scarce resources to take action on visible crime, seldom on the hypothetical terrorism threat. For example, in response to a wave of shootings and murders, Philadelphia Police Commissioner

[64] K. Jack Riley, Gregory F. Treverton, Jeremy M. Wilson, Lois M. Davis, *State and Local Intelligence in the War on Terrorism (*Santa Monica, CA: RAND, 2005), 12.

Sylvester Johnson moved in late 2004 to take back some of the limited personnel he had assigned to a terrorism unit. When questioned by the media about moving these officers back to fight urban crime, Commissioner Johnson emphasized the violent crime problem and stated, "We haven't seen the Taliban in Philadelphia."[65]

Incorporation of the tribes into the counterterrorism community has also been problematic. Although uttering "tribal" when mentioning "state" and "local" has become a sort of shibboleth for Homeland Security professionals, the actual integration of tribal law enforcement into the anti-terrorism community has been limited. Traditionally, there has been a lack of integration and jurisdictional clarity between Native American communities and local, state and federal officials regarding law enforcement, which will have to be overcome.[66] The importance of tribal participation is underscored by the international border and port security issues that concern Tribal lands, as well as the critical infrastructure located on Tribal lands, such as dams and reservoirs, electrical generation plants and energy pipelines, drinking water wastewater systems, and railroads and bridges.

---

[65] "Budget Crunch Forces Pinch in Cops' Anti-Terror Unit, Some Members Being Reassigned" *Philadelphia Daily News* (December 29, 2004).

[66] Native American Law Enforcement Association, *Tribal Lands Homeland Security Report*" (NNALEA's 10th Annual Training Conference, October 22-24, 2002), 6. http://www.nnalea.org/hlsecurity/summitreport.pdf (accessed December 14, 2006).

THIS PAGE INTENTIONALLY LEFT BLANK

V. EVOLUTIONARY ROADBLOCKS - THE STRUGGLE TO COLLABORATE

Collaboration has been seen as an integral part of the solution in response to many of the main counterterrorism issues and problems detailed in the previous chapters, especially in overcoming information sharing difficulties. Accordingly, much of the counterterrorism reform effort over the past five years has been devoted to developing collaborative models. Illustrative is Homeland Security Presidential Directive 8, which sets out "expanded regional collaboration" as one of the overarching national priorities in the National Preparedness Goals, and "strengthening information sharing and collaboration capabilities" as one of the main capability based priorities.[67]

This fecund period has produced a bounty of offspring, and as in nature, there tends to be an overproduction of offspring, resulting in a competition for survival. This thesis juncture is thus where we attempt to identify the favorable variations that should be passed on to subsequent counterterrorism progeny, and the unfavorable traits that may lead to die-out and ideally would be "selected out." As in nature, "natural selection" is not the only process at work; we also have to consider the influence of non-adaptive factors, such as politics, on counter-terrorism evolution.

A. COLLABORATION

Since "collaboration" will be a common thread sewn throughout the remainder of the chapters, and terms like "effective collaboration" and "truly collaborative" are employed in this thesis, this is a useful point to briefly explore the underlying principles of what is being advocated when there is a call for "collaboration."

"Collaboration" is different from "coordination" and "cooperation," even though all three are important. "Coordination" is the least intensive relationship; coordination is about efficiency, about developing a framework to ensure that otherwise disparate forces act more harmoniously, e.g., local and federal law enforcement agreeing to avoid duplicative or conflicting efforts. "Cooperation" is more in depth than coordination. It

[67] George W. Bush, *National Preparedness,* Homeland Security Presidential Directive (HSPD): 8 (Washington, DC: The White House, December 17, 2003), 1. Available at https://www.hsdl.org/homesec/docs/dhs/HSPD8.pdf (accessed March 7, 2007).

involves individual agencies maintaining their separate mandates and responsibilities, but working together to accomplish common goals. For example, multiple agencies co-locating resources in an intelligence center, but with each agency still primarily responsible for directing its own personnel to meet their respective agency missions, constitutes "cooperation."

"Collaboration" is more intense and more ambitious. In collaborating, people and organizations are willing to fundamentally change their previous way of doing business and share responsibilities and resources. From an organizational point of view, researchers from the Wilder Research Center define collaboration as:

> Collaboration is a mutually beneficial and well-defined relationship entered into by two or more organizations to achieve common goals. The relationship includes a commitment to: a definition of mutual relationships and goals, a jointly developed structure and shared responsibility, mutual authority and accountability for success, and sharing of resources and rewards.[68]

Consequently, a "collaborative" counterterrorism center would have certain characteristics, such as the participants jointly designing, and especially jointly governing, according to a shared vision and mission and shared resources. The participants would also share responsibility for failures and success. As such, in a politically dominated and bureaucratically inclined system, collaborations are inherently much more difficult to achieve than cooperative approaches.

Importantly, a collaborative approach is also about creating something new, not merely moving existing structures and systems to a new location. A collaborative approach seeks to create synergy from a holistic view. Michael Schrage describes this evolutionary modus operandi in his book on innovation and collaboration, *Shared Minds*:

[68] Paul W. Mattessich, Marta Murray-Close, and Barbara R. Monsey, *Collaboration: What Makes it Work,* 2nd Ed. (St. Paul, MN: Fieldstone Alliance, 2001), 34.

> Collaboration is the process of shared creation: two or more individuals with complementary skills interacting to create a shared understanding that none had previously possessed or could have come to on their own. Collaboration creates a shared meaning about a process, a product, or an event. … Something is there that wasn't there before.[69]

Accordingly, the benefit from a collaborative approach, and what makes the struggle worthwhile, is that our prevention and response capabilities can be increased because the whole will be greater than its parts. More importantly, beyond just greater efficiencies in using Homeland Security resources, and improved information sharing, collaborations create the possibility of new solutions. The possibility of new solutions is especially important in the face of an adaptive enemy.

B. FEDERAL CENTRIC ISSUES

Most observers agree that are nations' counterterrorism efforts have not followed a collaborative approach; rather they have been primarily *federally coordinated* efforts, with a recent trend toward more cooperative, and hopefully collaborative, approaches. The previous chapter detailed the reasons our counterterrorism system has developed predominantly federal characteristics, many of which are logical and expected, but there are problems with this development. To begin with, a federal dominated, federal centric program is just that—a program that focuses on federal priorities. The National Governor's Association recently surveyed each of the state Homeland Security directors. The Homeland Security directors were virtually unanimous in voicing concern over the lack of state input into federal policy development, and in recommending that the federal government coordinate with states prior to adopting and implementing Homeland Security policies.[70]

The International Association of Chiefs of Police (IACP) has also surveyed its members and come to the conclusion that a serious and fundamental flaw exists in our national strategy in that it was developed "without sufficiently seeking or incorporating the advice, expertise or consent of public safety officials" at the state, local and tribal

[69] Michael Schrage, *Shared Minds: The New Technologies of Collaboration* (New York: Random House, 1990), 140.

[70] *2006 State Homeland Security Director's Survey: New Challenges, Changing Relationships* (Washington, DC: National Governors Association, Center for Best Practices, April 3, 2006). Available at http://www.nga.org/Files/pdf/0604HLSDIRSURVEY.pdf (accessed November 1, 2006).

level. In arguing for putting more of a state, local and tribal presence in the gene pool, the IACP report stresses the importance of local, not federal design.[71] Stephen Flynn, a former member of the National Security Council and a senior fellow at the Council on Foreign Relations has extensively studied counterterrorism reform efforts, and he concurs that a central reason that serious problems remain is that "it's a top-down, purely federal enterprise."[72]

To illustrate the problems of perspective, recent bombings in London and Madrid had enormous implications for local officials' response and prevention efforts regarding public transportation systems. Nonetheless, when contacted immediately after the attacks, federal authorities simply did not have the information local authorities needed. As Charles Ramsey, former chief of the Washington Metropolitan Police stated, "the FBI is worrying about who might have done it, but what I care about is that there was an attack on a transit system and I have rush hour coming up . . . I need to know what I can do proactively to strengthen the security of our transit system."[73] In the absence of timely information from the federal government, many local jurisdictions instead relied on the NYPD who had their own people on the scene looking for locally relevant information within hours of the attacks. The NYPD liaison was on the scene in minutes, and his report to NYPD in New York enabled them to take preventative measures in time for the morning rush hour, including doubling the number of officers assigned to the subways. NYPD Commissioner Kelly explained the presence and perspective of local officers abroad "gives the NYPD the advantage of immediate, firsthand intelligence about the methods terrorists employed in attacking mass transit, hotels and synagogues in foreign cities."[74]

---

[71] International Association of Chiefs of Police, *From Hometown Security to Homeland Security. IACP's Principles for a Locally Designed and Nationally Coordinated Homeland Security Strategy.* (Alexandria, VA: International Association of Chiefs of Police, May 2005). Available at www.theiacp.org/leg_policy/HomelandSecurityWP.PDF (accessed March 7, 2007).

[72] Stephen E. Flynn, speech titled *America the Vulnerable: How Our Government Is Failing To Protect Us From Terrorism*, sponsored by Council on Foreign Relations, July 20, 2004, transcript available at http://www.cfr.org/publication/7214/america_the_vulnerable.html?breadcrumb=default (accessed March 7, 2007).

[73] Charles H. Ramsey, interview by John Broder, "Police Chiefs Moving to Share Terror Data" *New York Times* (July 29, 2005), A15.

[74] Raymond Kelly, "A Report from the Front" *New York Daily News* (September 10, 2006).

There further appears to be widespread dissatisfaction with the timeliness and quality of information sharing. The National Governor's Association survey of state Homeland Security directors revealed that a majority of the directors are "somewhat or completely dissatisfied with the specificity and actionable quality of the intelligence their states receive from the federal government."[75]

On the local government level, according to Chief of Police William Lansdowne, the San Diego Police Department relies on cable television news to stay abreast of threats because in his experience the dissemination system runs about eighteen hours behind the actual event.[76] William Bratton, former New York City Police Chief, and current head of the Los Angeles Police Department, has voiced similar concerns about untimely information, saying that it often arrived so late that it was of little value.[77] Chief Bratton stated that he often got his information from cable news networks, hours before bulletins came from federal agencies, and he blamed it on a system of JTTF's and analytical agencies that are focused on investigations and not geared to provide real-time intelligence to local officials who need to respond operationally to threats.[78] Interviews of the chiefs of the Chicago, Las Vegas and Washington D.C. Metropolitan departments revealed the same concerns expressed by Chief Bratton.[79]

C. INTEGRATION OF STATE, LOCAL AND TRIBAL RESOURCES INTO THE COUNTERTERRORISM COMMUNITY

If the benefits described in the previous chapter of non-federal law enforcement staying out of the fray are many, so are the costs. To begin with, federal law enforcement simply does not have adequate resources to fulfill the counter-terrorism task. Relying on a federal-centric prevention program is counter-intuitive when you consider that the FBI has only a little over 12,000 agents, but there are some 800,000 local law enforcement

---

[75] *2006 State Homeland Security Director's Survey.*

[76] Robert Schmidt, "Terrorism Fighters May Focus on Fed as Model for Sharing Data" *Bloomberg.com*, http://www.bloomberg.com/apps/news?pid=20601087&sid=a9p3U5a.EBLA&refer=home (accessed December 14, 2006).

[77] Interview of William J. Bratton by John M. Broder, "Police Chiefs Moving To Share Terror Data" *New York Times* (July 29, 2005), A15.

[78] Ibid.

[79] Ibid.

officers--personnel who understand and have extensive interaction with the communities they police. These officers are often in a better position to be terrorism related intelligence collectors, in a vastly more extensive manner than the federal government.

Type of agency	Number of agencies	Number of full-time sworn officers
Total		796,518
All State and local	17,784	708,022
Local police	12,666	440,920
Sheriff	3,070	164,711
Primary State	49	56,348
Special jurisdiction	1,376	43,413
Texas constable	623	2,630
Federal		88,496

Table 3. Law Enforcement Agencies and Officers[80]

In addition to excluding the largest portion of our nation's law enforcement resources from the national security effort, a federal-centric role also omitted the non-federal perspective from the design of the Homeland Security apparatus. Because of this, there has been widespread concern that state and local needs have not been met.

To address the concern regarding the role of local authorities in the counterterrorism effort, the International Association of Chiefs of Police (IACP) has launched the Taking Command Initiative (TCI). The IACP has pinpointed five key principles about local involvement that it feels are essential to consider in the development of an effective national strategy to safeguard the Homeland.[81]

1. All Terrorism Is Local

Even though terrorist acts may have national implications, they are all inherently local crimes that local and regional officials will have the primary responsibility to handle, at least initially. More significantly, because terrorists typically live and operate in local communities, as demonstrated by the September 11 terrorists, local authorities are considerably more likely to encounter them. To cite an example, the vast majority of

[80] Bureau of Justice Statistics, *Law Enforcement Statistics, 2000*. Available at http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed on October 24, 2006).

[81] Ibid.

contacts with persons on the terrorism "watch list" are made by local law enforcement officers (and undoubtedly many other members of the counter-terrorism community such as firefighters, public health officers and private security).[82] Local authorities are also much more likely to notice suspicious behavior, especially subtle changes, than federal authorities are. The recent London Metro terrorist bombings and the failed British airplane plot reinforced the IACP's position, as these terrorist acts demonstrate the threat of local, or "home grown" terrorists is increasing.

Thus, properly trained and equipped local officials are often best positioned to interdict terrorists before an attack occurs, and an effective national security strategy "must be developed in an environment that fully acknowledges and accepts the reality that local authorities, not federal, have the primary responsibility for preventing, responding to and recovering from terrorist attacks."[83]

2. Prevention Is Paramount

Because there is a distorted view of the appropriate role of local authorities, federal support of response and recovery efforts by local authorities have superseded support of prevention efforts. No one disputes the importance of the first responder role, but fundamentally, the focus, as with all crime, should be on prevention.

3. Hometown Security Is Homeland Security

Since local authorities have a unique position in combating crime and the greatest opportunity to deal with suspects in their communities, a properly funded group of local authorities promotes national security. Additionally, this is one of the cornerstones to the "all-crimes" approach to Homeland Security. The idea behind "all-crimes" is that the actual acts of terrorism are thus far rare and difficult to detect. However, terrorists, such as the 9/11 terrorists, frequently need to rely on other crimes to facilitate their plots. Consequently, investigating and interdicting crimes such as identity theft, license violations, human smuggling, weapons trafficking, and crimes that fund terrorists, e.g.,

---

[82] The Federal Bureau of Investigation's (FBI) Violent Gang and Terrorist Organization File (VGTOF) helps manage information on organized criminal activities, including domestic terrorism.

[83] IACP Report.

fraud and theft, is a logical strategy to disrupt and prevent attacks. Many, if not most of these crimes are handled by local authorities, emphasizing why local participation in the design and implementation of Homeland Security is crucial.

4. Homeland Security Strategies Must Be Coordinated Nationally, Not Federally

The ability for local authorities to impact policy has been limited because they have been treated as "advisors" to the federal government. The Taking Command solution is to adopt a national, rather than a federal approach to Homeland Security planning and strategy development.[84] Traditional "federal" efforts have not ensured that all levels of government were treated as "full and equal" partners. A collaborative approach will not only allow for better information sharing (essential to all aspects of the counterterrorism triad of intelligence, investigations and operations), but it is essential to ensure that the counterterrorism programs that are created actually meet SLT needs, as well as federal. A collaborative approach also increases the likelihood of buy in by all members of the counterterrorism community, an important consideration in enlisting the participation of as much of the nearly 800,000 local law enforcement community as possible.

5. The Importance of Bottom Up Engineering, the Diversity of the State, Tribal and Local Public Safety Community and Non-Competitive Collaboration

The IACP members feel the one-size-fits-all approach to Homeland Security planning is neither appropriate, nor will it be successful, because of the diversity of needs of each jurisdiction. The IACP also is concerned about the competitive atmosphere that has been created in the quest for funding, and the impact that this has on collaborative efforts among all levels of government.

[84] Though it is beyond the scope of this thesis to delve into the etymology of the transposition of the terms "national" and "federal," in a nod to Constitutional scholars and linguists, I will point out that to avoid confusion I am using them in colloquial terms, not their more historically correct and opposite meanings. Admittedly, what we refer to as the "federal" government today is the opposite of its usage in earlier times when it referred to the collective government of the states. Likewise, "national" historically referred to the corporate central government structure or what we now call the "federal" government.

D. DISSEMINATION ISSUES

One of the significant collaboration challenges is addressing the dissemination of sensitive information. The government fears that sensitive information might be leaked to the wrong people, endangering national security. Fear of improper disclosure of information is understandable and pervades all information sharing collaborations, at least initially, when "outsiders" are let in. This concern increases when collaborations are extended to Homeland Security disciplines other than law enforcement, especially the private sector, because these other disciplines are viewed as not as having experience dealing with sensitive investigative or national security information, and they have generally not undergone the same level of background screening. On the other hand, the private sector also has concerns about sharing sensitive information with the government, fearing that confidential business information may be leaked to competitors or disclosed to the public.

Withholding information for security reasons has its roots in the Constitution. Article I, Section 5, specifies that each house of Congress "shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy."[85] Ever since, the nation has struggled over the proper balance between the public's right to know and the need to protect national security and other legitimate interests. Moreover, in the "new normalcy" of a domestic terrorism threat, we have struggled over how to share information with Homeland Security stakeholders without compromising national security and public safety.

The intelligence communities protect information according to two fundamental principles briefly mentioned in Chapter III: "need to know" and "right to know." "Right to know" refers to whether or not a recipient of criminal intelligence information is legally permitted to receive the intelligence. For example, does the recipient have the necessary security clearance? "Need to know" is established if the intelligence information is relevant to the duties the recipient is empowered to perform. As an illustration, in the case of criminal intelligence, the question is will the intelligence assist

[85] *Constitution of the United States of America*, Article I, Section 5.

a recipient in anticipating, investigating, monitoring, or preventing possible criminal activity or is it relevant to protecting a person or property from a threat of imminent serious harm.

When intelligence needs to be protected from unauthorized disclosure in the interest of national security, a specific degree of protection called "classifying" is utilized. Special classifications restrict dissemination to those who have passed a specific background investigation. Violation of these restrictions is a felony under federal law. The classifiers base the desired degree of secrecy upon their determination of the damage to national security that improper release of the information would cause. The resulting dissemination designation is referred to as a "security classification," such as "for official use only," "secret," "top secret," etc, and is discussed more fully below.[86]

Persons called "original classifiers" do the actual classifying. Original classifiers are designated by executive order and there are approximately 4000 original classifiers, with 800 of these being able to classify a document as "top-secret." Once a document is "originally classified," any document that draws upon that original document will carry the same security classification. This process of "derivative classification" leads to an exponential increase in the number of classified documents.

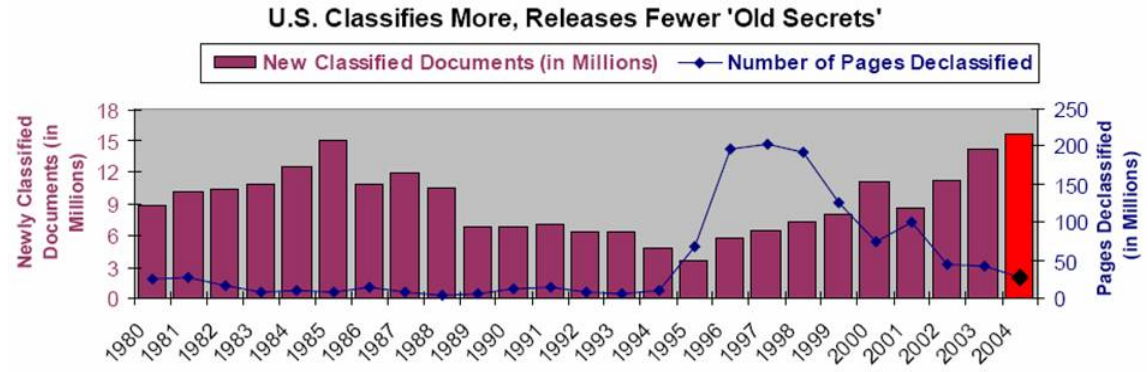


Figure 4. Classification/Declassification Historical View[87]

[86] The United States Government classification system was established under Executive Order 13292.

[87] Rick Blum, *Secrecy Report Card 2005, Quantitative Indicators of Secrecy in the Federal Government: A Report by OpenTheGovernment.Org* (Washington DC: Americans for Less Secrecy, More Democracy, 2005), 3. Available at http://www.openthegovernment.org/otg/SRC2005.pdf (accessed March 7, 2007). This includes both original and derivative classifications.

Classifying information has been the subject of much concern, both from those supporting the public's right to know, and from those who feel important intelligence is not being shared. This has led some to feel there is a sort of "anti-epistemology" bias in the intelligence field. There is a concern that in a "need and right to know" culture, intelligence is frequently needlessly classified; thus unnecessarily restricting sharing to a limited group who possess the necessary clearance.

In particular, the law enforcement community has traditionally not been issued security clearances and consequently has complained loudly about the need to both issue more clearances, more quickly, and to produce intelligence with a "need to share" emphasis, i.e., not at a classified level whenever possible.[88] Senior officials at the Department of Homeland Security concede, "The process of declassifying information takes too long and frequently prevents the department from quickly sharing concrete, actionable information with law enforcement."[89]

The WMD Commission has voiced a novel and provocative view of the information sharing and dissemination problem:

> The term information "sharing" suggests that the federal government entity that collects the information "owns" it and can decide whether or not to "share" it with others. This concept is deeply embedded in the Intelligence Community's culture. We reject it. Information collected by the Intelligence Community—or for that matter, any government agency—belongs to the U.S. government. Officials are fiduciaries who hold the information in trust for the nation. They do not have authority to withhold or distribute it except as such authority is delegated by the President or provided by law.[90]

The WMD Commission offers as a solution that we should move toward a culture of "stewardship" of intelligence information instead of ownership. They suggest that the DNI or the DNI's designee should control access to such information.

---

[88] *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information* (Washington, DC: Department of Justice, Office of Inspector General, Report No. 04-10, December 2003). http://www.usdoj.gov/oig/reports/FBI/a0410/final.pdf (accessed December 12, 2006).

[89] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 474.

[90] Ibid., 430.

> As a baseline standard or norm, the DNI should require the submission of all intelligence information, with proper classification controls, to the Information Sharing Environment.[91] Those who seek to exclude particular information from the environment must carry the burden of proving that such exclusion is clearly in the nation's interest.[92]

The WMD Commission's solution may appear Pollyannaish when viewed in light of a "real world" application. The idea of the submitting *all* sensitive information to the trusted Information Sharing Environment as the arbiter of what should be restricted does not recognize the impracticality of having just one institution handle this workload. For example, in 2004 alone, the government classified approximately 15.6 million original and derivative documents.[93] The WMD panel would no doubt argue that this is exactly the point, and there will be fewer classified documents under their proposal. However, the sheer volume of sensitive information to be processed for *possible* classification suggests the recommendation may be unfeasible.

Another significant information-sharing challenge caused by security classifications is the lack of uniformity in classification labels and standards. To begin with, state and local law enforcement use different categories from the federal intelligence community. State and local authorities generally use the following to protect information:

- SENSITIVE
  - Information pertaining to significant law enforcement cases currently under investigation.
  - Corruption (police or other government officials), or other sensitive information.
  - Informant identification information.
  - Criminal intelligence reports that require strict dissemination and release criteria.

[91] Discussed under "reforms" in the next chapter.

[92] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 444.

[93] Blum, 1.

- CONFIDENTIAL
  - Criminal intelligence reports not designated as sensitive.
  - Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.
- RESTRICTED
  - Reports that at an earlier date were classified sensitive or confidential and the need for high-level security no longer exists.
  - Non-confidential information prepared for/by law enforcement agencies.
- UNCLASSIFIED
  - Civic-related information to which, in its original form, the public had direct access (i.e., public record data).
  - News media information – newspaper, magazine, and periodical clippings dealing with specified criminal categories.[94]

On the other hand, the federal government uses the following categories:

- TOP SECRET information is information, which, if disclosed without authorization, could reasonably be expected to cause exceptionally grave damage to the national security.
- SECRET information is information, which, if disclosed without authorization, could reasonably be expected to cause serious damage to the national security.
- CONFIDENTIAL information is information, which, if disclosed without authorization, could reasonably be expected to cause damage to the national security.[95]

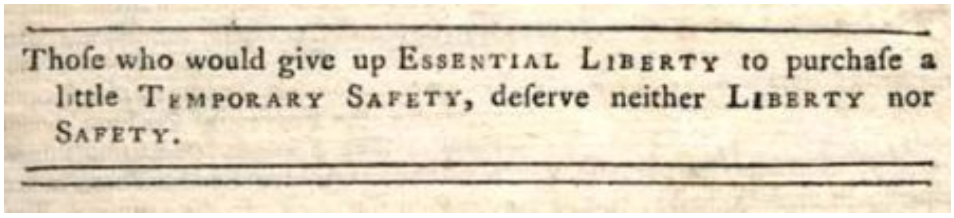
In addition to this tripartite system of classification markings, there is a fourth category "Sensitive, but Unclassified" for information that is deemed sensitive enough to require protection from public release, but falling short of the security classifications allowed under the executive orders. A recent Government Accounting Office (GAO) report found the inconsistent use of this fourth category was contributing to information sharing problems. The GAO report found information-sharing barriers remain from a lack of government wide policies or procedures that describe the basis for when such

[94] David M. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (Washington, DC: Department of Justice, Office of Community Oriented Policing Services, November 2004), 217. Available at http://www.cops.usdoj.gov/mime/open.pdf?Item=1439 (accessed February 2, 2007).

[95] George W. Bush, "Classified National Security Information," Executive Order 12958, April 17, 1995.

designations should be used, coupled with the fact that government agencies are using 56 different designations for "sensitive but unclassified" classification, such as "law enforcement sensitive," "confidential" and "for official use only," to name just a few.[96]

E. CIVIL LIBERTY AND PRIVACY CONCERNS


Thoſe who would give up ESSENTIAL LIBERTY to purchaſe a little TEMPORARY SAFETY, deſerve neither LIBERTY nor SAFETY.

Benjamin Franklin[97]

Ben Franklin's warning to fellow colonists has been bandied about so much in the national counterterrorism dialogue the past few years that it risks becoming a platitude.[98] However, the fossil record of the national security and counterterrorism efforts in America tells an important story about the negative impacts these desirable "species" have, at times, had on civil liberties and privacy.

The anti-terrorism struggle has reignited the national debate about civil liberties and privacy, but the quote attributed to Franklin may incorrectly frame the debate as an "either/or" contest that appeals to extremists in both camps but is unhelpful in understanding the larger context. In reality, when examined thoughtfully, the debate is not really between liberty *or* safety as Franklin's quote implies; instead, the national deliberation is over the proper *balance* between security and liberty. Indeed, as Anthony D. Romero, Executive Director of the American Civil Liberties Union recently agreed: "The task for all of us here has got to be to find a way to secure both goals, not to set up a

[96] United States. Government Accountability Office, GAO Report to Congressional Requestors, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information* GAO-06-385 (Washington, DC: GAO, March 2006). Available at http://www.gao.gov/new.items/d06385.pdf (accessed February 28, 2007).

[97] While not intending to detract from the resurrection of this great American, another bromide attributed to him, "honesty is the best policy," compels me to point out that many researchers now believe that Franklin's fellow diplomat, Richard Jackson, to be the author.

[98] A Google search of the term "terrorism" with the phrase "those who would give up essential liberty to obtain a little temporary safety" turned up over 48,000 hits.

Faustian bargain where you're asked to give up one in the name of the other."[99] Also reflecting an awareness of the need to balance these two oft-competing goals was William Stephenson, the famous spymaster and the head of the Secret Service in Britain during World War II. Despite the grave danger posed to Britain that justified a strong spy network, Stephenson cautioned:

> Among the increasingly intricate arsenals across the world, intelligence is an essential weapon, perhaps the most important. But it is, being secret, the most dangerous. Safeguards to prevent its abuse must be devised, revised, and rigidly applied. But, as in all enterprise, the character and wisdom of those to whom it is entrusted will be decisive. In the integrity of that guardianship lies the hope of free people to endure and prevail.[100]

Recognizing the need to balance both competing interests bridges the political divide in contemporary American society. Republican Senator George Allen has warned, "And what makes us a great nation is that this is a country that understands that people have God-given rights and liberties. And we cannot—in our efforts to bring justice—diminish those liberties."[101] On the other side of the aisle, Democratic Representative Marty Meehan concurs, "It is a delicate task to prevent terror while preserving the civil liberties that have long distinguished our nation. We must rededicate ourselves to finding a balance that both protects and empowers the American people."[102]

As our nation searches for the proper "reflective equilibrium," regarding the liberty and security balance, the debate centers on three main areas.[103]

---

[99] Anthony D. Romero, speech at *Conference on Information Technology and Homeland Security* at the University of California at Berkeley, September 23, 2003. Available at http://www.wired.com/news/conflict/0,60541-0.html?tw=wn_story_page_prev2 (accessed December 12, 2006).

100 William Stevenson, *A Man Called Intrepid* (New York: Harcourt Brace Jovanovich, 1976), xvi.

[101] George Allen, "Terrorist Attacks Against the United States" *Congressional Record* (September 12, 2001), S9289.

[102] Marty Meehan, "Expressing Sense of Senate and House of Representatives Regarding Terrorist Attacks Launched Against United States" *Congressional Record* (September 11, 2001), H5582.

[103] While it is not an unbiased view, for a good compendium of the contemporary concerns about the impact of the war on terrorism on privacy and First Amendment expression, see the report by Mark Schlosberg, *The State of Surveillance: Government Monitoring of Political Activity in Northern and Central California* (ACLU of Northern California, 2006). Available at http://www.aclunc.org/issues/government_surveillance/asset_upload_file714_3255.pdf (accessed March 7, 2007).

1. Profiling- where race, religion or ethnic background is used as a basis for some type of government action; for example, when an Arab or Muslim is singled out based solely on their religion or ethnic background for a search or a detention by a law enforcement officer.
2. Privacy concerns- where an individual's private affairs are potentially illegally or unreasonably subject to government scrutiny, such as the monitoring of international telephone calls. And,
3. First Amendment expression- where government actions may have a chilling effect on the expressing of First Amendment rights, including speech, assembly, and press, e.g., government monitoring or infiltration of a protest group might discourage participation in lawful protests.

In response to these concerns, President Bush's executive orders mandating increased information sharing and creating the National Counterterrorism Center contain provisions protecting privacy and other legal rights.[104] Congress also addressed these issues when it passed the Intelligence Reform and Terrorism Prevention Act (IRTPA). Congress included a provision that established a Privacy and Civil Liberties Oversight Board within the Executive Office of the President, charged with reviewing regulations, policies, and laws relating to counterterrorism to ensure that each of these takes into account privacy and civil liberties concerns.[105]

Additionally, the President must report annually to Congress on the status of information sharing efforts. This report has to include the actions taken in the preceding year to implement or enforce privacy and civil liberties protections. Moreover, the Privacy and Civil Liberties Oversight Board must issue guidelines in consultation with the President to protect privacy and civil liberties in the development and use of the Information Sharing Environment, including specifying the "means by which privacy and civil liberties will be protected."[106]

Even more significantly, the IRTPA requires placement of a Civil Liberties Protection Officer in the ODNI, with a direct report to the Director of National Intelligence, and the IRTPA recommends, though does not require, that other intelligence entities do likewise.[107]

---

[104] Executive Orders 13354 and 13356, (August 27, 2004).

[105] IRTPA, Section 1061.

[106] Ibid., The Information Sharing Environment (ISE) is discussed at length in the next chapter.

[107] Ibid., at Section 1062.

These privacy laws are federally focused, but they are important to state, tribal and local authorities to the extent that a collaborative national counterterrorism network of regionalized centers under federal auspices is created. Though most states, and many units of local government have laws designed to protect civil liberties and privacy in the collection of intelligence, other than the Constitution, the primary, and perhaps only, federal regulation of SLT intelligence collection is by 28 CFR Part 23. This law attempts to protect civil liberties and privacy by regulating the collection of intelligence into any federally funded database. It is a lengthy code, but its core operating principles protecting civil liberties and privacy include the following:

- A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.
- A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.
- A project shall not include in any criminal intelligence system information, which has been obtained in violation of any applicable Federal, State, or local law or ordinance.[108]

Finally, the Fusion Center guidelines, discussed in the next chapter, call for each center to develop, publish, and adhere to a privacy and civil liberties policy with "the capacity and commitment to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties."[109] However, similar to the IRTPA *recommendation* that other entities follow the requirements that establishing a privacy board in the executive office, the fusion center guidelines concerning privacy protection are voluntary.

---

[108] 28 CFR § 23.20 (Criminal Intelligence Systems Operating Policies).

[109] US Department of Justice. Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: Department of Justice, 2006), Guideline 8, 41. Available at http://it.ojp.gov/documents/fusion_center_guidelines.pdf (accessed March 7, 2007).

F. MILITARY –CIVIL INTELLIGENCE SHARING

It is not within the scope of this thesis to do an analysis of the complicated Posse Comitatus Act, but it is worth noting that the military has generally been prevented from performing a domestic law enforcement role since Congress passed the Act in 1878. The law does not apply to the Coast Guard or the National Guard when called up by state governors, but Posse Comitatus effectively bars the military from assisting domestic law enforcement agencies in domestic intelligence collection. Since 9/11, there have been calls to modify the Act, but the prohibition remains, and with some limited exceptions, such as dealing with threats to the physical security of Defense Department employees, installations, or operations, the military is prohibited from gathering domestic intelligence. However, foreign intelligence that the enormous military intelligence apparatus gathers can be shared with domestic agencies, generally through the FBI.

After 9/11, the Pentagon established Northcom, or Northern Command, in Colorado Springs to help in defending against attacks on the Homeland. Northcom has become an integral member of the homeland defense community as it provides command and control of Department of Defense homeland defense efforts and coordinates defense support of civil authorities.

VI. EMERGING FROM THE PRIMORDIAL SOUP-THE ROAD TO COLLABORATION

Prior to the terrorist attacks of September 11, only a relatively small number of counter-terrorism organisms, such as the Joint Terrorism Task Forces (JTTF's), were dedicated to a multi-agency or multi-level of government approach. The post September 11 period is dramatically different. In response to unanimity that our previous counter-terrorism efforts were grossly deficient, hundreds of millions of dollars have gone into creating new counter-terrorism organisms, such as Terrorism Early Warning groups, more JTTF's, regional intelligence centers, analytical centers, and now fusion centers.

Most of these new organizations were created to respond to a central theme of post-9/11 "what went wrong?" analysis, i.e., that information sharing and cooperation among all levels of the government and between agencies was a primary cause of the failure to prevent the attacks.[110] As a result, most of these newly created organizations are centered around the theme of inclusiveness, i.e., they include representatives from multiple agencies, from multiple levels of government –state, local, and federal-- housed together for some specific counter-terrorism purpose, usually information sharing, and less often, investigations and operations.

Another characteristic of the early efforts is that they were focused almost exclusively on law enforcement agencies. As we will discuss, with the passage of time, there has been a growing, and among some, perhaps a grudging recognition that it was not only the perspective of SLT law enforcement that was missing from the Homeland Security effort, but non-law enforcement perspectives were similarly omitted.

Finally, these early efforts reflect an initial evolutionary step towards collaboration as almost all involve some co-location of personnel, following the example the military took to overcome barriers to collaboration. Co-location was forced on the military services in the Goldwater-Nichols Defense Reorganization Act in 1986. This Act addressed a seemingly implacable problem among the military services as inter-service rivalries prevented the different branches from working effectively together as a joint

[110] National Commission on Terrorist Attacks, *9 /11 Commission Report* (New York: W.W. Norton & Company, First Edition, 2004).

team when conducting military operations. In response, the Act created unified regional commands under one admiral or general, and the Act requires officers serve a tour assigned to a Joint Staff in order to be eligible for most high-level promotions. One of the principles promoted by the legislation was co-location to foster the building of personal relationships to help overcome barriers and broaden perspectives. While not a panacea, the Act is generally conceded to have significantly improved inter-agency understanding and cooperation.

> Goldwater-Nichol's intent--and its stunning accomplishment--was to drain the military's bureaucratic swamp. Today, the service chiefs direct the training, organizing, and equipping of their men--the management side. When it comes to fighting, they step back and let a unified commander in the field, advised by a newly empowered JCS chair, run the show: a simple idea with critical strategic ramifications.[111]

In a similar vein, developing the capacity for interagency collaboration is critical for efficiently completing the routine tasks that law enforcement and other disciplines must "cooperatively" handle on a daily basis, e.g., power outages, mass casualties, fires, etc., as well as responding and improvising in the face of natural disasters and terrorist attacks.[112] When the Anthrax attacks occurred shortly after 9/11, Dr. Gerberding of the Center for Disease Control (CDC) admitted her staff had not achieved the "layers and levels of collaboration among a vast array of government agencies and professional organizations that would be required to be efficient and successful in the anthrax outbreak."[113] Another official conceded that the CDC lacked the established links with the FBI so that they did not even initially know whom to call.[114] This problem has since been addressed, but it illustrates the problems of a "relationship deficit" when it comes to both preventing and responding to terrorism.

---

[111] Katherine Boo, "How Congress Won the War in the Gulf" *Washington Monthly*, 23, no. 10 (October 21, 1991), 31.

[112] Susan Hocevar, Erik Thomas, and Gail Fann Thomas, *Building Collaborative Capacity for Homeland Security Preparedness* (Naval Postgraduate School, Monterey, CA, 2006). Available at http://bosun.nps.edu/uhtbin/hyperion.exe/NPS-GSBPP-04-008.pdf (accessed March 7, 2007).

[113] Lawrence K. Altman and Gina Kolata, "Anthrax Missteps Offer Guide to Fight Next Bioterror Battle" *New York Times*, January 6, 2002, 14.

[114] Charles Perrow, "The Disaster After 9/11: The Department of Homeland Security and the Intelligence Reorganization" *Homeland Security Affairs* II, no. 1 (April 2006). http://www.hsaj.org/?article=2.1.3 (accessed March 7, 2007).

A. EARLY COLLABORATIVE EFFORTS

1. Joint Terrorism Task Forces

Perhaps the earliest domestic collaborative counterterrorism effort was the creation in 1980 of a Joint Terrorism Task Force in New York City, consisting of eleven NYPD and eleven FBI agents. A Joint Terrorism Task Force (JTTF) is a Federal Bureau of Investigation (FBI) led cadre of FBI agents, assorted federal agencies, and state and local law enforcement cooperation under the supervision of the FBI to share information and work on terrorism related investigations. As described by FBI Director Mueller, the mission of the JTTF's "is to identify and target for prosecution terrorists and terrorist organizations planning or carrying out terrorist acts occurring in or affecting a geographic region and to apprehend individuals committing such acts."[115]

Subsequently developed JTTF's vary in size and structure in relation to the terrorist threat dealt with by each FBI field office, with an average of forty to fifty people assigned full-time, and others assigned only part-time.[116] The JTTF structure recognizes that each level of law enforcement brings different resources and perspectives necessary to do effective terrorism investigations. From an investigative point of view, there have been demonstrated successes of the JTTF model, one example being the successful investigation by the Seattle JTTF and resulting prosecution of James Ujaama for providing material support to al Qaeda.[117]

The JTTF has also traditionally been the primary apparatus for terrorism information sharing between federal, state and local government (though fusion centers are quickly beginning to rival the JTTF structure as described below). JTTF's provided a "quick-fix" after 9/11 since they were an already familiar structure and appeared to address a priority of developing federal and local partnerships to overcome the problem that information was not being shared between these levels of government, and counter-

---

[115] Robert S. Mueller, Testimony on *War Against Terrorism: Working Together to Protect America,* Before the United States Senate Committee on the Judiciary (Washington, DC, March 4, 2003). http://judiciary.senate.gov/print_testimony.cfm?id=612&wit_id=608 (accessed January 24, 2007).

[116] Riley, 15.

[117] See US Department of Justice Press Release, *Earnest James Ujaama Sentenced For Conspiring To Supply Goods And Services To The Taliban* (February 13, 2004) http://www.usdoj.gov/opa/pr/2004/February/04_crm_086.htm (accessed March 7, 2007).

terrorism efforts were not being coordinated. Prior to September 11, there were only thirty-four JTTF's in the nation; now there are one hundred and one, more than four times the pre-September 11 number. The JTTF's house 2,196 Special Agents, 838 state/local law enforcement officers, and 689 professionals from other government agencies including the Department of Homeland Security, the CIA, and many other federal agencies.[118]

2. Terrorism Early Warning Groups

The Los Angeles Terrorism Early Warning Group, known as the LA-TEW, was the first domestic collaboration founded by local officials, and included some federal participation, but focused on state and local information sharing and fusion. The Los Angeles Sheriff's Department (LASD) established the TEW in 1996. LASD Deputy (now lieutenant) John Sullivan had the vision that there was a void in the greater Los Angeles area regarding information and knowledge about terrorism, as well as the capability to respond to a terrorist attack. His solution was to establish an inter-agency, multi-disciplinary group and process to increase awareness of local threats and consequences.

Sullivan brought together police, fire, medical experts and psychologists, emergency management, the military, public health and others that would have the expertise to increase the opportunities for early warning of terrorist attack by using a "predictive intelligence" approach. The same group would provide, if an attack occurred, the technical expertise and intelligence support to incident commanders. The LA TEW model uses four key tools to accomplish its mission: Vulnerability Analysis, Threat Modeling, Indications and Warning, and Situation Awareness.[119]

After 9/11, the LA-TEW served as the model for an on-going federally funded effort to expand this concept to other metropolitan areas in the nation. There are now

---

[118] Federal Bureau of Investigation website, available at http://www.fbi.gov/aboutus/transformation/overview.htm (accessed November 30, 2006).

[119] National TEW Resource Center. *Resource Guide, Book 1: TEW Concepts and Overview* (Los Angeles: National TEW Resource Center, 2005?), 12-20. Available at http://www.ojp.usdoj.gov/odp/docs/ResourceBook1_TEW.pdf (accessed March 7, 2007).

several TEW's in various metropolitan areas, some having full-time members, others only liaisons. The National TEW Resource Center, which is funded in part by the U.S. Department of Homeland Security, coordinates these efforts.

Though not specifically referred to as a "fusion center," the LA-TEW appears to have been the forerunner for what are now widely referred to as fusion centers. To what extent a TEW can be distinguished from a fusion center is debatable. It appears to have the characteristics of a fusion center, described below. It may simply be that the "fusion center" name designation has outpaced the development of the TEW acronym since the term "fusion center" was widely used by the military, and is more widely understood. One difference, however, may be that the LA-TEW model appears to be more focused on providing intelligence and technical expertise support to operational elements to prepare for and respond to attacks than are most fusion centers.

3. Field Intelligence Groups

One of the findings of the 9/11 Commission was that the FBI should build a stronger relationship with state and local agencies, in order to more effectively share information.[120] Thus, in addition to increasing the number of JTTF's, in 2003, FBI Director Mueller ordered the establishment of Field Intelligence Groups (FIG) in all 56 field offices to serve as an intelligence focused arm for the FBI supporting the JTTF's in particular, but also sharing with state, local and tribal partners.

The FIG's augment the primarily investigative responsibility of the JTTF's with an intelligence capacity as part of the Bureau's effort to transform itself into a stronger intelligence agency. As the primary intelligence group within the Bureau, the FIG's manage the intelligence cycle within the field offices, a capacity that that did not exist prior to September 11. The FIG's don't focus exclusively on terrorism; they also produce and disseminate intelligence on counterintelligence and criminal programs, such as gang interdiction. The FBI's Directorate of Intelligence oversees the FIG's, and most FIG's contain intelligence analysts, special agents, linguists and other members of federal law enforcement and intelligence communities.

[120] National Commission on Terror Attacks Upon the United States, 417.

B. THE EMERGENCE OF FUSION CENTERS

While it is recognized that federal efforts, such as increasing the number of JTTF's, and creating FIG's to support the JTTF's, have improved information sharing, the expectations have evidently been too great and many apparently treated them as a panacea for the information-sharing problem when vehicles such as JTTF's were never designed or resourced for this mission. For example, despite being the primary vehicle for information sharing with state, local and tribal officials, one year following the 9/11 attacks, it was telling in that only a third of local law enforcement agencies reported interacting with the FBI's JTTF's, and this was confined mainly to larger agencies.[121] Despite the investigative successes of the JTTF model, both congressional investigations and private researchers have pointed out limitations *in information sharing* under this model. Further, as described previously, these were federally designed efforts. Under such a scenario, it is predictable that information sharing and other unintentional barriers to collaboration would remain.

From a Congressional point of view, Senator Lieberman's report on the state of information sharing in sum noted that despite improvements, first responders still did not systematically receive the information needed to prevent or respond to terrorist attacks, whether it is from the DOJ or DHS, and the information from locals still did not flow smoothly upward.[122] Plotkin and Murphy identify several areas to improve including: lowering expectations of the JTTF's, increasing resources, and improved communications, as many of the federal, state and local law enforcement officials surveyed pointed out that the JTTF needs to remain focused on investigations and still does not have anywhere near enough personnel to handle information sharing responsibilities on a wide scale.[123] The studies and surveys also showed that the JTTF

---

[121] Riley, 15.

[122] United States. Senate. Governmental Affairs Committee Minority Staff, *State and Local Officials: Still Kept in the Dark About Homeland Security* (Washington, DC: GPO, August 13, 2003). Available at http://hsgac.senate.gov/_files/sprt10833min_hs_statelocal.pdf (accessed March 7, 2007).

[123] M.Plotkin et al, *Protecting Your Communities From Terrorism, Strategies for Local Law Enforcement, Volume 1: Local-Federal Partnerships.* (Washington DC: PERF, 2003). Available at http://www.cops.usdoj.gov/mime/open.pdf?Item=1361 (accessed March 1, 2006).

model is hampered by the need for the SLT participants to have high-level security clearances, a process that can easily take a year or more.[124]

A Markle Foundation task force research also revealed that the federal intelligence community does not fully understand the importance and relevance of information held in the non-federal levels of government.[125]

> Meetings with state and local officials and the private sector have led us to believe that the federal government has not yet realized the value of information identified by state and local entities. A system to integrate this information has not been developed. Much more attention must be paid to this gap, because we as a government are ignoring a critical component of national security. This must be done jointly with the Department of Homeland Security because it is partly the reason why that department was created. We know this is one of the toughest challenges facing the federal government, but it must be done.[126]

Consistent with these described problems, the National Governor's Association survey of state Homeland Security directors revealed a majority of the directors are still "somewhat or completely dissatisfied with the specificity and actionable quality of the intelligence their states receive from the federal government." This survey occurred in 2006 and surprisingly showed a sharp increase in dissatisfaction from a previous survey.[127]

In response to the type of concerns voice by the Markle Foundation, the IACP and others, as well as reviews of the performance of the JTTF's showing mixed success of the JTTF model as a cure for information sharing problems, there has been a focused effort to creating a more robust collaborative organism. Obviously, the JTTF model needed to evolve, or some other model needed to emerge to create more fulsome collaborations to tie together a greater number of participants than could participate in a JTTF. The alternative was to risk continued information sharing roadblocks.

---

[124] Riley, 15.

[125] Testimony of William Crowell, former Deputy Director at the NSA and a member of the Markle Task Force on National Security in the Information Age, before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives, November 8, 2005.

[126] Ibid., testimony of William P. Crowell, p. 6.

[127] *2006 State Homeland Security Director's Survey,* 2.

Consequently, alternative counter-terrorism organizations have been proposed and are now being born into the Homeland Security family. Moreover, as the Homeland Security community has identified strengths and weaknesses in our counterterrorism systems, and as we have identified new requirements caused by the changing threat environment of a dynamic adversary, we have changed focus and structure, moving from the JTTF as the primary information-sharing organism.

The next evolutionary step from the JTTF model appears to be the "fusion center." The "fusion center" term is adopted from the military intelligence system where information from different sources was "fused" together. Fusion centers are designed to overcome the problems of the previous "top-down" approach. They are primarily a state, local and tribal adaptation, but most still contain federal participation in both design and implementation and are central locations at which SLT and federal officials work in close proximity to receive, integrate and analyze information and intelligence. "Fusion Center" is now the common term for what may also be called a "regional intelligence center," "joint analytical center," "coordination center," "terrorism early warning" or some other related term.

All of the multi-government level fusion centers developed to date appear to follow a "cooperative" fusion center model, with the JTTF's and FIG's co-located within one center along with state and local authorities, but retaining their distinct identities and supervisory structure. In a fully "collaborative" model, the federal, state, tribal, and local resources, including the JTTF's, FIG's, and other groups would be jointly governed and shared.

Three of the earliest and well-regarded fusion centers are in Georgia, Arizona and Illinois. Officials in those states all report tremendous satisfaction with the early results of their fusion centers.[128] The satisfaction results from a reported marked improvement in both the fusing of information, as well as dissemination to key stakeholders. Information sharing progress and a move toward greater integration of state, local and tribal (SLT) resources with federal efforts continues to be made as the fusion centers evolve. To illustrate, the Maryland Coordination and Analysis Center (MCAC) houses members of

[128] Illinois Homeland Security, Statewide Terrorism Intelligence Center Report. Available at www.illinoishomelandsecurity.org/ittf/terrorismreport19.htm (accessed January 22, 2006).

23 state, local and federal agencies and maintains a 24-hour watch center with a terrorism hotline. In 2004, state police stopped a vehicle after a passenger was seen videotaping critical infrastructure in a suspicious manner. The officers contacted the fusion center, which learned that the driver of the vehicle was an unindicted co-conspirator in a case involving Hamas in Chicago. The MCAC then contacted federal authorities in Chicago who issued a warrant for the driver.[129]

Challenges remain, however, and the National Governor's Association report on fusion centers has identified four key themes in the research as obstacles to effectiveness:[130]

- Legal limits and cultural differences among agencies can impede information sharing.
- The role of the center must be decided early in the planning process. Will it play a purely analytical role, or will it also act on information?
- The location of the center can affect its operations. Centers viewed as adjuncts to federal operations may enjoy only limited participation and cooperation by local officials.
- Start-up, as well as long-term, funding is in limited supply but is essential for the success of state fusion centers.

Despite these challenges, because the fusion center model appears to address many of the counterterrorism problems described in this and previous chapters, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) have officially endorsed the recommendation that each state create a joint "fusion" center that brings together the disparate entities involved in counter-terrorism collection.[131] President Bush noted this vision: "All across our country we'll be able to tie our terrorist information to local information banks so that the front line of defeating terror becomes

---

[129] Mary Beth Sheridan, Spencer C. Hsu, "Localities Operate Intelligence Centers To Pool Terror Data" *Washington Post,* December 31, 2006.

[130] *Establishing State Intelligence Fusion Centers.* (Washington, DC: National Governors Association, Center on Best Practices, October 2005.)

[131] U.S. Department of Justice and U.S. Department of Homeland Security Global Justice Information Sharing Initiative, *Recommended Fusion Center Standards* (Washington, DC: Department of Justice, June 2005), 3. http://it.ojp.gov/documents/Fusion_Center_Executive_Summary.pdf (accessed January 17, 2007).

activated and real, and those are the local law enforcement officials."[132] State officials have clearly concurred as well with seventy percent of state Homeland Security directors listing the development of a state fusion center as their top priority.[133]

There are now approximately 43 fusion centers in forty-one states, and over $380 million dollars in federal grants have been spent in support of them.[134] Federal officials hope to eventually have 70 fusion centers nationwide, providing a coast-to-coast intelligence blanket. Some focus exclusively on terrorism; others track all manner of criminal activity. The fusion centers developed to date have several common characteristics:[135]

- Most centers include staff from multiple agencies at the state, local and federal levels;
- The centers maintain clear and direct communication channels to field officers and policy makers; and
- Centers are designed to be multi-purpose, focusing not only on terrorism prevention but also on fighting crime in general

However, the 43 fusion centers have been developed independent of any coordinated federal guidance, and no national standards existed until recently to guide the design and implementation of the centers. Because the fusion centers have developed independently, there are several variations in their structure:[136]

- Some centers only have analytical roles while others also have the personnel and capabilities to act on intelligence;
- Some centers have a regional outlook; sharing information among states; others have a vertical structure, connecting states to local and federal agencies, but not other states; and
- Some centers are contained within the federally led JTTF's others are independent.

None of this suggests that the JTTF or FIG has become a vestigial organ. In nature, vestigial organs are structures that were useful in ancestral species but have a

[132] George Bush (Speech, FBI, Washington, D.C., February 14, 2003), http://www.whitehouse.gov/news/releases/2003/02/20030214-5.html (Accessed January 17, 2007).

[133] *2006 State Homeland Security Director's Survey,* 6.

[134] Sheridan.

[135] NGA Center for Best Practices Issue Brief, *State Intelligence Fusion Centers: Recent State Actions* (Washington, DC: National Governors Association, Center for Best Practices, July 7, 2007), 1.

[136] Ibid.

greatly reduced or almost eliminated importance in more recently derived species. In the case of fusion centers, the JTTF model still has tremendous importance, as per presidential directive, the FBI remains the lead investigative agency for terrorism, and the JTTF is still the primary mechanism used to carry out the investigative and counterterrorism mission described by Director Mueller. Moreover, the still developing Field Intelligence Groups are a vital intelligence resource to integrate into fusion centers.

Thus, fusion centers are not designed to supplant JTTF's and FIG's; the opposite is true. The fusion centers species are an adaptation that grew out of the recognition that the threat environment required more than the JTTF organism was designed to provide. The ideal fusion center model integrates the successful aspects of the JTTF's and FIG's, i.e., the federal investigative and intelligence resources, with a broader set of DNA, e.g., other disciplines and components, and state and local participation in design and governance. Indeed, in interviews across the country, one of the common threads was that the fusion centers viewed as most successful all integrated an existing JTTF as an essential part of their counterterrorism efforts, and there is an increasing trend to locate FIG's in fusion centers as the primary federal intelligence component.[137]

C. THE INFORMATION SHARING ENVIRONMENT

Consistent with the disparate development of the multitude of independent fusion centers, a recent Markle Foundation Task Force report pointed out that despite the evolution of the fusion center model, the DHS had still not articulated its vision for how federal, state, local and tribal authorities would participate in a network.[138] Responding to this and other criticism that not enough progress has been made at improving information sharing and integrating federal state, local and tribal authorities, and because of the positive reception to the initial fusion center effort, DHS Secretary Michael Chertoff recently outlined a new vision for a more collaborative and effective approach:

---

[137] Interview of Norm Beasley, former ACTIC director and member of DHS Fusion Center Support Team. September 26, 2006 [author interview].

[138] Markle Foundation Task Force, *Creating a Trusted Network for Homeland Security* (New York: Markle Foundation, 2003), 8.

> We are going to build upon some of our early initial efforts to establish fusion centers by creating a national network of intelligence fusion centers to support state and local decision-makers, chiefs of police, and state and local intelligence officials. We're going to build new information systems to further facilitate collaboration and sharing of classified and unclassified information, and to allow real-time working collaboration between state and local and federal law enforcement officials, including the ready transmission of classified information over secure communication facilities.[139]

Secretary Chertoff's vision originates from a mandate in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calling for creation of the Information Sharing Environment (ISE), as well as requiring designation of a Program Manager for the Information Sharing Environment (PM-ISE). The ISE is an approach to facilitate the sharing of terrorist related information. It achieves this by establishing policies, processes, protocols and technology that enable the sharing of this information among federal, state, local, tribal and private sector entities, as well as our foreign partners.[140] The first and current Program Manager is Thomas McNamara, and he is responsible for overseeing the creation of an Implementation Plan.

The newly released Implementation Plan contains some significant milestones on the road to reform. Under the Plan sent to Congress in late 2006, the Plan cites substantial accomplishments in information sharing. These achievements include revisions to existing policies and procedures, development of new policies, establishment of information fusion centers that include all levels of government, and fielding new collaborative capabilities and programs. These programs allow ISE participants to implement systems, architectures, and standards to provide solutions for ISE users that enable them to access, share, and analyze terrorism information. However, the Plan also candidly concedes that "significant hurdles" remain and a greater degree of coordination

---

[139] Remarks by the Secretary of Homeland Security Michael Chertoff at the International Association of Chiefs of Police Annual Conference October 16, 2006.

[140] Program Manager, Information Sharing Environment. *Information Sharing Environment Implementation Plan* (Washington, DC: Office of the Director of National Intelligence, November 2006). Available at http://www.ise.gov/docs/ise-impplan-200611.pdf (accessed December 12, 2006).

and integration than exists today is needed. Specifically, the Plan finds that the current environment "does not consistently provide the optimal level of cross-community terrorism information sharing."[141]

Consequently, a primary goal in the Plan is to provide a robust information-sharing framework that creates an integrated view for federal, state, local and tribal decision-makers and the private sector by giving them access to a broad spectrum of terrorism information to support "collaborative counterterrorism operations." This primary goal translates into three main reforms that are especially relevant to our study:

1. Creation of an Interagency Threat Assessment and Coordination Group to coordinate information for SLT governments and the private sector.
2. Designation of Fusion Centers as the focus point for SLT governments to share and receive information with the federal government. And,
3. Promotion of a nationwide integrated State and Major Urban Area Fusion Center network

1. Interagency Threat Assessment and Coordination Group

The crucial need for some entity, such as the National Counterterrorism Center (NCTC), to serve as a national coordinating body is still apparent nearly six years after 9/11, perhaps even more so with the ever increasing number of fusion centers and other information sharing enterprises producing an ever increasing number of intelligence products. Recalling the earlier discussion about the "white noise" problem, there still is no mechanism to coordinate what funding and other competitive pressures have too often resulted in "bulletin factories" racing to be the fastest and/or most prolific. Illustrative is a recent incident at the Port of Miami in which local and federal officials appropriately handled a suspicious incident, but the initial limited information that came out of the incident rapidly was circulated nationally without proper vetting among various information- sharing groups, including fusion centers. Unfortunately, much of the initial information was wrong, including reporting that one of the subjects detained was on the Terrorism Watch List. This inaccurate and widespread dissemination contributed to needless "spinning up" and another "cry wolf" scenario.[142] In another example of a lack

[141] *Information Sharing Environment Implementation Plan*, 10.

[142] David Ovalle, "False Alarm Tests Miami Port's Security" *Miami Herald*, January 7, 2007, and interviews with multiple fusion center and Homeland Security officials, January 8-9, 2007.

of coordination and needless duplication of effort by scarce resources, in preparation for the 2006 Winter Olympics, eight of the sixteen federal intelligence agencies all produced and circulated arguably redundant finished intelligence products: independent assessments of the possible terrorist threat to the games that concluded the same thing.[143]

However, even though the National Counterterrorism Center is perhaps best situated to provide national coordination of intelligence production, a major criticism of the NCTC is that it has served only federal authorities, and did not meet the needs of state, local or tribal law enforcement officials. Specifically, concern has been raised that the NCTC omits the participation of SLT officers who could use their perspective to identify and vet information that the non-federal community needed.[144]

Responding to this criticism, the just issued ISE implementation plan states that a newly formed Interagency Threat Assessment and Coordination Group (ITACG) will be collocated with the NCTC. The primary purpose of the ITACG "will be to ensure that classified and unclassified intelligence produced by federal organizations within the intelligence, law enforcement, and Homeland Security communities is fused, validated, deconflicted, and approved for dissemination in a concise and, where possible, unclassified format."[145] Note that this does not specifically address how, if at all, state, tribal and locally produced intelligence will be handled.

At the ITACG, federal departments and agencies assigned mission-specific roles will also provide terrorism information to facilitate the production of "federally coordinated" terrorism information products intended for dissemination to SLT officials and private sector partners. It is unclear what role state, tribal and local law enforcement will actually play within the ITACG, as the Plan appears to limit participation to representatives from DHS, FBI, DOD, and other "relevant *Federal* (emphasis added) organizations."[146] Further, the Plan emphasizes that, although it is going to be co-located

---

[143] DeYoung, 5.

[144] *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information* (Washington, DC: US House Committee on Homeland Security Democratic Staff Report, December 28, 2005), 3. Available at http://www.fas.org/irp/congress/2005_rpt/vital.pdf (accessed March 7, 2007).

[145] *Information Sharing Environment Implementation Plan*, 29.

[146] Ibid.

with the NCTC, the ITACG "will not be a part of the NCTC," and it "is not intended to duplicate, impede, or otherwise interfere with the existing and established counterterrorism roles and responsibilities."[147]

Consequently, on several levels, the ITACG does not appear to address fully the concern that the NCTC is lacking in non-federal representation. Indeed, the Plan's language refers to producing "*federally* coordinated" information instead of "*jointly* coordinated," or more ideally, "*collaboratively produced intelligence*." Moreover, the "existing counterterrorism roles and responsibilities" that this Plan seeks to preserve, are exactly what critics have pointed out need to be changed. Currently, this is not a *national* center, it is a *federal* center, as it omits SLT authorities from the one place that by Congressional and Presidential intent is designed to serve as the primary organization for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism. This omission is especially glaring as the absence of SLT authorities is occurring at an organization that has as a mission statement "to inform, empower, and help shape the national and international counterterrorism effort to diminish the ranks, capabilities, and activities of current and future terrorists."[148]

2. Fusion Center Focus

ISE Program Manager McNamara has commented that state and local fusion centers "are a critical component of the ISE because they can dramatically enhance efforts to gather, process, and share locally generated information regarding potential terrorist threats and to integrate that information into the Federal efforts for counterterrorism."[149] This recognition led to the reaching of a major milestone in developing a national information-sharing network. The Plan states "Fusion centers will become the focus- but not exclusive focal points- within SLT governments for receiving and sharing terrorism information."[150] The Plan recognizes that there are fusion centers

---

[147] *Information Sharing Environment Implementation Plan*, 29.

[148] NCTC website, available at http://www.nctc.gov/about_us/about_nctc.html (accessed January 7, 2007).

[149] Thomas McNamara, prepared statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. *Building the Information Sharing Environment: Addressing Challenges of Implementation,* 109th Cong., 2nd sess. 2006.

[150] *Information Sharing Environment Implementation Plan*, 30.

associated with both "states" and "major urban areas," and consistent with their respective roles and responsibilities, federal departments and agencies will provide terrorism information to SLT authorities primarily through these fusion centers. Reinforcing the point highlighted in an earlier section regarding the viability and importance of existing entities, the Plan emphasizes the fusion center collaborations will include the JTTF's.[151]

The Centers will have to operate consistent with the DHS/DOJ Fusion Center Guidelines, discussed below, and obviously with any relevant federal, state, and local regulations. To accomplish this goal, the Plan contemplates that the Centers will all achieve a baseline capacity level. This baseline is not defined in the Implementation Plan; that job appears to fall to the yet to be released National Fusion Center Guidelines. The Plan does not require a state or major urban area to establish a fusion center, and in those states that have multiple fusion centers; one will be designated as the primary statewide center to interface with the federal government. The federal government will then coordinate through this center to organize the gathering, processing, analysis and dissemination of Homeland Security information.[152]

3. Integrated National Fusion Center Network

In another important milestone, the Implementation Plan proclaims that the federal government will promote the establishment of a nationwide and integrated *network* of State and major urban area fusion centers to facilitate effective terrorism information sharing. To facilitate this network, the Plan calls for assigning representatives of federal organizations and co-location of personnel and resources whenever feasible; however, the Plan does not provide further details of the proposed network.[153] Instead, the Departments of Homeland Security and Justice, along with the Program Manager of the ISE "are in the final planning stages of an effort to identify a State or regional Evaluation Environment" as a means of further developing the concept of a national network of fusion centers.

---

[151] *Information Sharing Environment Implementation Plan*, 116.

[152] *Draft Public Affairs Guidance, State and Major Urban Area Fusion Centers*, January 5, 2007.

[153] *Information Sharing Environment Implementation Plan*, 29.

The ISE as currently proposed:

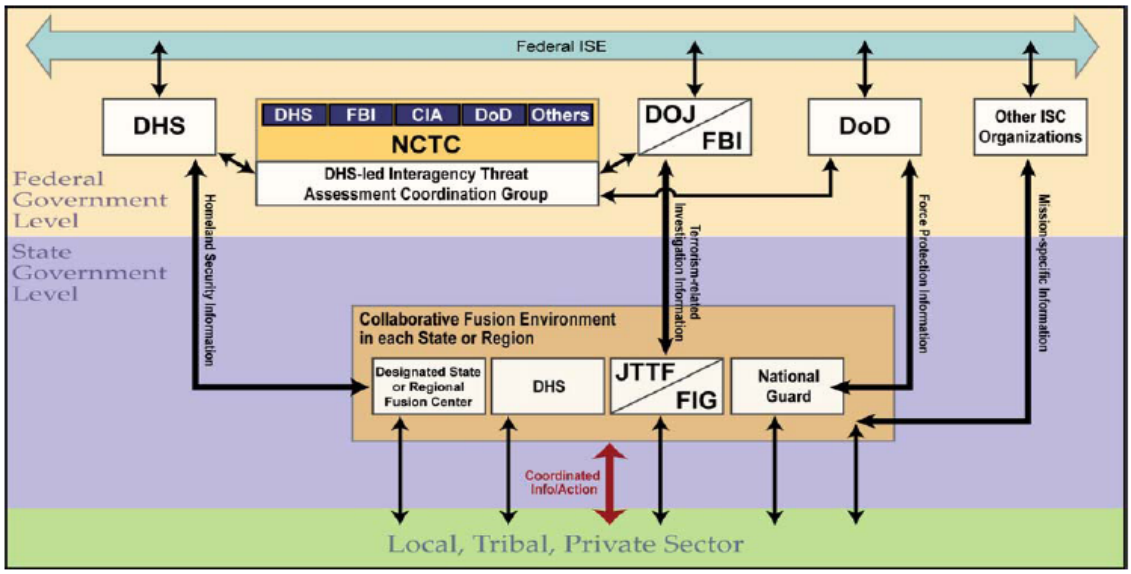


Figure 5. Figure-Information Sharing Environment as Proposed in 2006 Implementation Plan

The challenges faced in establishing an integrated fusion center network include both political and logistical challenges. Politically, DHS has set up a battle by deciding that each state will have one "primary" statewide center with which the federal government will interface, and through which the federal government will coordinate the intelligence cycle as it relates to Homeland Security information in that state. In states that have more than one fusion center, such as California and New York, it remains to be seen how receptive local governments and major urban area fusion centers will be to this concept.

The plan also defers details of how the actual network will be developed, other than reciting that DHS is in the final planning stages of an effort to identify a State or regional Evaluation Environment that would develop the concept. Logistics of connectivity, as well as discussion of how such a network would be coordinated or directed are omitted. Again, the political sensitivities in resolving the state versus federal versus local "control" are significant.

D. PUBLIC-PRIVATE PARTNERSHIPS

While it is axiomatic that the government has a role and vested interest in protecting critical infrastructure, it is widely believed that the private sector owns approximately 85% of the nation's critical infrastructure.[154] In addition to their role in protecting much of our country's critical infrastructure, private sector personnel also represent a vast potential resource and information sharing partnership to assist law enforcement in protecting critical infrastructure and key resources (CI-KR). To provide just one example, it is estimated that there are almost two million private security officers deployed throughout America, many already directly assigned to protect CI-KR.[155]

As a result, President Bush called for an active collaboration and partnership with the private sector in Homeland Security Presidential Directive 7 (HSPD-7), but challenges, including difficulties in overcoming information-sharing barriers, have inhibited full integration. A recent year long study concluded that despite the emphasis placed by Presidential and Congressional mandates, the "capabilities, assets, and goodwill of the private sector to bolster our Homeland Security remain largely untapped."[156] In terms of information sharing, the report cited what others have noted as impediments: private sector companies worry about liability issues and information being leaked to competitors; similarly, government partners had difficulty sharing sensitive information because they feared it might be improperly disseminated.[157]

The National Infrastructure Protection Plan (NIPP) is intended to respond to these and other concerns by providing the overarching framework for a structured partnership between government and the private sector for protection of critical infrastructure and key resources.[158] These policies in the NIPP call for the formation of Sector

---

[154] Despite painstaking research, the original source of this now accepted truism could not be found.

[155] Andrew Morabito and Sheldon Greenberg, *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships.* (Washington, DC: Bureau of Justice Assistance, 2005), vii. http://www.ncjrs.gov/pdffiles1/bja/210678.pdf (accessed December 14, 2006).

[156] Stephen E. Flynn, Daniel B. Prieto, *Neglected Defense, Mobilizing the Private Sector to Support Homeland Security* CSR No. 13 (Washington, DC: Council on Foreign Relations, 2006), 1. Available at http://www.cfr.org/content/publications/attachments/NeglectedDefenseCSR.pdf (accessed March 7, 2007).

[157] Ibid., 15.

[158] George W. Bush, *Critical Infrastructure, Identification, Prioritization, and Protection*, Homeland Security Presidential Directive (HSPD): 7. (Washington, DC: The White House, December 17, 2003).

Coordinating Councils (SCC's) and Government Coordinating Councils (GCC's). The GCC's and SCC's are intended to have a synergistic relationship with the government councils providing interagency coordination of CI/KR strategies and activities by bringing together federal, state, tribal and local authorities to work with the private sector based SCC's. The NIPP also strengthens the use of the Protected Critical Infrastructure Information Program (PCII).

The PCII provides a framework, which enables members of the private sector to voluntarily submit sensitive and confidential information regarding their facilities, i.e., 85 % of the nation's critical infrastructure, to the Department of Homeland Security (DHS) with the assurance that the information, if it satisfies the requirements of the PCII Act, will be protected from public disclosure.[159]

The private sector has shown leadership in setting up information sharing systems independent of the government run programs. Well before 9/11, many critical infrastructure sectors had set up Information Sharing and Analysis Centers (ISAC's) to share important security information regarding threats and vulnerabilities. While a presidential directive encourages the formation of ISAC's and some of them receive government funding to facilitate their development, the respective sectors operate the ISAC's, not the government.

There is an ISAC Council to assist in the formation of ISAC's, and the various ISAC's are at different stages of maturity in the development of their programs. Each ISAC has unique challenges, but the ISAC Council's own description best describes the desired collaboration:

> An ISAC is a trusted, sector specific, entity that provides to its constituency a 24/7 Secure Operating Capability that establishes the sector's specific information/intelligence requirements for incidences, threats and vulnerabilities. Based on its sector focused subject matter analytical expertise, the ISAC then collects, analyzes, and disseminates alerts and incident reports to its membership and helps the government understand impacts for their sector. It provides an electronic, trusted

[159] Flynn, 15.

ability for the membership to exchange and share information on cyber, physical and all threats in order to defend the critical infrastructure. ... whether caused by intentional or natural events.[160]

SECTOR	ISAC
Agriculture and food	Food
Banking and finance	Financial Services
Chemical	Chemical
Commercial facilities	Real Estate
Drinking water and water treatment systems	Water
Emergency services	Emergency Management and Response
Energy	Electric Energy
Government facilities	Multi-State
Information technology	IT Research & Education Network
Telecommunications	National Coordinating Center for Telecommunications
Transportation systems	Public Transit Surface Transportation (rail) Highway Maritime

Table 4. Operating ISAC's, as of July 2006

[160] ISAC Council White Paper, *A Functional Model for Critical Infrastructure Information Sharing and Analysis Maturing and Expanding Efforts* (ISAC Council, 2004), 5. Available at http://www.isaccouncil.org/pub/Information_Sharing_and_Analysis_013104.pdf (accessed January 7, 2007).

VII. EVALUATING EVOLUTIONARY PROGRESS

There is universal agreement that there was a generally dismal state of affairs in the intelligence and domestic counterterrorism communities that led to the successful attacks by al Qaeda on September 11, and the resulting development of a plethora of counterterrorism reforms. What is subject to dispute, however, is the success of those reforms. There is much debate about how much further domestic counterterrorism structures need to adapt and evolve. For example, the pace of the progress on collaborative efforts is open to dispute. Deputy Director of National Intelligence Dr. Thomas Fingar would take issue with viewing collaboration as a needed *evolutionary* change. He recently posited that even though collaboration was central to bringing about the need for radical change in intelligence, the collaboration vision would likely frighten many in the profession because the present state required change that was *more revolutionary* than evolutionary. Dr. Fingar based this on the explosive growth of information, and the complexity of the analysis required by the broad number of stakeholders to deal with the terrorism threat.[161]

Beyond just the pace of reform, there is a dispute about how successful the reforms have been. The previous chapters cite concern from a broad spectrum of observers and participants that there remain many failings in our domestic efforts to combat terrorism. On the other hand, since the enactment of some early reforms, there have been successes such as many domestic terrorism arrests and prosecutions.

Most significantly, there have been no further attacks on American soil. Does this by itself suggest that we have made the necessary changes and solved the failings in imagination, policies, capabilities and management identified by the 9/11 Commission? One conclusion is that the absence of attacks since 9/11 is a testament to the efficacy of our structural adaptations. Another conclusion is that al Qaeda and other terrorist groups simply have not decided to launch another attack.

[161] Thomas Fingar, speaking notes from *Information Sharing Conference*, Denver, CO, August 21, 2006.

While acknowledging that some progress has been made, the latest, and final, Report on the Status of 9/11 Commission Recommendations generally gives a failing grade to our reform efforts. In over half of the major categories, such as information sharing, creating a FBI national security workforce, and civil liberties protection, the report finds minimal or unsatisfactory progress some four years after 9/11.[162] Similarly, the 9/11 Public Discourse Project, composed of former members of the 9/11 Commission, gave the government wide information sharing reform effort a "D," explaining that designating individuals to be in charge of information sharing, e.g., the DNI, is not enough to overcome still remaining information sharing barriers.[163]

What are the appropriate metrics to measure our current effectiveness? The 9/11 Public Discourse Project and most other reviewers who have studied counterterrorism changes and found serious problems remain have primarily relied on qualitative research and study. Their analysis is predominantly anecdotal, based on informed observation, case study reports, and random investigations rather than systematic quantitative evaluation. On the other hand, using quantitative data, the Department of Justice's latest summary of the "war on terrorism"[164] presents a much more sanguine view in its summary of the Department's anti-terror record since 9/11. The DOJ website touts that the United States of America is "winning the war on terrorism with unrelenting focus and unprecedented cooperation." The following are excerpts from the summary relating to domestic counterterrorism.[165]

---

[162] *Report on the Status of the 9/11 Commission Recommendations*, October 20, 2005.

[163] Thomas H. Kean, et al., *Final Report on 9/11 Commission Recommendations* (December 5, 2005), 5.

[164] There are different perspectives in the counterterrorism community on the use of "war" as a metaphor to defeat terrorism in the counterterrorism community. "War" has often been used to rally the nation against large public problems, e.g., the war on poverty, on drugs, etc., conveying that we, as a nation, are under attack. Those concerned with the "war" metaphor cite concerns such as it may unintentionally play into extremists' hands by magnifying their prestige in the Islamic world, support their propaganda that the West desires hegemony, and increases the psychological costs in our own communities. This camp generally favors a "crime-fighting" parallel.

[165] From Department of Justice website, "Preserving Life and Liberty, Anti-Terror Record" available at http://www.lifeandliberty.gov/subs/a_terr.htm (accessed January 13, 2007).

- Our intelligence and law enforcement communities, and our partners, both here and abroad, have identified and disrupted over 150 terrorist threats and cells;
- Five terrorist cells in Buffalo, Detroit, Seattle, Portland (Oregon), and Northern Virginia have been broken up;
- 401 individuals have been criminally charged in the United States in terrorism-related investigations;
- Already, 212 individuals have been convicted or have pleaded guilty in the United States, including shoe-bomber Richard Reid and "American Taliban" John Walker Lindh;
- Over 515 individuals linked to the September 11th investigation have been removed from the United States.
- Hundreds of suspected terrorists have been identified and tracked throughout the United States.
- Our counterterrorism investigations have more than doubled since 9/11.
- Our human sources of intelligence related to domestic terrorism have increased by 30% since 9/11.
- 113 individuals in 25 judicial districts have been charged with terrorist financing-related crimes, with 57 convictions or guilty pleas to date.

The danger in using statistics is of course that they are subject to different interpretations and use. As Mark Twain wrote in his autobiography, "Figures often beguile me, particularly when I have the arranging of them myself; in which case the remark attributed to Disraeli would often apply with justice and force: 'There are three kinds of lies: lies, damned lies and statistics."[166]

DOJ statistics have been analyzed by the Transactional Records Access Clearinghouse (TRAC), a research group at Syracuse University, which has attempted to use an empirical approach for analysis of government programs. TRAC's quantitative analysis and related interpretations of the data have been controversial. In the data from the Department of Justice, 401 individuals have been charged in terrorism related investigations, and 212 have pled guilty or been convicted.[167] TRAC's data analysis, however, showed a surprisingly low amount of jail time for people convicted of what the

[166] Mark Twain, *Mark Twain's Autobiography* (New York: Harper & Bros., 1924).

[167] TRAC, Syracuse University, *Criminal Terrorism Enforcement in the United States During the Five Years Since the 9/11/01 Attacks*, September 4, 2006. Available at http://trac.syr.edu/tracreports/terrorism/169/ (accessed January 13, 2007). Though the website does not indicate the time period, it is apparently updated only through 2003.

Justice Department had identified as "terrorism related crimes." TRAC's analysis showed the median length of sentence dropped from 41 months prior to 9/11, to 28 days in the two years after the attacks, to 20 days in the past three years.

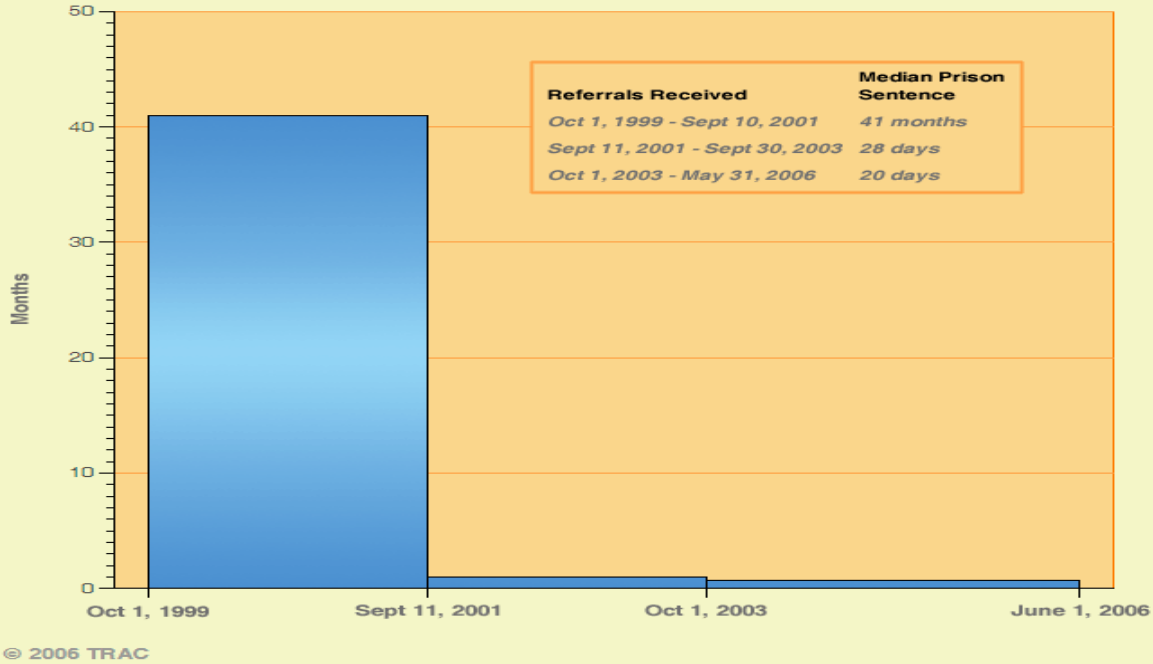


Figure 6. Length of Jail Sentences for Terrorism Related Crimes – TRAC

TRAC's data also showed that the prosecution of international terrorism related cases has returned to pre-9/11 levels.

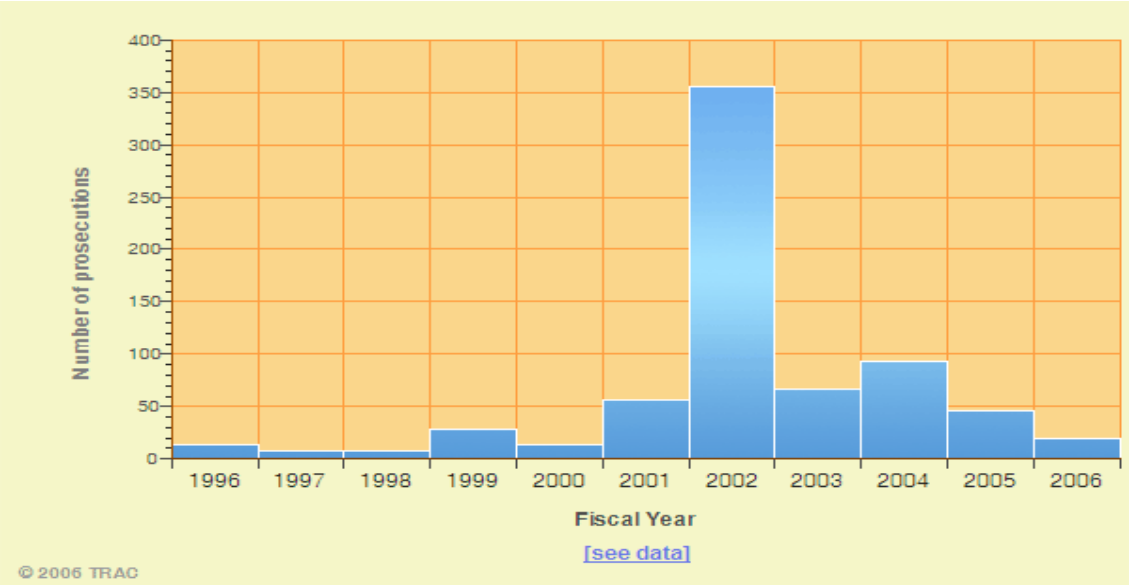


Figure 7. Number of Terrorism Related Prosecution - TRAC[168]

Critics have used the TRAC analysis to question the success of domestic counter-terrorism efforts. For example, Meredith Fuchs, general counsel at the National Security Archive at George Washington University, said the light sentences and drop off in prosecutions might mean that "we are catching people at the margins, not at the center of the plots," and the drop-off in prosecutions can be interpreted that "either a lot of that post-9/11 activity was not necessary or that they haven't identified key people or that key people in custody aren't being prosecuted."[169] The Christian Science Monitor alleges that the Monitor's independent review of the data found many of the cases had only tenuous connections to terrorism. They cite the prosecution of a Kentucky businessperson labeled as a successful prosecution related to "international terrorism" who was convicted of lying about selling forklift parts to an Iranian truck manufacturer but who was sentenced to only 50 hours of community service and one year of probation.[170]

---

[168] TRAC.

[169] Meredith Fuchs in Chicago Sun-Times as reported by Michael J. Sniffen, "Number Of Terror Cases Dwindles: Prosecutions Sink To Level Before" *Chicago Sun-Times*, September 4, 2006. Available at http://www.findarticles.com/p/articles/mi_qn4155/is_20060904/ai_n16708084 (accessed February 28, 2007)

[170] Alexandra Marks, "After a Surge, US Terror Prosecutions Drop to Pre-9/11 Levels" *Christian Science Monitor*, September 5, 2006, 1. Available from http://www.csmonitor.com/2006/0905/p01s04-usju.html (accessed February 28, 2007).

The Justice Department counters strongly that the TRAC report presents a "misleading analysis," and by going after small offenses DOJ is able to disrupt potential plotters "earlier than if we waited for them to act first."[171] The DOJ also stated the report "relies on a faulty assumption that every referral from an investigative agency should result in a criminal prosecution and ignores the reality of how the war on terrorism is being conducted, particularly the value of early disruption of potential terrorist acts with proactive investigation and prosecution."[172] The DOJ recently issued a "white paper" on the national counterterrorism record, further explaining that, "Significant resources have also been devoted to the investigation and mitigation of threats, many of which may not result in criminal prosecutions. Our prevention strategy measures success not only by prosecutions brought and won, but also by threats disrupted and terrorist acts avoided."[173]

Professor David Carter of Michigan State University has noted that evaluation is a critical component to determine if our strategies are successful, but he argues, "Typically, superficial data are collected nationwide... and are used as a barometer to measure program success. While these data provide insights on activity; however, they provide little insight on success."[174]

The simplest, but perhaps the most important, quantitative analysis would be to compare the number of attempted attacks versus the number of successes. For example, the Israelis feel that they have sufficient credible data to claim a success rate of 80% in

---

[171] Bryan Sierra, quoted in Dan Eggen, "Terror Prosecutions Drop; Analysis Show a Spike After 9/11, Then a Steady Decline" *Washington Post*, September 4, 2006, A6. Available from http://www.washingtonpost.com/wp-dyn/content/article/2006/09/03/AR2006090300768.html (accessed February 28, 2007).

[172] Press Release, *FBI And DOJ Response To TRAC Report*, http://www.fbi.gov/pressrel/pressrel06/trac110306.htm (accessed November 5, 2006).

[173] *Counterterrorism White Paper*, US Department of Justice (June 22, 2006), 12 https://www.hsdl.org/homesec/docs/justice/nps03-010807-03.pdf (accessed December 14, 2006).

[174] Email from Professor David L. Carter to Thomas M. Finan, Counsel and Coordinator House Committee on Homeland Security (August 12, 2006) on file with committee as referenced in *LEAP: A Law Enforcement Assistance and Partnership Strategy Improving Information Sharing Between the Intelligence Community and State, Local and Tribal Law Enforcement* (Washington, DC: Congress. House. Select Committee on Homeland Security, Democratic Office, September 2006), 15. Available at http://www.fas.org/irp/congress/2006_rpt/leap.pdf (accessed March 7, 2007).

stopping suicide bombing attacks.[175] In our analysis, we have very limited data for the number of attempts, but we know that there have been no successful attacks. Can the absence of attacks in of itself demonstrate the effectiveness of our reforms? Such a deduction would be a logical fallacy, a *post hoc ergo propter hoc* (coincidental correlation), in that we don't know if the lack of attacks is due to the design of our domestic intelligence apparatus, e.g., improved and better-coordinated intelligence, or some other factor. Al Qaeda's capacity to attack may have been sufficiently vitiated because of our foreign intelligence efforts by the CIA, or the Department of Defense efforts in Afghanistan and elsewhere may have degraded al Qaeda's capacity or actually interdicted plots. On the other hand, other, non-intelligence counterterrorism tactics, e.g., more border security, may have prevented attacks. Finally, Al Qaeda may also thus far have simply decided not to attack. Similarly, since in a free and open society no system can stop 100% of attacks, it would be wrong to deduce that a successful attack necessarily meant that our current intelligence structure was ineffective.

Absent sufficient quantifiable data about the number of attacks that we have prevented, we are largely left with a qualitative approach. For example, one useful starting point is to examine how we are performing in light of the National Security Strategy of the United States. As the Strategy points out, the President signed the document with the expectation that "our vast intelligence enterprise will become more unified, coordinated, and effective."[176] The fifteen objectives of the Strategy provide a reference standard on the need for further change, and these strategic and mission objectives center on tailoring our intelligence and counterterrorism apparatus to the threats of the 21st Century.

As detailed in the previous chapters, there are many who think that our efforts at reform have not addressed the fundamental problems with our domestic counterterrorism system, and our domestic counterterrorism efforts are not "united, coordinated and effective." How much further change is necessary? There is clearly a national consensus that the embryonic fusion centers are a primary organism to address some of the

[175] Joshua Sinai, A Presentation Delivered at a Briefing for Project Interchange, *Understanding the Terrorist Threats Challenging America and Israel* (Cleveland, OH, June 26, 2003).

[176] *National Security Strategy of the United States*, x and xi.

remaining shortcomings, but the potential consequences of overconfidence in the efficacy of our reform efforts merit continued careful analysis and observation to ascertain the strengths and weaknesses in our systems, and that it remains a dynamic, not static process.

In an effort to develop a more rigorous approach to evaluating Homeland Security efforts, including counterterrorism, in Section 312 of the Homeland Security Act of 2002, Congress mandated the creation of the Homeland Security Institute (HIS). The HIS operates under the sponsorship of the Department of Homeland Security's Science and Technology Directorate. Its objective is to use an integrated approach to evaluating Homeland Security systems and technologies at all stages of development, deployment and use. To date, as regards evaluating information sharing, HIS remains an unrealized tool, as it has not performed a comprehensive review of information sharing efforts. To date, HIS has focused on more specific elements of Homeland Security such as an independent assessment of DHS's strategic framework for cargo security, Homeland Security risk assessments, and an Assessment of the Transportation Worker Identification Credential (TWIC) Program.

In summary, the myriad of qualitative and conclusory findings in this and previous chapters share a common trait -- to view fairly the effectiveness of our current anti-terrorism efforts, one needs to evaluate the reform structures on a *relative* basis. Compared to the period prior to 9/11, we have made significant progress; nonetheless, in terms of our capacity to prevent future attacks, the analysis demonstrates that we have a considerable ways to evolve.

In an "evo-devo" sense, after the shock of 9/11, our domestic counterterrorism organisms have emerged from the primordial soup and are walking upright with opposable thumbs, and have organized into bands and tribes, but what additional evolution is necessary is still open to debate. The evidence presented in the previous chapters reveals large information sharing gaps, a lack of coordination of efforts, and inefficient and ineffective use of scarce counterterrorism resources all plague our Homeland Security undertakings. Moreover, even if our current systems were operating

"at a high level of efficiency and effectiveness, there is a need for Homeland Security counterterrorism to continue its evolution. The enemy is not standing still; it continues to evolve.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. RECOMMENDATIONS- WINNING THE CO-EVOLUTION RACE

In the pattern of co-evolution, both predator and prey evolve at the same time, both trying to adapt to the other. Applied to the counterterrorism arena, the number of jihadists is increasing, and the operational threat to the Homeland is also increasing as the global jihadist movement is spreading and adapting to our counterterrorism efforts, and continues to seek weapons of mass destruction.[177] Terrorists are evolving new communication systems, new tactics and new weapons. In the theory of organic evolution, if a species does not adapt to changing environmental conditions, it becomes extinct—al Qaeda's goal for the West. Thus, it is incumbent on us to ensure that our counterterrorism organisms evolve with the necessary adaptations for the new normalcy of the domestic terrorism threat environment. Consequently, the recommendations that follow in this chapter call for further significant reform in our domestic counterterrorism structures.

Our evolutionary game plan needs to include more timely and complete information sharing, including better situational awareness, a broader and more effective collaboration of all key Homeland Security partners, including an expanded role for state, local and tribal governments and non-law enforcement disciplines. We also need to include greater confidence building measures to assure the American public that their civil liberties and privacy protections are not being traded away for security.

These needs do not exist in a vacuum. They exist along side competing demands for scarce and, apparently, declining Homeland Security funds. One independent task force report estimates the shortfall for emergency responders alone is over 98 billion dollars over the next few years.[178] Therefore, it is imperative that we address these needs in the most cost-effective manner. To achieve the desired efficiencies and crucial

---

[177] United States. Office of the Director of National Intelligence. *Declassified Key Judgments of the National Intelligence Estimate, Trends in Global Terrorism: Implications for the United States* (Washington, DC: Office of the Director of National Intelligence, April 2006), 1. Available at http://www.dni.gov/press_releases/Declassified_NIE_Key_Judgments.pdf (accessed November 14, 2006).

[178] Warren B. Rudman, Richard A. Clarke, Jamie F. Metzl, *Emergency Responders: Drastically Under Funded, Dangerously Unprepared* (Council on Foreign Relations, New York, 2003), 2.

effectiveness, we should combine and connect logical Homeland Security partners in a collaborative manner such that Homeland Security prevention and response capacity, whether to deal with a terrorist attack or a natural disaster, is maximized.

A. FROM REDUCTIONISM TO HOLISM –ACHIEVING SYNERGY

The nation's nascent Homeland Security capability has benefited from the wide diversity of experiments and approaches to improve our counterterrorism capabilities. Our "national laboratory" of fusion centers, task forces, Terrorism Early Warning groups, and various other intelligence entities has provided a crucible for experimenting with different elements of counterterrorism to find the right mixture to meld a collaborative counterterrorism model. The result of this process is that we are clearly not starting at zero. We have been able to identify beneficial and detrimental elements. Nonetheless, the primary downside to this ad hoc approach is that we have yet to establish a truly collaborative effort that would achieve a high level of efficiency or high level of effectiveness. Nor have we marshaled our national counterterrorism resources into a network ready for the next time al Qaeda wants to test our mettle. The ad hoc nature of the process has also created tremendous competition for funds and turf, creating a disincentive to collaborate.[179]

Accordingly, based on the identified needs and available resources, we need to transition from this interim period of uncoordinated experimenting to a nationalized, not federalized, system. In science, this might be referred to as moving from a reductionist to a holistic or synergistic model. "Reductionism" involves a focus on the individual parts. In our counterterrorism efforts, we have too often focused on exactly that—intelligence entities such as fusion centers that exist as stand-alone units or that are isolated "intelligence" centers, omitting other key disciplines or components. Conversely, "holism" is often defined by Aristotle's famous statement: "The whole is more than the sum of its parts." Jan Smuts, diplomat, philosopher and naturalist originated the term "holism" in 1926, when he set out what should be the framework for our future counterterrorism efforts:

[179] DeYoung, 2.

> Compared to its parts, the whole constituted by them is something quite different, something creatively new, as we have seen. Creative evolution synthesizes from the parts a new entity not only different from them, but quite transcending them. That is the essence of a whole. It is always transcendent to its parts…"[180]

If we think holistically instead of parochially, we can achieve the necessary synergy to produce a more effective and efficient counterterrorism system. In adding "holism" and "synergy" to the lexicon of Homeland Security, we need to impart the essential qualities of these concepts if we want to develop collaborative counterterrorism models, not merely "coordinated" or "cooperative" approaches as described in Chapter V.

On the other hand, synthesizing our experiences, resources and organizations into a collaborative, holistic approach is not a call to abandon experimentation, or to have a centrally dictated, top-down approach. Instead, following our biology metaphor, it is a recognition that we need to end the "genetic isolation" that many counterterrorism organisms have experienced and have an "evolutionary convergence" of the best practices and characteristics of the various counterterrorism components, entities and disciplines into a true collaboration.

B. HYBRIDIZING A COLLABORATIVE COUNTERTERRORISM MODEL-FUSING MORE THAN INFORMATION

Nature has a variety of reproductive isolating mechanisms, such as seasonal and behavioral isolations, that prevent individuals of separate species from hybridizing since it is deemed advantageous for a species' survival to prevent gene flow into its pool. Too often, our organizations have misguidedly felt the same survival instinct as they have fought to preserve or acquire turf, funding and prestige by isolating other levels of government, other agencies or other disciplines. However, in order to develop a more efficient and effective counterterrorism organism that overcomes the problems identified in previous chapters, we need to overcome this reproductive instinct and recognize the benefits of hybridization. A hybridization process for counterterrorism would involve combining the best traits of different entities into one collaborative effort. One example

[180] Jan C. Smuts, *Holism and Evolution* (London: MacMillan, 1926), 367.

would be integrating the successful investigative resources of the JTTF model into a fully collaborative model that includes other key Homeland Security components and participants. This type of center, encompassing key local, state and federal resources from all of the Homeland Security disciplines, as well as the public and private sectors, would not only maximize the efficient and effective use of scarce resources, but would increase the prevention and response capacity of the national and regional counter-terrorism communities.

Of course, creating centers that are more effective is only half of the synergy formula; the other half is forming these centers into an effective Homeland Security counterterrorism network, but first we need to discuss the regional aspects of the network.

C. R.A.D.A.R. CENTERS

In keeping with Secretary Chertoff's observation that intelligence is the "radar of the 21st century," and in keeping with the benefits obtained from counter-terrorism and all-hazards resource collaboration, the Department of Homeland Security should establish **R**egional **A**ll-hazards **D**isaster and **A**nti-terrorism **R**esource (**RADAR**) centers.

RADAR centers would be jointly governed, multi-disciplinary, and combine key anti-terrorism components of intelligence, investigations and operations with the broader Homeland Security all-hazards prevention, preparedness and response community. DHS should establish a pilot **RADAR** center in region to serve as a national incubator to demonstrate and evaluate these benefits of a fully collaborative approach.

1. Regionalism and Collaboration

Because of the realization that disasters and terrorism impact regions, not just jurisdictions, the Homeland Security network should be built around regionalization. As stated recently by DHS Secretary Chertoff,

> We know that threats don't comfortably come confined to the political line drawing that describes what falls within one political jurisdiction or another political jurisdiction. Threats are risk-based, and the consequences of threats are region-based. And that means we have to look regionally at what we are doing to deal with risk. And of course, that was vividly

> exhibited on September 11th and in Katrina, where the spill-over effect of an event in one jurisdiction was acutely felt in multiple other jurisdictions. So we've begun to look at regionalization as an important positive element in determining where we put money.[181]

RADAR centers geographic coverage should encompass an area where effective operational control and efficient use of intelligence, investigations, and operations can be achieved. Towards that end, we should look to the work done by the Naval Postgraduate School and the Homeland Security Institute on finding common units of interest and the discussion regarding Capability Centers, Capability Clusters and Capability Contours. [182] The essence of this work relates to finding logically related units of interest when assessing how to coalesce Homeland Security capability.

As explained by its author, Sam Clovis, a ***capability center*** is any general-purpose jurisdiction where a capability (potential or actual application of skills and equipment to achieve an effect) can be joined with a professional area found in the idealized responder or prevention community. The community would then identify gaps and shortfalls that its own capabilities, inside that capability center, could not cover.

In some situations, a jurisdiction would have to arrange with surrounding jurisdictions (other capability centers) to create a ***capability cluster*** in order to develop the appropriate response or prevention capacity. For example, a 24/7 Situational Awareness Center (SAWC) may be beyond the personnel and technical resources of a particular jurisdiction so that agency would team up with other ***capability centers*** to staff and equip the SAWC.

It is also contemplated that there are certain desired response or prevention capabilities that a ***capability cluster*** may still not be adequate to cover. In that case, capability centers will have to consider ***capability contours*** that include those ***capability***

---

[181] Keynote Address by Secretary of Homeland Security Michael Chertoff to *The 2006 Grants & Training National Conference* (Washington, D.C. Grants & Training 2006 National Conference, November 28, 2006).

[182] Sam Clovis, Discussion Draft, *Thinking About National Preparedness, the National Planning Scenarios and Jurisdictional Own-source Capabilities*, Center for Homeland Defense and Security, Naval Postgraduate School. The essence of this work relates to finding common units of interest when assessing Homeland Security capability to place in clusters.

centers and ***capability clusters*** that lie along lines of communication that can provide the needed assets. These ***capability contours*** may well go across state lines and encompass vast areas of the country, especially in more sparsely resourced regions.

The **RADAR** centers will thus have to be regionally designed in a "bottom-up" but horizontally integrated approach that takes into account the unique capabilities of each participating agency, along with other relevant considerations such as geography, politics, culture, and demography.

2. Governance

The myriad of information sharing issues described in this thesis frequently shares a common thread of a failure to collaborate among the different levels of government. Co-location and coordination of resources is beneficial but it does not achieve the full benefits of collaboration described in Chapter V and elsewhere. To be truly collaborative will require joint design and governance of a **RADAR** center, with the accompanying mutual authority and accountability for success, sharing of resources and rewards.

It becomes self-evident, then, that a successful counterterrorism model requires that the **RADAR** centers are multi-jurisdictional. All levels of government-- state, local, tribal and federal-- have to participate. "Federal" includes more than the FBI. DHS, including its key agencies, such as ICE, ATF, Secret Service, etc., must be part of it. A special outreach needs to be made to tribal authorities that have traditionally been excluded from the process. Including tribal representatives in the design and implementation of a **RADAR** center may overcome this problem.

Governance of multi-lateral, multi-disciplinary centers is one of the trickiest problems to solve; inter-governmental and inter-disciplinary rivalries for funding, prestige and control continue to impair our national counterterrorism efforts. The quasi-military nature of the law enforcement agencies that participate in these centers also contributes to parochialism, as there tends to be a "chain of command" culture that promotes an agency specific focus. Finally, since the vast majority of the personnel at fusion centers are "donated" staff, still paid and employed by their parent agency, there is

a completely natural and understandable tendency for such staff to be focused on serving and meeting the needs of their parent agency. This "sectarian" tendency can present a major barrier to collaboration.

To overcome both the natural tendency to favor one's home agency, as well as the more dysfunctional tendencies to battle for ego, prestige and resources, the **RADAR** centers should look to the non-profit corporate governance model. In a corporate model of governance, a board of directors governs the organization. A board is a group of people who are legally charged with governance and the board is responsible for setting strategic direction, establishing broad policies and objectives, and hiring and evaluating the chief executive officer. The board of directors does not manage the day-to-day activities of the organization. Instead, the directors appoint officers who carry out these duties.

The corporate board model recognizes the potential conflicts of interest that may exist among the board of directors. Therefore, the laws governing corporations require that a corporation is ultimately accountable to its owners –stockholders in the case of for-profits and the public in case of non-profits. That accountability is accomplished by requiring that the Board of Directors of each corporation must represent the stockholders or the public. As a result, members of a governing Board have certain legally required duties, including duties of care, loyalty and obedience.

In a **RADAR** center, a board of directors' model would enable the governance structure to be comprised of representatives of the major stakeholders, but as a member of the board, each member would owe these fiduciary duties of care, loyalty and obedience, *not to their home agency but to the public at large*.

Finally, if a **RADAR** center is going to foster a multi-disciplinary collaboration, the board needs to have representation from disciplines beyond just law enforcement groups. Since law enforcement agencies will likely provide the vast majority of resources in a **RADAR** center, it may be equitable for the various non-law enforcement disciplines to select one or more representatives to an executive governing board, and the remainder of disciplines collectively selecting a representative on an advisory board that makes

recommendations to the executive board. This arrangement is especially appropriate for agencies, both law enforcement and other disciplines, which do not have full-time employees in the **RADAR** center.

3. Multi-disciplinary -- Terrorism Early Warning

As described above and elsewhere, there is a need to broaden the domestic intelligence and counterterrorism community beyond the law enforcement discipline. While law enforcement agencies have the specific responsibility to interdict terrorism, and thus form the cornerstone of intelligence, investigations and operations, a cornerstone is just part of the foundation. Public Health, Fire, Emergency Management, Utilities, Transportation, and Private Sector Security are examples of key players who need to be participants. Each of these disciplines is a both a consumer of counterterrorism intelligence and a partner in the *entire intelligence cycle*.

For example, as described above, the CDC and Public Health would be on the front line of any WMD scenario, such as an Anthrax or other bioterrorism attack. This response role is widely recognized, but health professionals also need to be in the loop of predictive intelligence so they can be alert and prepared for potential attacks. Similarly, their frontline public health and medical positions makes them ideal collectors of potential terrorism related intelligence. Their knowledge would be crucial in analyzing a WMD threat scenario, in producing a finished intelligence product, and in the dissemination of information to support prevention efforts.

The question is, however, how do you incorporate non-law enforcement disciplines in an effective manner? Most fusion centers do not have full-time representation from other disciplines. The proliferation of multiple centers may further limit the availability of representatives. Consequently, a regional center approach, in which disciplines could "share" a representative, will make the participation of non-law enforcement disciplines more feasible. Additionally, making these other disciplines full partners by including them in the governance structure on the proposed executive governing board and advisory boards, would increase their investment, maximizing the likelihood their participation would be more fulsome.

Based on the LA-TEW model, a Terrorism Early Warning group (TEW) can provide a place within the **RADAR** centers to house a multi-disciplinary working group to identify trends and assess potential threats. Because of their multi-disciplinary nature, such groups are well suited to provide the expertise to create "target folders" that assess potential targets of terrorism, establish common response protocols, and assist in mission planning, incident management planning, and allocation of resources before and during actual events.

A Terrorism Liaison Officer (TLO) program within the **RADAR** centers would complement the TEW by providing points of contact within each agency in the various Homeland Security disciplines. These specially trained and screened TLO's would provide a conduit for multi-lateral information sharing—to and from the TEW, and to and from the various agencies in the TLOs' respective sectors and disciplines. This also addresses the situations where full-time participation by a particular discipline or agency in a **RADAR** center is not feasible.

The TEW's can also be an effective vehicle for bringing successful public private partnerships into the **RADAR** centers. For example, the Pacific Northwest Economic Region (PNWER), is a public/private partnership composed of legislators, governments, and businesses consisting of five states (Washington, Oregon, Alaska, Idaho, and Montana) and three Canadian jurisdictions (British Columbia, Alberta, and The Yukon Territory), and is perhaps the premier example of an extant public-private collaboration. PNWER has designated nine business and industry sectors within the PNWER jurisdictions and developed proactive working groups for each sector. As an illustration, the Homeland Security Working Group incorporates a regional partnership for infrastructure security, which focuses on security issues in the United States and Canada. One of its major emphases has been on critical infrastructure protection, focused especially on the interdependencies of the region's critical infrastructure.

The other partnership that should be integrated in the **RADAR** centers are the Information Sharing and Analysis Centers (ISAC's) described in Chapter VI and representing the major critical infrastructure and key resources of our nation. Many of the

ISAC's already have a robust information sharing capacity and would provide an ideal vehicle to integrate non-law enforcement disciplines, especially the private sector participants, into the **RADAR** collaboration.

Lastly, the military discipline needs to be involved in the **RADAR** centers. This is not to suggest that Posse Comitatus issues be raised by involving the military in domestic intelligence collection or other law enforcement activities; however, Northcom's civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Northcom's mission also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction.

Equally important is that Northcom has the responsibility to provide for *homeland defense* in the event of an attack. To accomplish this mission, Northcom has substantial intelligence capabilities to monitor these threats. Currently, should Northcom develop intelligence about an imminent attack that intelligence would have to flow through many bureaucratic layers before it would be relayed to local and regional officials, who might be in the best position to interdict and who certainly would be the first responders to the scene. These layers inhibit timely, complete and accurate information sharing. The delays and layers are unnecessary, and may have catastrophic consequences. Likewise, if SLT officials develop time sensitive information that would be crucial to Northcom to defend the Homeland, it too would have to pass through so many layers before it reached Northcom that it may be too late to prevent an attack.

Consequently, in order to ensure timely, complete and accurate sharing of homeland security information with the military, we need to remove the extensive layers of bureaucracy. This can be accomplished by either placing Northcom liaisons in RADAR centers, or where this is not practical, establishing a virtual two-way 24/7 connectivity.

4. Co-location and Collaboration

We have discussed the advantages of a TLO program for extending the reach of partnerships to agencies who cannot assign individuals to the **RADAR** center; however,

personnel and resources should be co-located whenever feasible. Co-location can be pivotal to overcome barriers to collaboration. Co-location enables the "shared space" that Michael Schrage argues is indispensable to collaboration. As he puts it, "If you don't have a shared space you're not collaborating. One of the tests of a shared space is whether it's an invitation to innovation. Is it creating opportunities for other people to add value?"[183]

Thus, establishing "routine" interactions in a **RADAR** center between and among all of the Homeland Security disciplines, rather than meeting on the "battlefield" when there has been a disaster or attack, will build the "collegiality, trust, flexibility, openness, mutual respect, social capital, and pathways of communication" that Hocevar, et al, have identified as necessary for collaboration.[184] This can also be thought of as the "social capital" problem—determining how trust is "built, maintained, and used in a multi-agency, multi-level environment."[185]

Where co-location is impractical, information sharing and cooperation can be accomplished to lesser extent by technology advancements, such as video and other secure communication networks. Of course, as the point has been made, cooperation is not collaboration. To achieve a "shared space" virtually and to collaborate in a "virtual" sense is difficult, but there have been some advances. The Joint Regional Information Exchange System (JRIES) was a very successful partnership involving the Defense Intelligence Agency and major local police intelligence units, which were connected via a secure virtual private network. JRIES was more than just an information sharing cooperative mechanism because it contained a collaborative software tool called "Groove." Groove created a collaborative space where organic conversations, requests, postings, idea sharing, etc., could easily take place, both on an extended and real-time basis.

---

[183] Michael Schrage, *Shared Minds: The New Technologies of Collaboration* (New York: Random House, 1990).

[184] Ibid., 5.

[185] As described by Dr. Chris Bellavita, Naval Postgraduate School course Introduction to Homeland Security.

Many of the collaborative aspects of JRIES collapsed when DHS took it over and expanded it into the Homeland Security Information Network (HSIN). As HSIN, the membership was increased to thousands of users in many disciplines, and the Groove software was removed due to technical limitations of the software to support this huge number of users. The sheer size of the membership and the absence of the Groove collaborative space impaired the previous collaborative nature. While HSIN can still function as a national information sharing system, the JRIES' executive board, which includes intelligence directors from New York City, Washington, and Los Angeles, broke off discussions with DHS and ended the effort to assimilate the system into the HSIN. The board is attempting to reconstitute JRIES along its original lines.[186]

The Pacific Northwest National Laboratory (PNNL) has done considerable research on establishing a pilot *virtual capability* for counterterrorism centers to provide virtual collaborative spaces, including but not limited to two-way information sharing and virtual analysis spaces. This encompasses focused research from PNNL's National Visualization and Analytics Center work on cooperative analysis, as well as enabling users to define their own operating picture from a common operating picture that participants in a **RADAR** center would share. As explained by PNNL's Dr. Steve Stein, a virtual capacity in a **RADAR** type center would have two-way information sharing based on a secure and resilient system with analysis produced by a team of core resident and virtual analysts from local, state and federal homeland security disciplines. They would share a largely virtual database to enable integration, assessment, and secure, tailored dissemination of information provided to key stakeholders.[187]An organization such as PNNL should be enlisted as a technology facilitator within a pilot **RADAR** center to serve as a national test bed for developing this virtual capability and other counterterrorism technologies.

---

[186] Alice Lipowicz, "JRIES Homeland Security Network Falls Victim to Policy Dispute." *Government Computer News*, October 2005.Available at http://www.gcn.com/online/vol1_no1/37223-1.html (accessed February 3, 2007).

[187] Interview with Dr. Steve Stein, Pacific Northwest National Laboratory, August 16, 2006. Concept paper, Puget Sound/Washington State Partnership Information Sharing Working Group, December 14, 2006.

5. Subject Matter Coverage

The subject matters covered in a **RADAR** Center should address an "all-hazards" and "all crimes approach."

a. The "All Crimes" Approach

A **RADAR** center needs to be able to address the broad array of crimes that may facilitate terrorism or threaten Homeland Security. The "all crimes" focus on potentially terrorism related offenses is an integral part of a terrorism prevention strategy. This approach allows disruption of potential terrorist acts by arresting and prosecuting potential terrorists and their facilitators and supporters without waiting for a difficult to detect terrorism crime, or worse, a successful terrorist attack. An important caveat is that the **RADAR** center must ensure that those prosecutions labeled as "terrorism related" are carefully scrutinized in order to avoid unfairly and inaccurately labeling someone as a terrorist or supporter.

The "all-crimes" term can also be misleading, as no Center can ultimately be effective without a sharp focus. Every fusion center has limited resources and cannot afford a scattergun approach. Moreover, the funding that is supporting many of these centers, especially the analysts, is designed to support Homeland Security. There was considerable resistance to allow Homeland Security funds to be used for personnel costs. One of the fears was a misuse of the personnel to supplant local funding responsibilities for general law enforcement responsibilities. To the extent that Homeland Security grant funds are used to address non-Homeland Security general crime problems, such misuse would not only constitute a violation of the grant requirements, but would also undercut the tenuous support for personnel funding. The fusion center guidelines aptly describe the proper focus as being on crimes that have a "potential national security implication."[188] Examples of criminal activity that have an interrelation with terrorism and threaten Homeland Security are certain types of organized crime and gangs. Without a national security nexus focus, with the enormous crime problems that our communities face, and the fading public interest in counterterrorism, we risk our fusion centers becoming "all-crimes *but* terrorism."

[188] Unpublished Draft National Fusion Center Guidelines, Department of Homeland Security, 2006.

b. "All Hazards"

The "all hazards" method acknowledges the reality that the threat of natural disasters and hazards, such as earthquakes, hurricanes and pandemic flu is much more likely than a terrorist attack, at least for the present. It also recognizes that the same structures that we use to prepare to respond to and mitigate "all hazards" provide a framework for responding to and mitigating the impacts of a terrorist attack. Thus, if we build capacity to respond to natural disasters, we will at the same time increase our capacity to deal with intentional disasters. Additionally, the partnerships and collaborations we develop for these natural disasters, e.g., public health and law enforcement preparing to deal with pandemic flu, build the social capital to collaborate on information sharing to prevent terrorism. Finally, there are efficiencies that "clustering capabilities" such as situational awareness centers, analytical groups, etc., can achieve by sharing capabilities in everyday natural disaster planning and preparation.

6. Component Groups

As outlined in Chapter III, a **RADAR** center needs to fuse more than just intelligence. Effective counterterrorism relies on the synergy that arises from the counterterrorism triad. To be effective and efficient, as well as garner short and long-term support, a RADAR center needs to have a robust program containing three principal components: Intelligence, Investigations, and Operations.

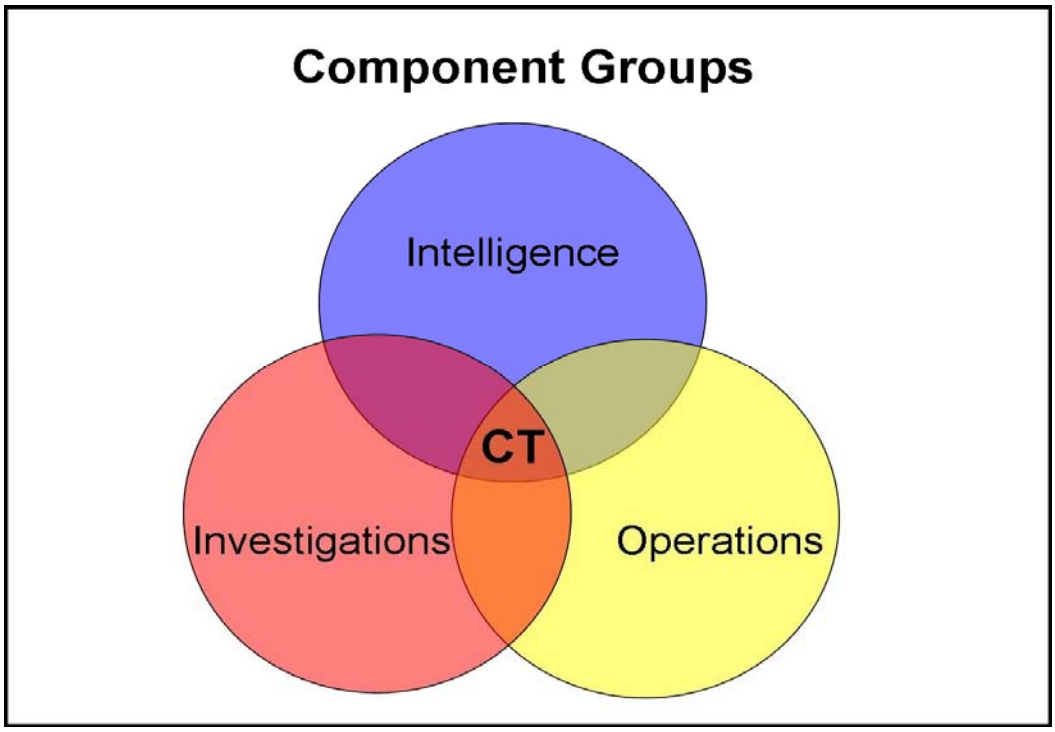


Figure 8. **RADAR** Center Component Groups

a. Intelligence and Investigations Components

To achieve the desired synergy, Intelligence, Investigations and Operations should be placed under one governing structure, and ideally, one roof. Jointly coordinating the counterterrorism triad in one center allows for the most efficient information sharing among these critical counterterrorism components. It also allows for the coordination and focusing of efforts that are difficult to achieve when these components are housed separately, especially under different chains of command.

Intelligence and **Investigations** would each include the logical subgroups of terrorism, and crimes with a national security implication, e.g., certain types of organized crime, and gangs, with the **Intelligence** component also containing a regional crime analysis component to identify region-wide crime groups or patterns that may have a nexus to homeland security. Other Intelligence sub-groups might typically include Special Events support analysis and Critical Infrastructure and Key Resource Protection groups.

b. Operations Component

Additionally, to meet the needs of the **RADAR** region in an efficacious manner, the **Operations** component should house a 24/7 Situational Awareness and Watch Center (SAWC). This will enable the region to have real time awareness and connectivity with international, national and regional partners. Whether it is information from Interpol about a bombing in London, or information from a traffic stop in the far reach of the **RADAR** center's area, to maximize the chances of preventing an attack in a region, a center needs to have this level of awareness.

Additionally, the SAWC component of a **RADAR** center will be able to provide real-time support to field units throughout a region. Along the lines of the recently created New York Police Department's Real Time Crime Center, or Washington DC's Support Operations Center, this access to information will enable a **RADAR** center to provide immediate support and two-way information sharing to field units, such as patrol officers, detectives, firefighters, health officials, etc. In the event of an actual attack, the 24/7 Situational Awareness and Watch Center will also be able to provide the real time connectivity and support to first responders and Emergency Operations Centers in the region.

Integrated with the **Operations'** SAWC will be the capability to send out Field Response Units from a **RADAR** center's investigative and intelligence components to support officers in the field with potentially terrorist related incidents and investigations, e.g., a stop of suspect on the Terrorism Watch list.

Finally, the **Operations** component will address the significant problem with enormous Homeland Security dollars being spent on highly technical equipment that is duplicative because individual entities, i.e., ***capability centers*** throughout the region are separately purchasing, operating and maintaining it. This problem is exacerbated by the lack of personnel at each entity to effectively maintain and deploy such equipment. Using the ***capability cluster*** concept, a regional, **RADAR** based, Technical Support unit would be able to support the technical needs of both the Center, as well as have the expertise and equipment to supplement regional needs in a more efficient manner. A tremendous example is the technical support capability achieved by housing a regional

computer forensics capacity in the Arizona Counterterrorism Intelligence Center (ACTIC). ACTIC demonstrated that it is immensely more efficient to have its center staff a small cadre of experts from multiple entities who purchase the hundreds of thousands of dollars worth of computer forensic equipment and then certify agency representatives who can come to their center to use the equipment on an as needed basis. This eliminates wasteful duplication of expensive equipment that has a short obsolescence cycle, and allows smaller jurisdictions to develop a forensic capability that they could never achieve on their own.

7. "Primary" versus "Secondary" Centers

DHS cannot ignore the political realities of the battle between major urban areas and states over control of resources and funding, and the Information Sharing Environment Plan recognizes that both entities may potentially have fusion centers. However, the Plan also states that each state will have a "primary" fusion center serving as the central interface point with the federal government for that state. This is setting up a battle in states that have more than one fusion center. For example, in New York State, will the federal government's primary interface be limited to NYPD's impressive fusion center or the also impressive Upstate New York Regional Intelligence Center (UNYRIC)?

While DHS is rightfully concerned about sustainability and about the ability to provide a base-line level of support to the ever-growing number of fusion centers, designation of only one center is again a "top-down, one size fits all," federal centric approach. Instead, DHS should let the **RADAR** centers arise as a natural outgrowth of the local organic conditions, including culture, demographics, resources, etc. DHS should recognize the regional benefits of the regional **capability clusters** process described above versus a geographic based approach.

It may be appropriate to have only one primary fusion center in some states; however, it may be appropriate for some areas to have more than one fusion center that interfaces directly with the federal government. Nowhere is this more evident than in the well-respected National Capital Region Intelligence Center located in Fairfax County Virginia. Because the regional partners formed this center according to their capabilities

and regional needs, it encompasses Homeland Security groups from Virginia, Maryland, and Washington DC. The critical assets and high threat of this area make it appropriate for this fusion center to be designated to interface directly with the federal government, as well as the Virginia and Maryland state fusion centers.

As another example, most observers would agree that both the Los Angeles Joint Regional Intelligence Center (LAJRIC) and the State Terrorism Threat Analysis Center (STTAC) in California have an equal need to interface and coordinate directly with the federal government. As previously described, LAPD Chief Bratton has already voiced serious concern about the timeliness of information sharing with the federal government. Adding a layer to "interface" or coordinate with will likely exacerbate this problem. We need to remove as many layers as possible to allow for the most timely two-way information sharing and related responses. Technology, training and a commitment to a multi-lateral approach certainly make it feasible to interface directly with more than one center.

D. A NATIONAL COUNTER TERRORISM NETWORK

Homeland Security Presidential Directive 8 calls for strengthening information sharing and collaboration capabilities by establishing prevention frameworks "based on expanded regional collaborations that are linked in a national network." Moreover, the Information Sharing Environment Implementation Plan calls for the establishment of a nationwide and integrated *network* of State and major urban area fusion centers to facilitate effective terrorism information sharing, but the Plan does not provide details of how such a network would be constructed. DHS and the ISE Plan indicate that they are still in the final planning stages of an effort to identify a State or regional Evaluation Environment that would develop the concept of a network.

The proposed **RADAR** centers, interconnected within a **National Counterterrorism Network** (**NCN**) would provide the environment described in the ISE Plan to develop a network. The **NCN** will consist of the **RADAR** centers, connected horizontally with other **RADAR** centers, and vertically integrated with the National Counterterrorism Center. Depending on their needs and capacities, some smaller **RADAR** centers might coalesce into a capability cluster of a **Super RADAR** center.

The **National Counterterrorism Network** and **RADAR** centers will both lessen information sharing problems, such as dissemination issues, and provide the requisite auspices and access to international and national counterterrorism intelligence and resources that the various **RADAR** centers will need to be effective. This will provide a **National Counterterrorism Network** consisting of **RADAR** centers protecting the nation in a concentric approach, with the common "center" being the NCTC for terrorism related issues.

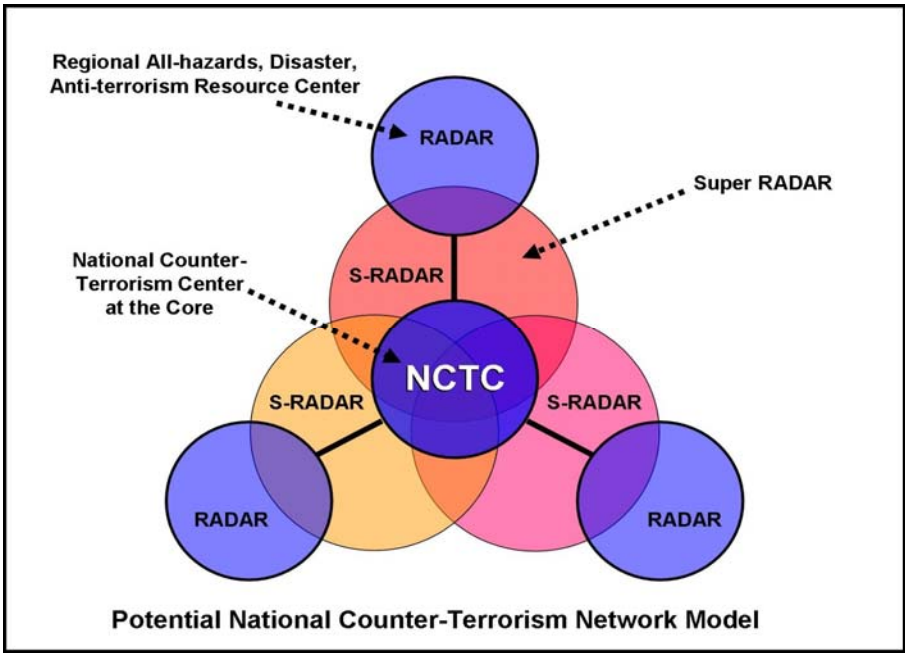


Figure 9. Potential RADAR center cluster within a National Counterterrorism Network

To facilitate timely, complete and accurate information sharing, both **RADAR** and **Super RADAR** centers need to be under the auspices of some entity that has the national standing to establish and enforce information sharing standards, certifications, technology protocols, etc., and have the resources to coordinate this national effort. Fortunately, two entities are ideally situated to meet both the terrorism and "all-hazards" networking and support needs of the **RADAR** centers: To handle the terrorism aspects, the National Counterterrorism Center (NCTC), to handle the "all-hazards" aspects, the National Operations Center's National Coordination Center (NCC).

The terrorism portion of the **RADAR** centers will operate under the auspices of the National Counterterrorism Center (NCTC). The NCTC is the proper entity since it has the national mandate to coordinate all domestic terrorist related information and operations. Also with the interrelated Interagency Threat Assessment and Coordination Group, the NCTC is already designated to perform an information coordination function nationally. The **RADAR** centers must, for timely and accurate information sharing and situational awareness, be able have two way sharing directly with the NCTC. The NCTC will be responsible for horizontal sharing with the NOC and other federal and international agencies of terrorism related information from the **RADAR** centers.

To lessen the problems of circular reporting and the "white noise" problem from overproduction of "unfinished" intelligence products, should time allow, all **RADAR** centers will be encouraged to send bulletins and other reporting information to the NCTC's Interagency Threat Assessment and Coordination Group (ITACG) for vetting and dissemination to the other components of the **NCN**. The ITACG will be jointly run and staffed by a co-equal arrangement of state, federal and local representatives. This revolutionary step will represent a quantum leap forward in the national intelligence cycle, ensuring that all Homeland Security intelligence is sent to one location. It will not replace the intelligence cycle efforts at the **RADAR** centers, but will enable for the first time a nationalized intelligence cycle of needs identification, collection, analysis, reporting, dissemination and feedback.

The "all-hazards" portion of the **RADAR** center will function under the auspices of the National Operation Center (NOC) and its accompanying National Coordination Center, enabling information sharing and situational awareness of natural disasters. For example, the reporting to the NOC will enable the NOC to disseminate the information to the remainder of the **NCN**, while the National Coordination Center addresses response and recovery coordination. Since the centers are "all-hazards," and since FEMA's mission within DHS is to lead the effort to prepare the nation for all hazards and effectively manage federal response and recovery efforts following any national incident, both **RADAR** and **Super RADAR** centers should be administratively "be placed" in the existing FEMA regions for purposes of coordination and support of the all-hazards intelligence functions of the centers.

Figure 10. FEMA Regional Offices

However, this is not to suggest that the individual **RADAR** centers have to report through the layer of the FEMA region to share information with the NOC. Should a **RADAR** center or the NOC deem it advantageous to communicate directly versus coordinating through the FEMA region, either entity may do so. This is also not to suggest that the **RADAR** centers will replace existing emergency operation centers (EOC) or FEMA's role. EOC's will continue to be the physical locations where organizations come together during an emergency to coordinate response and recovery actions and resources and manage incidents. However, effective coordination and management of incidents will require timely and accurate intelligence. The **RADAR** centers will provide this intelligence support. For example, in the event of a pandemic flu, the significant analytical capability of a **RADAR** center could be put to use to provide analytical support to Public Health to monitor disease progression in a region.

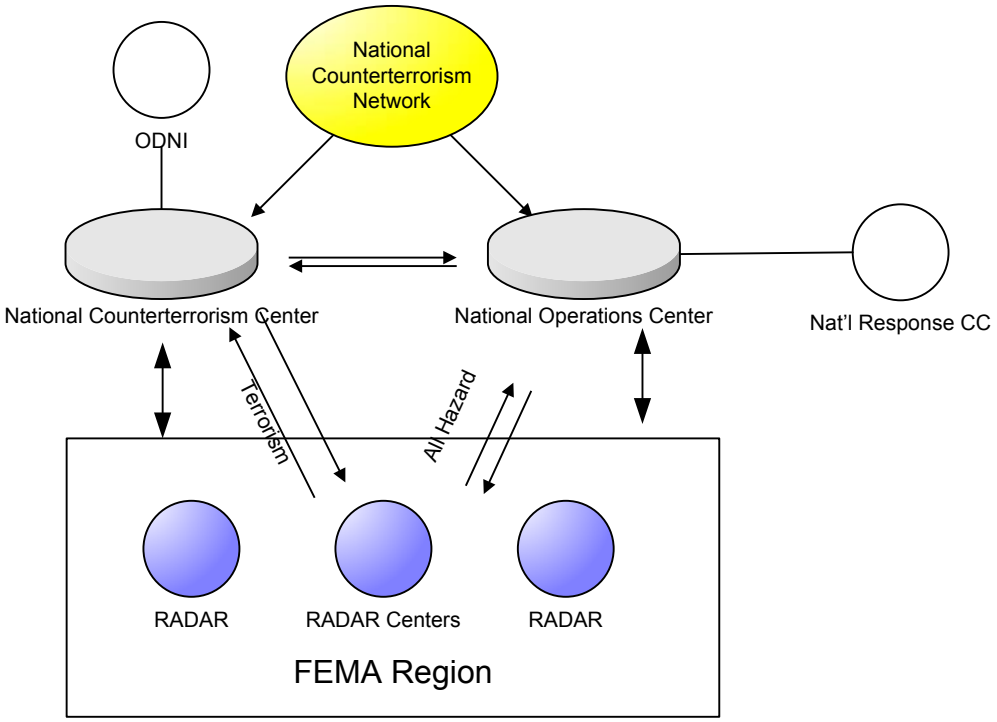


Figure 11. Proposed National Counterterrorism Network

E. PERSONAL PRIVACY AND CIVIL LIBERTIES PROTECTION

The capabilities of the counterterrorism and intelligence communities will be enhanced if these recommendations are enacted and a **National Counterterrorism Network** is created. This positive development should correspondingly be matched with an enhanced system of checks and balances to protect our civil liberties and privacy. Additionally, to realize its full potential, a **RADAR** centers and the **National Counterterrorism Network** will need the full participation and support of the broad array of proposed partners, including the American public. They will further need the support of policymakers for funding and other resources. Policymakers across the political spectrum and the public have expressed concern about the possible erosion of privacy and civil liberties in the name of security. Washington DC Chief of Police Cathy Lanier warned that even though fusion centers are becoming common, navigating the various state and federal privacy laws put us in a precarious position, warning about the possible loss of community support should civil liberty concerns not be addressed.[189]

[189] Sheridan.

Thus, to earn the public's trust, the protection of personal privacy and civil liberties have to as fundamental to a **RADAR** center and the **National Counterterrorism Network** as the promotion of information sharing. This underscores the need and benefit of enforcing national standards.

Fortunately, the contemporary Homeland Security community brings with it a proven commitment to the twin pillars of security and liberty. To cite just two examples, Public Health operates within strict medical privacy regulations, and the Law Enforcement community carries out its responsibilities under a sworn oath to uphold the Constitution. Thus, it is fully expected that all **RADAR** participants will bring with them an inherent respect and commitment to constitutionally sound anti-terrorism procedures, and they will fully comply without hesitation with all applicable federal, state and local privacy protections. However, those good intentions are not sufficient. History has shown that even well intentioned advocates may unintentionally transgress. Thus, privacy and civil liberty protections must be as robust as the anti-terrorism and analytical systems. This will entail both oversight and transparency.

Oversight should be modeled on the IRTPA requirements for the Office of the Director of National Intelligence. The **NCN** and **RADAR** centers should implement the recommendation in the IRTPA to emulate the requirement of a Civil Liberties Protection (CLP) Officer who directly reports to the Centers' directors. This person would also work in conjunction with a Privacy and Civil Liberties Oversight Board, again modeled on the IRTPA requirement for such a board to be established. The Oversight Board would report to the Executive Governing board of the Center.

In providing oversight, the Oversight Board would be charged with reviewing regulations, policies, and laws relating to counterterrorism to ensure that each of these areas takes into account privacy and civil liberties concerns, while the CLP Officer monitors day-to-day specific activities. The Board and the CLP Officer would also fulfill an advisory role to **RADAR** participants and managers, e.g., in participation in interpreting and implementing legal requirements for protecting privacy.

Both the public and the **RADAR** center participants must have confidence in the Board and CLP Officer. To inspire this confidence, those filling these positions must

have the necessary reputation, education and experience, as well as proper clearances, to monitor anti-terrorism efforts for compliance. The Board should include a member of the public, such as a former judicial officer, along with legal officials not directly associated with the Center. The Board and CLP Officer should issue publicly available reports on the Center's successes and failures to implement protections for and promotion of civil liberty and privacy, along with remedial actions. The Board and CLP Officer should serve as a sounding and review board for those with concerns related to these areas. Neither the Board nor CLP Officer would have authority over any aspect of the Center. Their effective "power" comes from the reporting role that their reports play in informing the Center directors, judicial and prosecutorial officials (in the case of misconduct), legislators and executives who can implement reforms, and finally, the public.

RADAR centers and the **NCN** design must overcome the cognitive hurdle of the natural reluctance some elements, such as the intelligence component, will have towards the transparency needed for public confidence. Transparency does not require compromising the counterterrorism triad. It can be accomplished via confidence building measures such as public outreach and education about the operation of the centers. As just one example, the CIA and FBI have demonstrated that websites can be used to solicit crucial information, educate the public, and provide transparency without hindering sensitive operations. These measures have to be substantive, not superficial. Measures such as public meetings, information brochures, a public website, etc., must include public involvement in the design of education and outreach process.

~~F. PROPOSED PILOT PROJECT~~

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

THIS PAGE INTENTIONALLY LEFT BLANK

IX. RECOMMENDATIONS FOR FURTHER RESEARCH

There is a paucity of data available on the full spectrum of the financial implications of creating a National Counterterrorism Network of regional RADAR centers. This knowledge gap is consistent for both the regional and national effort. We do not have good estimates of the major cost categories, such as capital, personnel or operating costs. Current Homeland Security funding for state and local government generally prohibits the use of funds for personnel or buildings. Consequently, the vast majority of existing collaborative counterterrorism efforts involves "donated" personnel and facilities with the more easily measured one-time grants being used for start-up and equipment costs. Personnel and facilities are the biggest costs of operating a counterterrorism center, but they remain hidden, other than to the agencies that donate them.

Concomitantly, fiscal prudence dictates that we adopt a sustainment plan for the regional centers and national counterterrorism network. Presently, we are victimized by a system of grants and other short term funding. We need to identify a national funding plan that is consistent with the long-term nature of the terrorism threat we face.

There is also a need to follow up on the work done by the Naval Postgraduate School and others in identifying the ideal composition of the potential regions.191 The geographic, demographic and resource diversity in America makes it impractical to have a "one size fits all" approach. Much more research needs to be done to identify resource capacities, threat commonalities, and the like to either divide the country into ideal regions or unite them within the most effective structure. Likely, this will continue to be an experimental process in which regional "laboratories" will continue to provide empirical data for further research.

Finally, there is much anecdotal evidence about waste in Homeland Security counterterrorism spending, but we lack metrics to evaluate how effectively the funds are

[191] Discussion Draft, *Thinking About National Preparedness, The National Planning Scenarios and Jurisdictional Own-source Capabilities*, Center for Homeland Defense and Security, Naval Postgraduate School. The essence of this work relates to finding common units of interest when assessing Homeland Security capability to place in clusters.

being spent. Further research in identifying measurement standards will help to compare the efficacy of different approaches and develop quality control programs. Independent review teams, perhaps by an Inspector General's office or GAO office, should be assigned to critically review the fusion centers to determine what is working and what needs to be improved.

X. CONCLUSIONS

All evolution in thought and conduct must at first appear as heresy and misconduct.

George Bernard Shaw

Homeland Security needs to be an evolutionary process, wherein America is continually adapting to a changing threat environment. As in biology, the process of natural selection drives evolutionary change. Natural selection is simply "survival and reproduction of the fittest," in which individuals who are better adapted to a given set of environmental conditions have an advantage over those that are not as well adapted. The key, however, is to keep in mind that we are in an evolutionary race with terrorists. In a biological sense, evolutionary fitness refers to the ability to survive. In a Homeland Security sense, evolutionary fitness refers both to our ability to survive and to our ability to evolve faster than the terrorists — the ability to evolve faster because to evolve otherwise risks a pattern of suffering the lethal consequences of an attack before adapting; the ability to survive because the WMD threat makes this more than hyperbole.

Natural processes of resistance to organizational change, coupled with a complex system of federal, state, tribal and local government inhibit innovation and the pace of change. For example, nearly six years after 9/11, we are still focused on and searching for a coherent way to share important information. Moreover, while information fusion is critical, much more than just information needs to be fused.

A review of the causes of the September 11 attacks on America highlight that we failed to prevent the attacks because there was a failure to fuse intelligence, investigations and operations. We thus lost their synergistic potential as a counterterrorism triad. There was an intelligence failure to effectively integrate and analyze disparate pieces of information stored in multiple locations and agencies in order to produce actionable intelligence. There was an investigative failure to effectively use our criminal investigative processes to prevent the attack, and there was an operational failure in that we neither interdicted the attackers nor responded effectively after the attack.

The primary cause of these three component failures was the lack of integration, not only among the triad components that would have produced the necessary synergy to have prevented the attack, but a similar lack of integration of other, non-federal, levels of government, non-law enforcement disciplines and other key stakeholders.

Consequently, our nation should adopt a new view of what should constitute the appropriate framework for an "intelligence community," and we have to have a corresponding change in how we perceive "national intelligence." This sea change in perception and organization is captured in the new National Intelligence Strategy (NIS) signed by President Bush in October 2005.[192] The Strategy recognizes that national intelligence must be reworked to meet the needs of the 21st Century. Towards that end, the Strategy calls for a unified enterprise of intelligence professionals that work in a collaborative manner. It emphasizes the need for an integrated intelligence capacity that creates "an information sharing environment in which access to terrorism information is matched to the roles, responsibilities, and missions of all organizations engaged in countering terrorism, and is timely, accessible, and relevant to their needs." Finally, the NIS calls for the elimination of redundant programs and programs that bring little added value to national security.

The current policy of promoting fusion centers and participation in Joint Terrorism Task Forces increases information sharing and integration; however, to the extent that we only fuse information or only the efforts of law enforcement, it is only a partial solution. This partial solution does not address the significant gaps that remain in our regional and national terrorism prevention and response capabilities.

Our domestic counterterrorism efforts also remain hampered by the lack of an effective **National Counterterrorism Network** that fully integrates the Homeland's entire intelligence assets and capabilities into one national counterterrorism system. A national network is needed to eliminate the proliferation of well intentioned, but stove-piped intelligence and Homeland Security entities. The failure to fully unify our domestic counterterrorism efforts is thwarting the creation of an efficient and effective national intelligence cycle, from identification of intelligence needs, to collection, to analysis and

[192] *The National Intelligence Strategy of the United States of America.*

finally dissemination. This omission also severely limits our ability to take action to either prevent or more effectively respond to attacks and natural disasters. In summary, to the extent that our evolutionary processes stops at coordination and cooperation, but does not evolve to collaboration, we will not achieve the synergistic benefits of a more holistic organism.

The most promising and effective solution to minimize gaps in our ability to protect the Homeland is to create a truly *national* network of key counterterrorism resources. This **National Counterterrorism Network** should unite Regional and Super-Regional All-Hazard, Disaster and Anti-terrorism Resource (**RADAR**) centers under the auspices of the existing National Counterterrorism Center for terrorism issues and the National Operations Center for "all-hazards" issues.

These regionally designed, but nationally networked and "accredited" **RADAR** centers would combine existing state, local, tribal and federal law enforcement intelligence, investigative and operational assets, along with the resources of key non-law enforcement government agencies and private sector groups, and the public, into one unified system dealing with "all-hazards" and "all-crimes" with national security implications. The resulting national network will not only minimize information sharing barriers, but will also ensure the most efficient and effective use of intelligence, investigative and operational resources.

By being multi-disciplinary and multi-agency, these same resources would be able to collaborate to deal with not only deliberate, but also natural disasters as well. Because the proper partners for defeating terrorism are the same as those for dealing with other more common hazards, these "all-hazards" centers would achieve unparalleled efficiency in resource utilization and coordination, as well as information sharing.

Finally, this collaborative effort must operate in a constitutionally sound manner that will promote the intertwining goals of public safety and civil liberties. Erosion of privacy and civil liberties is not solely the concern of the extreme left or extreme right; respected groups and individuals across the political spectrum have espoused this concern. The debate has unfortunately all too often be framed as an "either/or" issue when these twin goals are not mutually exclusive. Creation of a **National**

Counterterrorism Network of **RADAR** centers that operate with reasonable transparency and oversight will earn public trust and support, and preserve liberty from both external and internal threats.

LIST OF REFERENCES

2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships. Washington, DC: National Governors Association, Center for Best Practices, April 3, 2006. http://www.nga.org/Files/pdf/0604HLSDIRSURVEY.pdf (accessed November 1, 2006).

"About the National Counterterrorism Center." National Counterterrorism Center. http://www.nctc.gov/about_us/about_nctc.html (accessed January 7, 2007).

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (U.S.). *Forging America's New Normalcy: Securing our Homeland, Protecting our Liberty: Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, http://purl.access.gpo.gov/GPO/LPS41265 (accessed March 7, 2007).

Allen, George. "Terrorist Attacks Against the United States." *Congressional Record* 147, no. 118 (September 12, 2001): S9289.

Altman, Lawrence K. and Gina Kolata. "Anthrax Missteps Offer Guide to Fight Next Bioterror Battle." *New York Times,* January 6, 2002, sec. 1.

Angle, Jim et al. "MI5-Style Intel Agency could be Hard Sell in U.S." *Fox News,* April 21, 2004. http://www.foxnews.com/story/0,2933,117677,00.html (accessed January 5, 2007).

Baird, Zoë E., James Barkdale, and Michael A. Vatis. *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*. New York, NY: Markle Foundation, 2003. http://www.markletaskforce.org/Report2FullReport.pdf (accessed March 7, 2007).

Best, Richard A., Jr. *The Intelligence Community and 9/11: Congressional Hearings and the Status of Investigation.* Washington, DC: Library of Congress, Congressional Research Service, January 16, 2003.

Blockin, Martha and Gerald Murphy. *Protecting Your Communities from Terrorism, Strategies for Local Law Enforcement Series*. Washington, DC: Police Executive Research Forum, 2003-2005, http://www.cops.usdoj.gov/Default.asp?Item=118 (accessed March 7, 2007).

Blum, Rick. *Secrecy Report Card 2005, Quantitative Indicators of Secrecy in the Federal Government: A Report by OpenTheGovernment.Org*. Washington DC: Americans for Less Secrecy, More Democracy, 2005, http://www.openthegovernment.org/otg/SRC2005.pdf (accessed December 2, 2006).

Boo, Katherine. "How Congress Won the War in the Gulf." *Washington Monthly,* 23, no. 10 (October 1991), 31.

Broder, John M. "Police Chiefs Moving to Share Terror Data." *New York Times,* July 29, 2005, Sec. A.

"Budget Crunch Forces Pinch in Cops' Anti-Terror Unit, Some Members Being Reassigned." *Philadelphia Daily News,* December 29, 2004.

Bush, George W. "Classified National Security Information," Executive Order 12958, April 17, 1995.

_____. *Critical Infrastructure, Identification, Prioritization, and Protection*, Homeland Security Presidential Directive (HSPD): 7. Washington, DC: The White House, December 17, 2003. Available at http://knxup2.hsdl.org/homesec/docs/dhs/HSPD7.pdf (accessed March 7, 2007).

_____. "Further Amendment to Executive Order 12958, as Amended, Classified National Security System" Executive Order 13292, March 25, 2003.

_____. *Management of Domestic Incidents*, Homeland Security Presidential Directive (HSPD): 5. Washington DC: The White House, February 2003. Available at http://knxup2.hsdl.org/homesec/docs/dhs/HSPD5.pdf (accessed March 7, 2007).

_____. "National Counterterrorism Center." Executive Order 13354, August 27, 2004.

_____. *National Preparedness,* Homeland Security Presidential Directive (HSPD): 8. Washington, DC: The White House, December 17, 2003. Available at https://www.hsdl.org/homesec/docs/dhs/HSPD8.pdf (accessed March 7, 2007).

_____. *President Speaks at FBI on New Terrorist Threat Integration Center*. Washington, DC: White House, February 14, 2003. http://www.whitehouse.gov/news/releases/2003/02/20030214-5.html (accessed January 17, 2007).

_____. "Strengthening the Sharing of Terrorism Information to Protect Americans." Executive Order 13356, August 27, 2004.

_____. "United States Intelligence Activities" Executive Order 12333, December 4, 1981.

Carter, David L. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. Washington, DC: Department of Justice, Office of Community Oriented Policing Services, November 2004. http://www.cops.usdoj.gov/mime/open.pdf?Item=1439 (accessed February 2, 2007).

Chertoff, Michael. *Remarks by the Secretary of Homeland Security Michael Chertoff 2006 Bureau of Justice Assistance, U.S. Department of Justice and SEARCH Symposium on Justice and Public Safety Information Sharing*, http://www.dhs.gov/xnews/speeches/speech_0273.shtm (accessed March 7, 2007).

Commission on Roles and Capabilities of the United States Intelligence Community. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. Washington, DC: GPO, 1996. http://www.access.gpo.gov/int/report.html (accessed March 7, 2007).

Criminal Terrorism Enforcement in the United States during the Five Years Since the 9/11/01 Attacks. New York: Syracuse University, Transactional Records Access Clearinghouse (TRAC). http://trac.syr.edu/tracreports/terrorism/169/ (accessed March 7, 2007).

Department of Justice. Office of Inspector General. *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information*. DOJ IG Report No. 04-10, Washington, DC: Department of Justice, Office of Inspector General, December 2003. http://www.usdoj.gov/oig/reports/FBI/a0410/final.pdf (accessed March 7, 2007).

DeYoung, Karen. "A Fight Against Terrorism—and Disorganization." *Washington Post,* August 9, 2006.

Downs, Anthony. *Political Theory and Public Choice*. Northampton, MA: Edward Elgar, 1998.

"Earnest James Ujaama Sentenced for Conspiring to Supply Goods and Services to the Taliban." Department of Justice Press Release, February 13, 2004. http://www.usdoj.gov/opa/pr/2004/February/04_crm_086.htm (accessed March 7, 2007).

Eggen, Dan. "Terrorism Prosecutions Drop; Analysis Show a Spike After 9/11, Then a Steady Decline." *Washington Post,* September 4, 2006, Sec. A, http://www.washingtonpost.com/wp-dyn/content/article/2006/09/03/AR2006090300768.html (accessed February 28, 2007).

"FBI and DOJ Response to TRAC Report [Press Release]." Department of Justice, Federal Bureau of Investigation. http://www.fbi.gov/pressrel/pressrel06/trac110306.htm (accessed March 7, 2007).

Finley, Bruce. "Intelligence Fixes Floated at Conference." *Denver Post,* August 22, 2006.

Flynn, Stephen E. and Daniel B. Prieto. *Neglected Defense, Mobilizing the Private Sector to Support Homeland Security*. CSR No. 13. Washington, DC: Council on Foreign Relations, May 2006. http://www.cfr.org/content/publications/attachments/NeglectedDefenseCSR.pdf (accessed March 7, 2007).

"*A Functional Model for Critical Infrastructure Information Sharing and Analysis: Maturing and Expanding Efforts*." Information Sharing and Analysis Centers Council. ISAC Council White Paper). http://www.isaccouncil.org/pub/Information_Sharing_and_Analysis_013104.pdf (accessed January 7, 2007).

Hocevar, Susan, Erik Jansen, and Gail Fann Thomas. *Building Collaborative Capacity for Homeland Security*. Monterey, CA: Naval Postgraduate School, 2006. http://bosun.nps.edu/uhtbin/hyperion.exe/NPS-GSBPP-04-008.pdf (accessed December 14, 2006).

"Intelligence Agencies Face Staff Shortage." *USA Today*, December 27, 2004.

Intelligence Reform and Terrorism Prevention Act of 2004. PL 108-458, December 17, 2004.

International Association of Chiefs of Police. *From Hometown Security to Homeland Security: IACP's Principles for a Locally Designated and Nationally Coordinated Homeland Security Strategy*. Washington, DC: International Association of Chiefs of Police, 2005. http://www.theiacp.org/leg_policy/HomelandSecurityWP.PDF (accessed March 7, 2007).

Kaplan, David E. "When the Cops Saw Only Red." *U.S. News and World Report,* May 8, 2006. 48.

Kelly, Raymond. "A Report from the Front." *New York Daily News,* September 10, 2006.

Law Enforcement Statistics, 2000. Washington, DC: Bureau of Justice Statistics. http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed October 24, 2006).

LEAP: A Law Enforcement Assistance and Partnership Strategy Improving Information Sharing between the Intelligence Community and State, Local and Tribal Law Enforcement. Washington, DC: House, Select Committee on Homeland Security. Democratic Office, 2006. http://www.fas.org/irp/congress/2006_rpt/leap.pdf (accessed March 7, 2007).

Lipowicz, Alice. "JRIES Homeland Security Network Falls Victim to Policy Dispute." *Government Computer News,* October 6, 2005. http://www.gcn.com/online/vol1_no1/37223-1.html (accessed February 3, 2007).

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 3rd ed. Washington, DC: CQ Press, 2006.

———. *Intelligence: From Secrets to Policy*. 2nd ed. Washington, DC: CQ Press, 2003.

Marks, Alexandra. "After a Surge, US Terror Prosecutions Drop to Pre-9/11 Levels." *Christian Science Monitor,* September 5, 2006. http://www.csmonitor.com/2006/0905/p01s04-usju.html (accessed February 28, 2007).

Mattessich, Paul W., Marta Murray-Close, and Barbara R. Monsey. *Collaboration: What Makes it Work*. 2nd ed. St. Paul, MN: Fieldstone Alliance, 2001.

Morabito, Andrew and Sheldon Greenberg. *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Washington, DC: Bureau of Justice Assistance, 2005. http://www.ncjrs.gov/pdffiles1/bja/210678.pdf (accessed December 14, 2006).

National Commission on Terrorist Attacks upon the United States. "Final Report on 9/11 Commission Recommendations December 5, 2005." http://www.9-11pdp.org/press/2005-12-05%5Freport.pdf (accessed March 7, 2007).

———. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. 1st ed. New York: Norton, 2004.

National Native American Law Enforcement Association. *Tribal Lands Homeland Security Report. 10th Annual Training Conference, October 22-24, 2002*. Washington, DC: National Native American Law Enforcement Association, 2002, http://www.nnalea.org/hlsecurity/summitreport.pdf (accessed December 14, 2006).

National Preparedness. Homeland Security Presidential Directive, HSPD-8. Washington, DC: December 17, 2003.

National TEW Resource Center. *Resource Guide: Book One: TEW Concept and Overview*. Los Angeles, CA: National TEW Resource Center, 2005? http://www.ojp.usdoj.gov/odp/docs/ResourceBook1_TEW.pdf (accessed March 7, 2007).

O'Hanlon, Michael. *The Role of State and Local Governments in Homeland Security: Written Testimony for the Senate Committee on Homeland Security and Governmental Affairs.* Washington, DC: Brookings Institution, July 14, 2005. http://www.brookings.edu/views/testimony/ohanlon/20050714.pdf (accessed December 2, 2006).

Ovalle, David, et al. "False Alarm Tests Miami Port's Security." *Miami Herald,* January 7, 2007. http://www.miami.com/mld/miamiherald/news/local/16406515.htm (accessed March 7, 2007).

Palmieri, Lisa M. *Information vs. Intelligence: What Police Executives Need to Know* IACP Annual Meeting, 2005.

Perrow, Charles. "The Disaster After 9/11: The Department of Homeland Security and the Intelligence Reorganization." *Homeland Security Affairs* II, no. 1 (April 2006) http://www.hsaj.org/?article=2.1.3 (accessed March 7, 2007).

Posner, Richard A. *Remaking Domestic Intelligence*. Stanford, CA: Hoover Institution Press, 2005.

Program Manager, Information Sharing Environment. *Information Sharing Environment Implementation Plan*. Washington, DC: Office of the Director of National Intelligence, November 2006. http://www.ise.gov/docs/ise-impplan-200611.pdf (accessed December 12, 2006).

Reaves, Brian A. and Matthew J. Hickman. *Census of State and Local Law Enforcement Agencies, 2000*. Washington, DC: U.S. Dept. of Justice, Office of Justice Programs, 1998, http://www.ojp.usdoj.gov/bjs/pub/pdf/csllea00.pdf (accessed December 14, 2006).

Recommended Fusion Center Standards: Developing and Sharing Intelligence in a New World: Executive Summary. Washington, DC: Department of Justice, Bureau of Justice Assistance, June 2005. http://it.ojp.gov/documents/Fusion_Center_Executive_Summary.pdf (accessed March 7, 2007).

Riley, Kevin Jack. *State and Local Intelligence in the War on Terrorism*. Santa Monica, CA: RAND Corporation, 2005, www.rand.org/pubs/monographs/2005/RAND_MG394.pdf (accessed March 7, 2007).

Rudman, Warren B., Richard A. Clarke, and Jamie F. Metzl. *Emergency Responders: Drastically Under Funded, Dangerously Unprepared: Report of an Independent Task Force*. New York, NY: Council on Foreign Relations, 2003, http://www.cfr.org/content/publications/attachments/Responders_TF.pdf (accessed November 14, 2006).

Schlosberg, Mark. *The State of Surveillance: Government Monitoring of Political Activity in Northern & Central California*. California: ACLU of Northern California, 2006, http://www.aclunc.org/issues/government_surveillance/asset_upload_file714_3255.pdf (accessed March 7, 2007).

Schmidt, Robert. "Terrorism Fighters May Focus on Fed as Model for Sharing Data." *Bloomberg News,* September 7, 2006, http://www.bloomberg.com/apps/news?pid=20601087&sid=a9p3U5a.EBLA&refer=home (accessed December 14, 2006).

Schrage, Michael. *Shared Minds: The New Technologies of Collaboration*. New York, NY: Random House, 1990.

Schulhofer, Stephen J. *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11*. Washington, DC: Century Foundation Press, 2002.

Sheridan, Mary Beth and Spencer C. Hsu. "Localities Operate Intelligence Centers to Pool Terror Data." *Washington Post,* December 31, 2006, Sec. A.

Smuts, Jan Christiaan. *Holism and Evolution*. New York: Macmillan Co., 1926.

Sniffen, Michael J. "Number of Terror Cases Dwindles: Prosecutions Sink to Level Before." *Chicago Sun-Times,* September 4, 2006. http://www.findarticles.com/p/articles/mi_qn4155/is_20060904/ai_n16708084 (accessed February 28, 2007).

State Intelligence Fusion Centers: Recent State Actions. Washington, DC: National Governors Association, Center for Best Practices, July 7, 2005. http://www.nga.org/files/pdf/0509fusion.pdf (accessed March 7, 2007).

Stevenson, William. *A Man Called Intrepid: The Secret War*. New York: Harcourt Brace Jovanovich, 1976.

"Today's FBI: Changing to Meet Evolving Threats." Federal Bureau of Investigation. http://www.fbi.gov/aboutus/transformation/overview.htm (accessed November 30, 2006).

Twain, Mark. *Mark Twain's Autobiography*. New York: Harper and Bros, 1924.

United States. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*, http://purl.access.gpo.gov/GPO/LPS59410 (accessed March 7, 2007).

United States. Congress. House. Committee on Homeland Security Democratic Staff. *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information*. Washington, DC: U.S. House Committee on Homeland Security Democratic Staff, 2005. https://www.hsdl.org/homesec/docs/intel/nps23-010906-01.pdf (accessed March 7, 2007).

United States. Congress. Senate. Committee on Governmental Affairs. *State and Local Officials: Still Kept in the Dark about Homeland Security.* S. Prt. 108-33. Washington, DC: GPO, 2003. http://hsgac.senate.gov/_files/sprt10833min_hs_statelocal.pdf (accessed March 7, 2007).

United States. Congress. Senate. Select Committee on Intelligence. *Intelligence Authorization Act for Fiscal Year 2006: Report (to Accompany S. 1803)*. S. Rpt. 109-142. Washington, DC: GPO, 2005. http://purl.access.gpo.gov/GPO/LPS65452 (accessed March 7, 2007).

United States. Congress. Senate. Select Committee on Intelligence and United States. Congress. House. Permanent Select Committee on Intelligence. *Joint Inquiry Staff Statement. Part I*. Washington, DC: United States Senate Select Committee on Intelligence, 2002, http://purl.access.gpo.gov/GPO/LPS37136 (accessed March 7, 2007).

United States. Department of Justice. "Waging the War on Terror [Preserving Life & Liberty Anti-Terror Record]." http://www.lifeandliberty.gov/subs/a_terr.htm (accessed January 13, 2007).

United States. Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: Department of Justice, Global Justice Information Sharing Initiative, August 2006. http://it.ojp.gov/documents/fusion_center_guidelines.pdf (accessed March 7, 2007).

———. *The National Criminal Intelligence Sharing Plan*. Washington, DC: Department of Justice, Bureau of Justice Assistance, October 2003. http://www.iir.com/global/products/NCISP_Plan.pdf (accessed January 19, 2007).

United States. Department of Justice. Counterterrorism Section. *Counterterrorism White Paper*. [Washington, DC]: [Department of Justice], June 22, 2006. https://www.hsdl.org/homesec/docs/justice/nps03-010807-03.pdf (accessed March 7, 2007).

United States. Department of Justice. Federal Bureau of Investigation. *Report to the Commission on Terrorist Attacks upon the United States: The FBI's Counterterrorism Program*. Washington, DC: Federal Bureau of Investigation, April 14, 2004. http://www.fbi.gov/publications/commission/9-11commissionrep.pdf (accessed November 20, 2006).

United States. Government Accountability Office. *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*. Washington, DC: GAO, March 2006. http://www.gao.gov/new.items/d06385.pdf (accessed February 28, 2007).

United States. Office of Homeland Security. *National Strategy for Homeland Security*. Washington, DC: Office of Homeland Security, July 2002. http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (accessed December 14, 2004).

United States. Office of the Director of National Intelligence. *Declassified Key Judgments of the National Intelligence Estimate "Trends in Global Terrorism--Implications for the United States*." Washington, DC: Office of the Director of National Intelligence, 2006. http://www.dni.gov/press_releases/Declassified_NIE_Key_Judgments.pdf (accessed March 7, 2007).

———. *The National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*. Washington, DC: Office of the Director of National Intelligence, 2005. http://www.dni.gov/publications/NISOctober2005.pdf (accessed March 7, 2007).

United States. President (2001- : Bush). *The National Security Strategy of the United States of America*. Washington, DC: White House, 2006. http://purl.access.gpo.gov/GPO/LPS67777 (accessed March 7, 2007).

United States. White House. *National Strategy for Homeland Security*. Washington, DC: Executive Office of the President, 2002. http://purl.access.gpo.gov/GPO/LPS20641 (accessed March 7, 2007).

Zetter, Kim. "ACLU Chief Assails Patriot Spin." *Wired News,* September 23, 2003, http://www.wired.com/news/conflict/0,60541-0.html?tw=wn_story_page_prev2 (accessed December 12, 2006).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Captain Robert Simeral
   Naval Postgraduate School
   Monterey, California

4. Doctor Chris Bellavita
   Naval Postgraduate School
   Monterey, California

5. Assistant Chief Jim Pryor
   Seattle Police Department
   Seattle, Washington

6. Captain Mike Sanford
   Seattle Police Department
   Seattle, Washington