



NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

**EXPOSING THE SEAMS: THE IMPETUS FOR
REFORMING U.S. COUNTERINTELLIGENCE**

by

Todd E. Gleghorn

September 2003

Thesis Advisor:
Second Reader:

David Tucker
James Russell

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>
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 September 2003	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Exposing the Seams: the Impetus for Reforming U.S. Counterintelligence			5. FUNDING NUMBERS
6. AUTHOR(S) LT Todd E. Gleghorn			8. PERFORMING ORGANIZATION REPORT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			10. SPONSORING/MONITORING AGENCY REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited			12b. DISTRIBUTION CODE
13. ABSTRACT (maximum 200 words) U.S. counterintelligence is in need of reform. The September 11, 2001 attacks by <i>Al-Qa'ida</i> against America highlight this fact but are not in themselves the reason counterintelligence should be reformed. Not surprisingly these attacks have stirred a general debate on how U.S. intelligence ought to be reformed to more adequately protect the nation. However, amidst these various discussions one aspect of American intelligence capabilities seems to be conspicuously absent: counterintelligence. A review of counterintelligence functions and organization reveals that U.S. counterintelligence must be reformed organizationally. The current counterintelligence community structure hinders the effective employment of this crucial intelligence capability. In order to resolve this problem the author proposes a threefold approach to that reform: (1) Centralize U.S. counterintelligence operations under a single agency that will have the authority to conduct both domestic and foreign operations, (2) leave the remaining offices of counterintelligence located throughout the federal government in place to provide investigative and analytical support to the central operations agency, and (3) devolve U.S. counterintelligence down to the state and local levels along with encouraging greater private sector participation in order to provide wider coverage of the threat that both spies and terrorists pose to U.S. national security.			
14. SUBJECT TERMS Counterintelligence; Intelligence; Intelligence Reform; Espionage; Spies, Spying; Counterespionage; Foreign Intelligence Services; Double Agents; Moles; Terrorism; Counterterrorism; September 11; 9/11; Terrorists.			15. NUMBER OF PAGES 107
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

**EXPOSING THE SEAMS: THE IMPETUS FOR REFORMING U.S.
COUNTERINTELLIGENCE**

Todd E. Gleghorn
Lieutenant, United States Navy
B.A., University of Utah, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the

**NAVAL POSTGRADUATE SCHOOL
September 2003**

Author: Todd E. Gleghorn

Approved by: David C. Tucker
Thesis Advisor

James Russell
Second Reader

James Wirtz
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

U.S. counterintelligence is in need of reform. The September 11, 2001 attacks by *Al-Qa'ida* against America highlight this fact but are not in themselves the reason counterintelligence should be reformed. Not surprisingly these attacks have stirred a general debate on how U.S. intelligence ought to be reformed to more adequately protect the nation. However, amidst these various discussions one aspect of American intelligence capabilities seems to be conspicuously absent: counterintelligence. A review of counterintelligence functions and organization reveals that U.S. counterintelligence must be reformed organizationally.

The current counterintelligence community structure hinders the effective employment of this crucial intelligence capability. In order to resolve this problem the author proposes a threefold approach to that reform: (1) Centralize U.S. counterintelligence operations under a single agency that will have the authority to conduct both domestic and foreign operations, (2) leave the remaining offices of counterintelligence located throughout the federal government in place to provide investigative and analytical support to the central operations agency, and (3) devolve U.S. counterintelligence down to the state and local levels, along with encouraging greater private sector participation in order to provide wider coverage of the threat that both spies and terrorists pose to U.S. national security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

- I. THE IMPETUS FOR REFORMING COUNTERINTELLIGENCE1
 - A. INTRODUCTION.....1
 - B. OUTLINING THE THREAT ENVIRONMENT3
 - C. THE ROLE OF COUNTERINTELLIGENCE6
 - D. THE IMPETUS FOR REFORMING COUNTERINTELLIGENCE12
 - E. COUNTERINTELLIGENCE REFORM: THE WAY AHEAD15
- II. COUNTERINTELLIGENCE DELINEATED19
 - A. INTRODUCTION.....19
 - B. THE FUNCTIONS OF COUNTERINTELLIGENCE19
 - C. THE CORE COMPETENCIES21
 - 1. Identifying and Assessing the Threat.....21
 - 2. Neutralization and Exploitation23
 - a. *Neutralization Operations*.....23
 - b. *Exploitation Operations*.....26
 - D. THE TIMELESS NATURE OF COUNTERINTELLIGENCE FUNCTIONS31
 - E. COUNTERINTELLIGENCE RESPONSIBILITIES IN THE POST-SEPTEMBER 11 ERA34
- III. THE COUNTERINTELLIGENCE COMMUNITY.....43
 - A. INTRODUCTION.....43
 - B. CI OPERATIONS REQUIRE CENTRALIZATION45
 - C. THE KEY PLAYERS & SUPPORT ORGANIZATIONS47
 - 1. The Five Key Players47
 - 2. CI Support Organizations.....48
 - D. OUTLINING THE COMMUNITYSTRUCTURE.....52
 - 1. Overall Decentralization55
 - 2. Centralized Executive Structure56
 - E. HIGHLIGHTING THE FLAWS IN DESIGN.....57
 - 1. The Foreign-Domestic Divide59
 - 2. Unnecessary Overlap62
 - a. *Combining Law Enforcement & Counterintelligence*.....63
 - b. *Multiplicity of Organizations*.....64
 - F. FINAL ASSESSMENT: COUNTER-INTELLIGENT STRUCTURE67
- IV. COUNTERINTELLIGENCE REFORM: THE WAY AHEAD69
 - A. INTRODUCTION.....69
 - B. ORGANIZATIONAL REFORM69
 - 1. Centralized Operations, Distributed Support70
 - 2. Centralized CI Reporting78
 - 3. The Devolved Counterintelligence Community81
 - a. *State and Local Counterintelligence Offices*82
 - b. *Encouraging Private Sector Participation*83

c.	<i>The LA TEW as a model for devolving U.S. Counterintelligence</i>	83
D.	CONCLUSION	84
1.	Potential Problems & Benefits in Devolving U.S. Counterintelligence	84
2.	Concluding Remarks	86
	LIST OF REFERENCES	87
	INITIAL DISTRIBUTION LIST	93

LIST OF FIGURES

Figure 1.	Major Components of U.S. CI Community.....	53
Figure 2.	Executive U.S. CI Organization [PDD-75].....	54
Figure 3.	Structural Divide and Operational Overlap in CI Organizations.....	58

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to first of all thank my wife, Paola, not only for all the patience and understanding she showed as I wrote this thesis, but also for the constant reminder to stay focused and to be brief. Secondly, I would like to thank Professor David Tucker for his countless hours in editing my chapters. Throughout this process he has challenged my thinking, my arguments and my assumptions and in so doing, has truly helped refine and hone my writing skills like no one else. Thirdly, I would like to thank the numerous counterintelligence professionals whose contributions to this thesis were invaluable. The various discussions I had with Mark Faber, Chuck St. Pierre, and Rocco Rosano, to name just a few individuals, enlightened my understanding of the arcane and convoluted world of counterintelligence and have helped shaped my approach to the reforms and proposals contained in this thesis. And lastly, I dedicate this work to my father, who although he never seemed to understand my fascination with the world of intelligence, has nonetheless spurred me on towards greater heights of achievement in all my endeavors.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE IMPETUS TO REFORM COUNTERINTELLIGENCE

A. INTRODUCTION

In the wake of numerous intelligence failures witnessed by the United States over the past couple of decades – from the discovery of spies in the CIA’s clandestine service and among FBI counterintelligence officers, to the attacks on the World Trade Center and Pentagon in September 2001 – the Intelligence Community (IC) has not surprisingly come under a great deal of scrutiny. Central to the ongoing debate concerning intelligence and the community itself is the apparent inability of this labyrinth federation, nominally made up of 15 separate agencies¹, to prevent these failures from occurring. Accordingly, the discussion has involved various aspects of intelligence and its associated processes that range from issues of information sharing and intelligence fusion, to the under-utilization of human intelligence that appears to have been supplanted by an over-reliance on technical collection means to gather intelligence. However, despite the general breadth the debate on intelligence reform has encompassed, one vital intelligence discipline conspicuously seems to have been under-evaluated: counterintelligence.

While many recent works highlight these aforementioned intelligence failures along with their potential causes, few works analyze how counterintelligence may have contributed to these failures. Unfortunately, the lack of discussion to determine what role, if any, U.S. counterintelligence played in these failures is in spite of the fact that counterintelligence is one of the four cornerstones of U.S. intelligence.² The U.S. Intelligence Community is generally recognized as being organized around four essential elements that include collection, analysis, covert action and counterintelligence.³ In the aftermath of September 11, 2001, much debate surrounding America’s deficiencies in intelligence has occurred. The 9/11-intelligence debate has mainly focused on issues of

¹ *United States Intelligence Community*. Available [online]: <http://www.intelligence.gov/1-definition.shtml> [22 April 2003]. The recently created website provides an extensive overview of the U.S. Intelligence Community outlining each of the constituent agencies and their roles.

² Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*. (New Brunswick and London: Transaction Publishers, 2003), 1 [hereafter referred to as: Godson, *Dirty Tricks or Trump Cards*, pp.#].

³ *Ibid.*

collection and analysis, with a lesser focus being given to covert action. Counterintelligence, on the other hand, has been nearly absent from this debate altogether.

One reason that counterintelligence has been overlooked in these discussions is the nature of counterintelligence itself. Counterintelligence has been called the most arcane and least understood of all the intelligence disciplines.⁴ One must also bear in mind that this lack of understanding concerning counterintelligence does not refer to the general populace but refers specifically to many people within the U.S. government (USG) and IC itself; people who may rightly be perceived as having a responsibility to know the intricacies of this clandestine art, but people who are nonetheless ignorant in this regard. However, given the extremely sensitive nature of counterintelligence operations – counterintelligence sources and methods are some of the most closely guarded U.S. secrets – it should not be surprising to find so little discussed about it and so few people acquainted with this arcane discipline.⁵ So, despite a seemingly conspicuous dearth of dialogue concerning U.S. counterintelligence in the wake of September 11, this paucity is most assuredly an old and continuing phenomenon.

Therefore it seems appropriate to review and analyze U.S. counterintelligence, particularly in light of the continuing public debate on U.S. intelligence practices that have largely left counterintelligence alone. Regardless of how damaging the attacks of September 11 or the discovery of moles within the IC have been on U.S. security, these should not be construed as constituting the fundamental precedent for assessing U.S. counterintelligence effectiveness. Rather, the precedent for analyzing U.S. counterintelligence is long overdue and predicated on a checkered history of effectiveness that will be discussed in more detail later.⁶ Although counterintelligence is a relatively infrequent subject of debate concerning intelligence reform, it has not been

⁴ Godson, *Dirty Tricks or Trump Cards*, 6; William E. Odom, *Fixing Intelligence: For a More Secure America*. (New Haven, CT: Yale University Press, 2003), 167.

⁵ Due to the nature of classification and compartmentalization of counterintelligence practices even most intelligence analysts, unless they are working directly in this field and have a specific “need-to-know”, are kept ignorant of a majority of counterintelligence operations to protect these very perishable sources and methods.

⁶ The modern history of U.S. counterintelligence, which begins in the years just preceding World War II, serves as the point from which the current U.S. counterintelligence community takes its structure and from which the present day dynamics finds their origins.

forgotten. However, what little discussion has concerned this misunderstood art has been piecemeal at best and at worst has failed to effect changes necessary to rectify its deficiencies.

Before beginning the analysis of U.S. counterintelligence a brief discussion of the current threat environment is necessary. Once this environment has been outlined, the analysis will begin by defining counterintelligence and describing its role as a unique discipline of U.S. intelligence. Then the following section will highlight key problems of counterintelligence that constitute the impetus for reforming this oft overlooked and essential discipline. The chapter will conclude by identifying some measures for reforming counterintelligence in order to fix its long-standing problems.

B. OUTLINING THE THREAT ENVIRONMENT

The threat environment that the U.S. faces at the beginning of the 21st Century is dynamic and demarcated by a range of intelligence- and security-related threats. These threats, both foreign and domestic, emanate from a variety of state and non-state actors whose actions can generally be characterized as hostile, subversive, or otherwise inimical to U.S. security interests. A myriad of terms describe the threat that these actors pose to U.S. security interests, which include but are not necessarily limited to: terrorism, espionage, subversion, sedition, sabotage, and assassinations. This threat environment, although it has been described as emergent – and this seems to be an appropriate characterization given the dynamics of the actors involved – does not present a substantively new challenge to U.S. counterintelligence.

Initially this observation seems to contradict the conclusions of research into conflict that indicate that the threat environment today has changed from the recent past. This research is encapsulated in a variety of theories that all build upon one another. Most of these theories suggest the world is now in a new era of conflict, which some call the *fourth generation of warfare*,⁷ one that is steadily moving away from distinctly interstate conflict to a more inclusive conflict paradigm involving non-state actors.⁸ Whether or not

⁷ William Lind, et al., "The Changing Face of War: Into the Fourth Generation," *Military Gazette*, October 1989.

⁸ For further study on these concepts refer to the following list of representative works. Fourth Epochal Warfare: see Robert J. Bunker, ed., *Non-State Threats and Future Wars*. (London and Portland: Frank Cass & Company, 2003); Non-Trinitarian Warfare: see Martin Van Creveld, *The Transformation of*

one agrees that this phenomenon is new, there is nonetheless evidence to suggest that globalization and the information revolution, especially as a result of the proliferation of the internet and other advanced communication technologies, has aided the efforts of various hostile non-state actors to organize into networks.⁹ These theories certainly merit consideration in order to assess the potential impact these hostile non-actors may have on U.S. security both now and in the future.

This may come as a surprise, but the bottom line assessment is that this emergent threat paradigm does not significantly impact U.S. counterintelligence. This does not mean that these theories of conflict are invalid; rather it demonstrates the relative insignificance of these forms of conflict with respect to U.S. counterintelligence practices. The theory known as *netwar* in particular provides a cogent example of this insignificance. *Netwar*, among other things, highlights the advantages that some non-state organizations have over more centralized and hierarchical organizations (mainly nation-states) as a result of their network structure.¹⁰ However, network organizations hold no distinct advantage over counterintelligence organizations as the methods employed and the operations conducted by counterintelligence remain the same regardless of the adversary's organizational form. Thus, whether the organizations that pose a threat to the U.S. are networked, hierarchical or some hybrid form, and regardless of whether they are state or non-state entities, the task at hand for counterintelligence does not change.

To better understand why counterintelligence does not necessarily need to change in light of an emerging threat paradigm, a more thorough discussion of the current threat environment is warranted. For one reason, the threat environment has not changed enough over the years, from the end of World War II until the present, to warrant discarding the tried-and-true practice of countering state-based foreign intelligence service activity targeting the U.S. There are plenty of examples to draw upon, but one recent case is especially appalling. The case of former FBI counterintelligence officer,

War. (New York: Simon & Schuster, 1991); Asymmetric Warfare: see Colin S. Gray "Thinking Asymmetrically in Times of Terror," *Parameters*. Spring 2002, pp 5-14; Netwar: see John Arquilla and David Ronfeldt, eds. *The Advent of Netwar*. (Santa Monica and Washington, DC: RAND, 1996).

⁹ For a particularly cogent discussion of one of these theories see: John Arquilla and David Ronfeldt, eds. *In Athenas' Camp: Preparing for conflict in the Information Age*. (Santa Monica and Washington, DC: RAND, 1997), 27-29.

¹⁰ John Arquilla and David Ronfeldt, eds. *Networks and Netwars: The Future of Terror, Crime and Militancy*. (Santa Monica and Washington, DC: RAND, 2001).

James J. Smith being duped by his long-time Chinese informant and lover, Katrina Leung, who was actually working as a double agent for the Beijing government, demonstrates that thwarting state-based espionage needs to continue.¹¹ Although traditional espionage of this type has not changed over the years, the threat environment has fundamentally changed in at least a few ways. One noticeable change is that state-based foreign intelligence services are no longer the sole players in the world of espionage. Foreign and domestic corporations as well as individuals who do not have ties to nation-states are also increasingly involved in illicit attempts to acquire sensitive U.S. information and technologies.¹² Another change to this threat environment, at least in terms of economic and industrial espionage, is that America's most sensitive military technologies and other closely guarded secrets, the so-called "crown jewels", no longer seem to be the target of choice for hostile intelligence collectors.¹³ Although this threat is not new per se, economic espionage was not recognized as a serious threat to U.S. national security until the 1980's.¹⁴ In fact, until 1996 no U.S. law existed that specifically outlined the threat or responsibilities of the counterintelligence community to counter either economic or industrial espionage activities being directed against the USG or private sector corporations.¹⁵ Interestingly these two changes appear to converge on another recent trend: economic espionage is not solely or primarily a security issue stemming from the hostile activities of "rogue states" or traditional foes, it is a problem of exploitation by "friends" and allies who utilize their relationships with U.S. companies, organizations or research institutes as a way to collect intelligence.¹⁶ This is

¹¹ U.S. Federal Bureau of Investigations, *Affidavit - Katrina Leung*. (Washington, D.C.: GPO, 2003) [hereafter referred to *Leung Affidavit*]; and Eric Lichtblau, "Ex-Agent Gets Some Immunity in Spy Case." *New York Times*. 1 May 2003. Available [online]: <http://www.nytimes.com/2003/05/01/politics/01SPY.html> [01 May 03].

¹² For a discussion of this refer to the annual report put out by NCIX that details the economic and industrial espionage activities against the U.S. See: Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002*. (Washington D.C.: GPO, 2003), vii. Available [online]: http://www.ncix.gov/news/2003/may/Annual_Economic_Report_Version.pdf. This is the seventh and most recent edition of the annual report that was first published in July 1995. [hereafter referred to as *Annual Report to Congress on Foreign Economic Espionage--2002*, #].

¹³ *Ibid.*, 1.

¹⁴ Interagency OPSEC Support Staff (IOSS), *Intelligence Threat Handbook*. (Greenbelt: IOSS, 2000), 19.

¹⁵ *Intelligence Threat Handbook*, 20-21.

¹⁶ *Annual Report to Congress on Foreign Economic Espionage--2002*, 8.

not to say that the U.S. has more to worry about from allies than it does from its historical enemies. In light of the recent espionage incidents involving Chinese agents – which includes the industrial espionage case against Qing Chang Jiang for illegally exporting missile technology to China¹⁷ as well as the FBI counterintelligence flap involving a Chinese double-agent¹⁸ mentioned above – it is clear that the covert intelligence activities of traditional U.S. foes continue to remain a threat to sensitive U.S. programs (technology and information) across a wide front.¹⁹ However, the illicit acquisition of sensitive information and technologies, which includes the proprietary information or trade secrets of corporations and businesses, appears to be a trend that is growing increasingly costly.²⁰ Thus, on balance it appears that adversary intelligence collectors have a wide array of targets and avenues for conducting espionage against the U.S., via the private and public sectors, targeting military secrets and corporate trade secrets. The combination of these threats demonstrates that the threat environment is continually diversifying and dynamic.

Although the threat environment has noticeably changed, these changes alone do not necessarily present an impetus to reform counterintelligence. In order to explain this more cogently one must understand how counterintelligence can mitigate these threats. The next section addresses this topic.

C. THE ROLE AND CAPABILITIES OF COUNTERINTELLIGENCE

Having briefly elaborated on the threat environment the U.S. currently faces today, what must be answered next is where counterintelligence fits into this equation. The logical place to start is to define counterintelligence and describe its role as a unique discipline within the intelligence community. Defining counterintelligence is somewhat problematic as there appears to be no readily agreed upon definition of it. Counterintelligence can and is defined in both broad and narrow terms. In narrow terms,

¹⁷ Rachel Conrad, “Chinese arrests raise concern over technology exports.” *Naples Daily News*. 23 January 2003. Available [online]: <http://www.naplesnews.com/03/01/business/d885278a.htm> [25 January 2003].

¹⁸ *Leung Affidavit* and “Ex-Agent Gets Some Immunity in Spy Case”

¹⁹ *Intelligence Threat Handbook*, 18-19.

²⁰ *Annual Report to Congress on Foreign Economic Espionage—2002*, 1 & 4.

one leading U.S. academic on the subject defines counterintelligence in the following way:

Counterintelligence, as practiced by most states, is the effort to protect their secrets, to prevent themselves from being manipulated, and (sometimes) to exploit the intelligence activities of others for their own benefit.²¹

Similarly, another leading writer on intelligence and counterintelligence matters defines counterintelligence narrowly by stating that:

Counterintelligence ... is defined as intelligence gathered about an adversary's intelligence activities and capabilities. In other words, the CI function is no more than collecting information to unmask adversarial intelligence operations and capabilities.²²

However, these definitions are in direct contrast to a broader definition of counterintelligence posited by the U.S. government in a variety of its official publications dealing with counterintelligence. The primary government definition of counterintelligence is arguably found in *Executive Order 12333 (EO1233)* as this is the guiding document for U.S. intelligence and counterintelligence activities. However it is essentially the same as the definition found in the *National Security Act of 1947*, but its wording appears to have been slightly reworked. First consider the definition found in *EO1233*:

Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.²³

And similarly, consider the definition in the *National Security Act of 1947*:

The term 'counterintelligence' means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign

²¹ Godson, *Dirty Tricks or Trump Cards*, 2.

²² Bernard C. Victory. *Modernizing Intelligence: Structure and Change for the 21st Century with a Note from LTG William E. Odom, USA (ret) Study Chairman*. (Fairfax: National Institute for Public Policy, 2002), 99.

²³ U.S. President. Executive Order. "United States Intelligence Activities, Executive Order 12333," *Federal Register* 46, no. 59941 (4 December 1981). Available [Online]: <http://www.fas.org/irp/offdocs/eo12333.htm> [20 February 2003]. [hereafter referred as *EO12333*]

governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.²⁴

Both of these definitions clearly define U.S. counterintelligence more broadly than the previous definitions specifically because they stipulate an additional, yet specific responsibility “to protect against international terrorist activities” besides protecting the U.S. against the activities of foreign intelligence services. It is worthy to note that no other intelligence discipline aside from counterintelligence is specifically stipulated, by definition, to protect the U.S. from the hostile activities of either foreign intelligence services or terrorists. Some further discussion on this point is imperative.

It seems that role counterintelligence plays in combating terrorism is one that has been the subject of debate. This is not a new debate either. Rather, this issue appears to have surfaced as terrorism, both domestic and international, became a cause for greater concern to U.S. at least as early as the late 1960’s.²⁵ On the one hand, the definition found in *EO12333* could be interpreted more narrowly than protecting against all terrorist activities generally. If one considers that the stipulation to “protect against” is perhaps not intended to cover all aspects of terrorism, but only “sabotage, or assassinations conducted for or on behalf of ... international terrorist activities”,²⁶ this means that counterintelligence has a very limited counter-terrorism responsibility. However, counterintelligence in practice seems to imply that a broader role to prevent and protect against terrorist activities beyond assassination and sabotage is the more correct view of this definition. A couple of examples of this are found by observing the comments made in the recently released *Report of the Joint Inquiry into the attacks of September 11, 2001*.²⁷ The first example concerns the FBI’s establishment of a unit specifically to deal with Islamic terrorist groups called the Radical Fundamentalist Unit (RFU):

²⁴ *National Security Act of 1947. U.S. Code*, vol. 50, secs. 401a-3 (1947); Available [online]: <http://www4.law.cornell.edu/uscode/50/401a.html> [10 October 2002].

²⁵ Roy Godson ed., *Intelligence Requirements for the 1980’s: Counterintelligence*. (Washington D.C.: National Strategy Information Center, 1980.), 156. [hereafter referred to as: Godson, *Counterintelligence*, pp.#]

²⁶ *EO12333*; see definition provided earlier.

²⁷ U.S. Congress, Senate and House. Permanent/Select Committees on Intelligence. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 with additional views*. 107th Cong., 2d sess., 2002. [hereafter referred to as *Joint Inquiry Report*, pp.#].

[At the FBI, the Radical Fundamentalist Unit was created in March 1994 to handle responsibilities related to international radical fundamentalist terrorists, including Usama Bin Ladin. This unit also handled **other counterintelligence matters**, and was responsible for the coordination of extraterritorial intelligence operations and criminal investigations targeted at radical fundamentalist terrorists. In 1999, the FBI recognized the increased threat to the United States posed by Bin Ladin and created the Usama Bin Ladin Unit to handle *Al-Qa'ida*-related **counterterrorism matters**.] (emphasis added)²⁸

These comments on the Radical Fundamentalist and the Usama Bin Ladin units suggest that the FBI, at least in terms of international terrorist activity occurring domestically, considers countering the threat posed by international terrorists to be both a counterintelligence and counterterrorism matter. Another discussion found in the *Joint Inquiry Report* concerning the state of the U.S. counterintelligence community, which reflect the comments of Lt. General (ret.) William Odom on counterintelligence and terrorism, is also instructive:

Counterintelligence, he urged, “is in the worst shape of all.” Five agencies have counterintelligence operations – FBI, CIA, and the three military services – “with no overall manager.” As a consequence, “[t]he parochialism, fragmentation, and incompetence are difficult to exaggerate in the U.S. counterintelligence world.” Fragmentation and lack of skills ensures “dismal performance” because “terrorists, like spies, come through openings.”²⁹

Gen. Odom’s comments clearly indicate that counterintelligence has a specific responsibility to prevent terrorists, like spies, from “coming through the openings” and that these efforts are significantly hampered by the current counterintelligence community arrangement. And finally, in a discussion held during a colloquium in 1980, it was stated that counterintelligence was being proscribed with respect to employing certain methods against terrorists:

In addition several of the senior CI officials who were beginning to make substantial inroads on these terrorists, are themselves under indictment for employing the previously accepted techniques of aggressive, effective CI.

²⁸ *Joint Inquiry Report*, 4-5.

²⁹ *Joint Inquiry Report*, 402.

And various restrictions threaten to strip us of the tools we must have to meet the threat of the 1980's.³⁰

This final example demonstrates that the role counterintelligence has in combating terrorism is a debate that stretches back to at least the late 1970's, one that includes both policy makers and intelligence professionals. The culmination of the evidence shows that counterintelligence has been historically used up to the present day, albeit with some debate, as a tool to counter the threat of terrorism. It should be noted that nowhere in this discussion is counterintelligence equated with counterterrorism. Even the earlier FBI example demonstrates that while terrorism is a counterintelligence matter, it is not the same as counterterrorism. Counterterrorism is a broad function denoting the comprehensive efforts of the U.S. intelligence, military, and law enforcement communities to (1) preemptively and aggressively respond to acts of terrorism directed against it via its military means, (2) prevent, deter, or neutralize terrorist operations via intelligence operations, and (3) to use law enforcement to apprehend and prosecute terrorists for planning and conducting such attacks.³¹ Counterintelligence falls under this definition as one specific means of countering terrorism. Therefore, counterintelligence should be viewed as encompassing a unique but limited role in countering terrorism. The specifics of this role will be outlined in greater detail in the second chapter.

Although the different organizations within counterintelligence community use various definitions of counterintelligence they appear to essentially encompass the same responsibilities as delineated in *EO12333*, which includes the terrorism dimension. Therefore it seems reasonable to use the *EO12333* definition of counterintelligence as the basis for analysis throughout this work. Based on this definition then, counterintelligence can be described as: those activities taken to identify, assess, neutralize and exploit the hostile actions of both foreign intelligence services (FIS) and terrorist organizations. Sometimes counterespionage is used interchangeably to describe counterintelligence but this is problematic and misleading. Counterespionage in reality describes the more

³⁰ Godson, *Counterintelligence*, 156.

³¹ U.S. President. *Presidential Decision Directive 39*. "U.S. Counterterrorism Policy," Washington, D.C.: Government Printing Office, 21 June 1995. Available [Online]: <http://www.ojp.usdoj.gov/odp/docs/pdd39.htm> [01 September 2003].

narrow function of counterintelligence: to both prevent the theft of U.S. secrets by foreign intelligence services and to use their agents as a means to deliberately deceive them.³² This is in contrast to the definition of counterintelligence as a discipline, which where it concerns terrorism specifically, means activities undertaken to penetrate international terrorist groups in an effort to deter or preempt their efforts to successfully conduct attacks.³³ In order to avoid confusion therefore, counterespionage will not be used to describe counterintelligence, except where it specifically and narrowly applies.

Counterintelligence is separate and distinct from the other intelligence disciplines that are nominally categorized by virtue of their collection means, such as human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT). Counterintelligence's explicit responsibility to the IC is to determine to what the extent the U.S. is the target of foreign penetration, whether spies or terrorists. Likewise, counterintelligence efforts are focused on the domestic and foreign activities of both adversary intelligence services and international terrorists in order to assess their capabilities as well as the risk they pose to U.S. security. Once this risk has been established U.S. counterintelligence must then determine where and to what extent penetration has occurred. In addition to assessing the threat of and discovering foreign penetrations, counterintelligence is also responsible for thwarting those activities as well.

Aside from being multidisciplinary, it is the responsibility of counterintelligence to thwart these threats that makes it unique; something one leading academic in this arena has best described as an *offensive-defense* role.³⁴ This description is best understood by separately expounding upon each adjective in turn. Its defensive role does not mean counterintelligence is static. Rather, some aspects of counterintelligence are notably defensive in nature, such as its analysis functions undertaken to determine the existence of hostile intelligence and terrorist activity directed against the U.S. But just because they

³² U.S. Army, Regulation 381-20. *The Army Counterintelligence Program*. Washington, DC: Department of the Army. (15 November 1993) [hereafter referred to as *AR 381-20*], 48.

³³ This broad definition is potentially problematic as it suggests a doctrinal and methodological overlap between "positive" intelligence operations (specifically human intelligence operations) and counterintelligence. However, if one focuses on the fundamental difference between the two, this argument can be clarified. Foreign or "positive" intelligence efforts seek to penetrate organizations (governments/terrorist) to learn their interests and intentions. This is different from the basic goal of counterintelligence, which is to penetrate these organizations in order to mitigate the risk that the activities of these groups pose, by neutralizing or exploiting their operations.

³⁴ Godson, *Dirty Tricks or Trump Cards*, 184.

are defensive does not mean they are passive in nature. Defensive or low-level source operations, which are counterintelligence activities that employ clandestine tradecraft to establish human intelligence networks, are active measures taken for defensive purposes.³⁵ These defensive measures though, are in contrast to the more aggressive functions of counterintelligence that are offensive and aimed at neutralizing or exploiting the activities of hostile intelligence service or terrorists.³⁶ These offensive operations, known by a variety of names, are essentially conducted to control or manipulate the intelligence networks of a foreign intelligence service or the covert apparatus of a terrorist organization. Together this dual-functionality highlights the wide range of capabilities counterintelligence can uniquely bring to bear against the hostile activities of foreign powers. Although only briefly touched upon here, this feature of counterintelligence will be described in further detail in the following chapter.

The aim of the second chapter, in addition to describing counterintelligence capabilities, is to ascertain whether or not counterintelligence capabilities require reform. As will be observed in the following chapter, U.S. counterintelligence capabilities are, in general, adequate to counter the threat posed by the various actors who seek to undermine U.S. security. This is largely the result of the nature of counterintelligence as an essentially timeless function. Though counterintelligence is dynamic in regards to incorporating new sources and methods, it is otherwise an unchanging art. Despite the generally unchanging nature of counterintelligence, it is in the domestic arena that counterintelligence encounters most of its problems. The specific areas of trouble seem to originate from where law enforcement and counterintelligence meet. Principally, these problems revolve around sources and methods used by counterintelligence domestically. This includes both the more intrusive means of intelligence collection and to a lesser extent the methods of counterintelligence analysis.

D. THE IMPETUS TO REFORM COUNTERINTELLIGENCE

Thus far the initial analysis has concerned both the threat environment and the role of counterintelligence with respect to mitigating the threat posed by the various

³⁵ These methods are also used in the course of conducting positive human intelligence operations.

³⁶ Robert David Steele, *The New Craft of Intelligence: Personal, Public, & Political*. (Oakton, OSS International Press, 2002), 22.

actors who seek to undermine U.S. security. What this analysis has determined is that U.S. counterintelligence is essentially responsible for identifying, thwarting, and sometimes manipulating, the activities of foreign spies and terrorist organizations. This analysis also shows that the threat environment is changing both in terms of the actors themselves and some of the targets of their activities. However, this does not itself provide the impetus to reform counterintelligence. Even if one considers that U.S. counterintelligence efforts failed to prevent Russian spies from infiltrating our intelligence services – and reporting suggests that counterintelligence deficiencies not only allowed spies to penetrate the IC, it helped them to remain undetected for 20 years³⁷ – this does not necessarily mean that counterintelligence requires wholesale change. This is because the problems that allowed spies to operate undetected for such long periods of time may be more of an issue of internal security practices within the penetrated organizations than any problem of how these organizations cooperated with one another. A more telling indication of the need for the counterintelligence community to be reorganized was the terrorist attacks of 9/11.

The attacks by *Al-Qa'ida* against the World Trade Center towers and the Pentagon in September 11, 2001, are normally discussed in terms of a failure of intelligence. This characterization of the attacks is definitely warranted as the Intelligence Community is among other things chartered to prevent attacks against the homeland from occurring. But, these same attacks are not often or specifically characterized as a failure of counterintelligence. Yet, given that U.S. counterintelligence is responsible for countering the activities of international terrorists it is reasonable to conclude that 9/11 was also specifically a counterintelligence failure as much as it was a “failure of intelligence” generally. It is important to note that the September 11 attacks alone do not constitute a systemic or organizational failure on the part of counterintelligence. Stating it another way: the 9/11 attacks are not the illness itself, but merely a symptom of the greater problem that plagues the Intelligence Community, of which the

³⁷ Both of the damage assessments of the Aldrich Ames and Robert Philip Hanssen cases discuss these deficiencies and indicate the U.S. counterintelligence efforts to detect or deter these individuals were abysmal. For further reference see *the Center for Counterintelligence and Security Studies (CI Centre)* website that has compiled virtually all of the available material on these two cases: http://www.cicentre.com/Documents/DOC_Hanssen_1.htm and http://www.cicentre.com/Documents/DOC_SSCI_Ames_Assessment.htm [01 August 2003].

counterintelligence community is a part. This problem is the division that separates counterintelligence organizations based on their area of operations, with one component of the community focused on the foreign arena and the other focused on the domestic arena. In fact, the recently released *Joint Inquiry Report* has stated very plainly that in relation to the attacks of September 11 the FBI and CIA failed to cooperate effectively thus leaving the U.S. more vulnerable to those attacks.³⁸ As previously indicated, this foreign-domestic split is not only a problem for counterintelligence but for the Intelligence Community as a whole. In fact this problem is really a consequence of the way the IC was formed over the past fifty years or so. Not surprisingly, this approach to organizing the IC has directly affected the way the U.S. counterintelligence apparatus was structured too. The reason for separating the organizations within the IC, and thus the counterintelligence community, along this foreign-domestic line is based on the United States' historical aversion to the encroachment of central government in the lives of its citizens. The belief that American citizens must retain a wide measure of freedom from unwarranted intrusion by the central government is a long-standing principle of the U.S. federal system. This belief itself is an outgrowth of the fear that the federal government will use the more intrusive means at its disposal, which is to say its intelligence services, to encroach on the lives of its citizens. Yet this capability is necessary for use against U.S. adversaries. Therefore the solution to the problem of retaining covert intelligence means for use against foreign adversaries, while still hindering the employment of these same means against one's own citizens, was resolved by creating two separate organizational types: one foreign, one domestic. However, in spite of the historical precedent of separating intelligence and counterintelligence into foreign and domestic components, America needs to rethink this approach to organizing its Intelligence Community. This old paradigm needs to be rethought because dividing U.S. intelligence and counterintelligence organizations in terms of their geographic responsibility, while certainly understandable and well intentioned, is unnecessary and hinders their effectiveness.

The current design of the IC, and specifically where it applies to the counterintelligence community, is problematic as a result of this unnecessary foreign-

³⁸ *Joint Inquiry Report*, 45.

domestic division. These problems are most clearly seen in the relationship that exists between the principle U.S. counterintelligence organizations, the Central Intelligence Agency (CIA) and the Federal Bureau of Investigations (FBI). The CIA, as outlined by *EO12333*, has been given the responsibility to conduct foreign intelligence and counterintelligence activities abroad. Conversely, the FBI has by this same executive order been given the responsibility for conducting intelligence and counterintelligence activities in the U.S. Unfortunately and although this structure was created with good intent, it noticeably hinders the effectiveness of counterintelligence activities. Since counterintelligence is responsible for thwarting the activities of both spies and terrorists, and given that the world is extremely interconnected allowing these adversaries to target America from abroad as well as from within the continental U.S., dividing counterintelligence into separate organizations hinders the unity of effort needed to succeed in these tasks.

This problem is not new, nor did it only recently become an issue. The September 11 attacks, as stated before, are symptomatic of a historically unresolved problem within counterintelligence that provides a catalyst for discussing and fixing this long-standing problem. Many years before 9/11 would even be planned, during the period between 1939 and 1947 when the FBI had the lead domestic counterintelligence role³⁹ and the CIA, would eventually gain control over foreign intelligence and counterintelligence efforts⁴⁰ the seeds of division were being sown that would overtime bloom into a whole host of problems. Although the initial division of (intelligence and) counterintelligence responsibilities by geographic location was not as strict in the beginning as it is today, FBI and CIA abuses in the period between their creation and the 1970's fed a growing public anathema to counterintelligence, this in turn led to the Pike and Church Committee hearings, which resulted in solidifying these divisions for future generations.⁴¹ It would be prohibitive to try and list or discuss here the various problems associated with this

³⁹ Joseph E. Persico. *Roosevelt's Secret War: FDR and World War II Espionage*. (New York: Random House, 2001), 17.

⁴⁰ Frank J. Rafalko, ed., *A Counterintelligence Reader, Volume II: Counterintelligence in World War II*. (Washington D.C.: National Counterintelligence Center, 1999), Chapter 1.

⁴¹ Wannal, W. Raymond, "Undermining Counterintelligence Capability," *International Journal of Intelligence and Counterintelligence*. 15 (2002): 326.

foreign-domestic divide extant in the counterintelligence community. Thus, this will be the subject of the third chapter of this work.

Unfortunately, and despite numerous attempts – both from within and outside the U.S. government – to address the issues arising from this foreign-domestic split, the problem remains. Thus, a few recommendations are in order that will hopefully resolve some of these issues.

E. COUNTERINTELLIGENCE REFORM: THE WAY AHEAD

In light of the need to reform counterintelligence, this section will briefly outline some proposals that are intended to resolve some of the more outstanding issues facing U.S. counterintelligence currently. As stated earlier, these reforms are neither inclusive nor do they claim to fix all the problems that involve counterintelligence operations. However, these reforms do address the core issues such as the foreign-domestic split, the overlap in law enforcement and intelligence as well as the key shortfall in counterintelligence capabilities, its analytical function.

The recommendations are as follows:

- Remove the offensive counterintelligence operational capability from the five existing agencies that currently have this responsibility. This includes the CI component from the FBI, CIA, AFOSI, NCIS and from the U.S. Army's INSCOM
- Create a new, stand-alone counterintelligence agency that is the only agency with the charter to conduct offensive counterintelligence operations.
- Leave in place the rest of the counterintelligence offices, departments and divisions that are spread throughout the IC in order to act in a support role. These offices, like the former operational components, would have the authority and responsibility to conduct investigations and analysis in order to identify hostile intelligence or terrorist activities.
- Create a single, integrated counterintelligence database that includes threat reporting from all counterintelligence offices, regardless of type, military, intelligence, law enforcement or other civilian agencies. This would widely disseminate threat reporting detailing foreign adversary modus operandi and

the like as well as restricting the flow of insider threat information and intelligence to the new national-level counterintelligence operations agency to ensure security to offensive operations.

- Devolve counterintelligence down to the state, county and local level. Encourage the establishment of counterintelligence offices in all major governmental divisions.
- Encourage the development of private sector counterintelligence offices to conduct analysis and internal investigations to identify insider/outsider threat to trade secrets and confidential proprietary information.

These recommendations will be explained in more detail in the last chapter. The second chapter will go on to describe both the role and capabilities of counterintelligence as well as identifying any areas that need to be reformed. The third chapter will discuss the counterintelligence community and the impetus that this structure provides for reforming and ultimately reorganizing U.S. counterintelligence for a more secure nation.

THIS PAGE LEFT INTENTIONALLY BLANK

II. COUNTERINTELLIGENCE DELINEATED

A. INTRODUCTION

It remains to be seen exactly whether or not counterintelligence practices need reform. In order to determine if change is necessary, the traditional functions of U.S. counterintelligence must first be outlined. These functions will be drawn from the publicly available counterintelligence manuals and other open source intelligence literature. These functions will then be analyzed and categorized in an attempt to more coherently organize and delineate those tasks into a set of “core competencies” of counterintelligence. We will then examine what affect a dynamic threat environment has on these core competencies, if any. Additionally, counterintelligence capabilities need to be assessed to determine if there are any deficiencies that should be corrected to ensure they do not hinder counterintelligence achieving its aims. Ultimately, this analysis seeks to ascertain if and how counterintelligence practices have contributed to a series of very damaging U.S. intelligence failures.

B. THE FUNCTIONS OF COUNTERINTELLIGENCE

According to the Army’s most recent counterintelligence manual *FM 34-60* and the Marine Corps’ counterintelligence manual, *MCWP 2-14*, there are essentially four functions around which counterintelligence is organized and operates: collection, investigations, analysis, and operations.⁴² While these four functions are derived specifically from *FM 34-60* and *MCWP 2-14*, the other official armed service and Department of Defense counterintelligence directives also generally note these fundamental functions. Rather than discuss each manual in turn and since both the Army and Marine Corps counterintelligence manuals are quite detailed, they will be relied upon as the key source material. The Federal Bureau of Investigation (FBI), one of the two

⁴² U.S. Army, Field Manual 34-60. *Counterintelligence*. Washington, DC: Department of the Army. (3 October 1995) [hereafter referred to as *FM 34-60*], and U.S. Marine Corps, Marine Corps Warfighting Publication 2-14. *Counterintelligence*. Washington, D.C.: Headquarters of the Marine Corps. (5 September 2000) [hereafter referred to as *MCWP 2-14*].

principle national-level counterintelligence agencies, recognizes these functions as being essential as well. These functions are outlined in the *Attorney General Guidelines for Foreign Intelligence Collection and Foreign Counterintelligence Investigations*⁴³, which specifies that investigations, intelligence collection and support operations, are all FBI counterintelligence activities. A review of non-official sources reveals that counterintelligence is generally broken down into two or three broad functional areas, with collection and exploitation being the most common, and with others adding analysis.⁴⁴

In spite of some apparent differences in counterintelligence functions as described by the various sources, it seems counterintelligence can nonetheless be broken down into two general functions: (1) identifying and assessing the threat posed by hostile intelligence services or terrorist organizations and (2) exploiting the adversary intelligence or terrorist operations to the advantage of the U.S. Although these functions are perhaps not all encompassing they do take into account the key variations in definition and task delineation that exist between the agencies and offices responsible for counterintelligence. Referring to these two broad categories eliminates some of the confusion in terminology, allowing us to focus once again on the essential mission of counterintelligence.

These two basic functions are essentially a harmonization of the definitions and responsibilities of counterintelligence. This is readily discernable by considering the scope of each function. The first function requires that both adequate collection and investigative means be employed in order to identify and locate a potential intelligence or terrorist threat. In addition, the first function demands a coherent, detailed and “fused”

⁴³ U.S. Federal Bureau of Investigation, *Attorney General Guidelines for Foreign Intelligence Collection and Foreign Counterintelligence Investigations*. Washington, DC: Government Printing Office. (18 April 1983). Available [online]: <http://cryptome.sabotage.org/fbi-guide.htm> [10 January 2003]. This document is a declassified FBI directive that was made available to Cryptome through a FOIA request via Jeffery Richelson and Michael Evans of the National Security Archive, whose website is located at: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>.

⁴⁴ Collection and exploitation are readily agreed upon central facets of counterintelligence as drawn from the following works: *Fixing Intelligence: For a More Secure America* by Lt. Gen (Ret.) William Odom; *A Short Course in the Secret War*, by Christopher Felix; *Intelligence from Secrets to Policy*, by Mark Lowenthal; *Fixing the Spy Machine*, by Arthur S. Hulnick; whereas analysis is emphasized in a couple, notably: *A Never Ending Necessity: The Ten Commandments of Counterintelligence* a CSI article by James M. Olson, and *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence* by Roy Godson.

analysis of the relevant intelligence to successfully assess the threat. The second function involves taking whatever measures are necessary to neutralize or exploit the adversary to the advantage of the United States. This function also requires integrating finished counterintelligence products into the operational support process. Operational support used in this context means providing counterintelligence operators, especially those who will be conducting investigations or offensive operations, with the most comprehensive assessment of the adversary being targeted. Suffice it to say that without integrating counterintelligence analysis and counterintelligence operations, counterintelligence would prove to be a fruitless endeavor. This is because counterintelligence effectiveness is dependent on timely and credible intelligence assessments of the organizations or individuals targeted; without these an operator will either lack the context or the content needed to adequately focus his/her efforts against the adversary. This is regardless of the kind of counterintelligence organization conducting the operation, whether civilian, law enforcement or military service.

C. THE CORE COMPETENCIES

The ultimate aim in breaking counterintelligence down into two general functions is to facilitate the development of a set of core competencies that can serve as a guidepost for counterintelligence responsibilities regardless of the threat environment. There are four core competencies that can be logically drawn out from the two general functions of counterintelligence.

1. Identifying and Assessing the Threat

The first two core competencies are *identifying hostile intelligence & terrorist threats* and *assessing the threats*. *Identifying hostile intelligence & terrorist threats* covers a number of counterintelligence activities, but specifically includes counterintelligence investigations and the broad array of collection operations. Of note, since counterintelligence is by nature multidisciplinary, it relies on the entire spectrum of intelligence collection sources and methods. Thus, in order effectively to identify and locate the hostile activities of an adversary intelligence service or a terrorist organization, counterintelligence must integrate technical collection, clandestine human sources and

open source information. The second core competency, *assessing the threats* is a crucial task that by definition means a process of analysis conducted to determine both the threat from and the vulnerability to hostile intelligence and terrorist operations. The “value added” of this analysis comes from the evaluation and recommendations made concerning security and countermeasures that can mitigate the threat. This also highlights the absolute need for a comprehensive intelligence database, one that includes adversary as well as “friendly” operational information and intelligence, as well as a trained analytical staff proficient at fusing intelligence from a variety of sources, both open and secret.

Counterintelligence analysis provides the foundation to conducting operations against an adversary. The specific analyses made of adversary capabilities, intentions, and actual operations (penetrations of the U.S.), are used to highlight the weaknesses and vulnerabilities of the adversary in order to provide tailored direction to the counterintelligence operator who will be targeting this adversary. Particularly where the possibility exists of multiple operations being conducted against the same target, counterintelligence analysis should include knowledge of allied or “sister-agency” operations in order to prevent an inadvertent compromise of an operation or a duplication of effort to develop. The danger in this kind of information being available via a database with wide access is obvious in its potential to compromise extremely sensitive sources. This requires such information to be closely guarded and access to it severely limited. However, if access to “allied” or “friendly” (other U.S. organizations) efforts are warranted, access to such data could be made readily available. Where counterintelligence information or products concern the capabilities, intentions, or *modus operandi* of foreign intelligence services and terrorists, the accessibility to such information should be made readily available. And ultimately, where threats and specific vulnerabilities to infrastructure or personnel are identified through operations or analysis, such data should also be made available to as many as possible to assist the development of countermeasures.

2. Neutralization and Exploitation

The second two core competencies are *neutralization operations* and *exploitation operations*. Since counterintelligence has been described as an “offensive-defense”⁴⁵ it would seem rational to separate these second two core competencies based on their relative offensive or defensive nature. Therefore *neutralization operations* are defined here as the mainly defensive measures taken to hinder or thwart the collection efforts of the enemy through either concealing the information itself or denying the enemy access.⁴⁶ *Neutralization operations* also include the measures taken to hinder terrorist intelligence activities as well. *Exploitation operations*, on the other hand, are defined as primarily offensive operations that seek to mitigate the threat by turning the adversary’s operations on their head. Despite the distinction made between these two core competencies based on their relative offensive or defensive nature, *neutralization* and *exploitation operations* are essentially two sides of the same coin, for to mitigate the threat posed by adversary intelligence operations or terrorist organizations each must employ both passive and active measures as well as capitalize on the intelligence collected and the analyses conducted.

a. Neutralization Operations

Neutralization operations largely fall under two general categories: (1) security programs, which are designed to limit access to the sensitive programs within their specific areas of concern, and (2) countermeasures, which are designed to thwart the activities of adversary intelligence services and terrorist from a distance⁴⁷. It should be noted that counterintelligence neutralization operations as defined and described here are potentially limited in their capacity to neutralize the activities of terrorist organizations. In order to clarify this it should be noted that security programs as function of neutralization operations by design hinder any insider, thus a spy, from gaining unwarranted access to a sensitive facility or sensitive information. The insider threat does not generally apply to terrorists as most terrorists groups do not normally use clandestine

⁴⁵ Godson, *Dirty Tricks or Trump Cards*, 184.

⁴⁶ *MCWP 2-14*.

⁴⁷ Godson, *Dirty Tricks or Trump Cards*, 230.

agent networks to gain intelligence on a potential target; such intelligence as needed for an attack is often times readily available through overt surveillance.⁴⁸ Therefore, by and large security programs do not pertain to terrorists. Countermeasures on the other hand can potentially hinder the activity of either spies or terrorists. At the same time, however, it should be noted that since terrorists generally pose a physical security threat to personnel and facilities, the passive and defensive countermeasures that most effectively hinder their activity are logically carried out by physical security forces. In terms of terrorist pre-attack surveillance and other intelligence related activity, certain countermeasures described below may hinder their intelligence collection activity as well. However, given that most pre-attack surveillance efforts are conducted in such a manner as to make them appear innocuous, it is uncertain how successful these countermeasures will be at thwarting terrorist intelligence activity. Although neutralization operations may adversely affect terrorist operations – specifically in terms of hindering intelligence collection – they clearly do not counter terrorist activity to the same extent as physical security countermeasures. The only other possible exception to this is the active measures of neutralization operations, the defensive collection operations that are described at the end of this section. It seems then, that the following section is more directly applicable to countering the efforts of foreign intelligence services than terrorists. This is so because neutralization operations appear to facilitate passive and defensive counterespionage activities but have a limited capacity in protecting against terrorism.

Some good examples of security programs are personnel security investigations (PSI), and direct security violation and counterintelligence investigations, which are also called SAEDA (Subversion and Espionage Directed against the U.S. Army) investigations within the U.S. Army.⁴⁹ These security programs are passive in

⁴⁸ Pre-attack preparations always involve surveillance activity and often times involve “dry-runs” as a way to collect intelligence and test the security response of the target of attack. These activities in of themselves are usually sufficient to successfully conduct an attack, thus no clandestine network of agents is necessary. However, it does appear that some groups, particularly *Al-Qa’ida*, have considered using insiders get better intelligence as is evidenced by instructions to this end found in their training manual, “*Declaration of Jihad Against the Country’s Tyrants: Military Series*”, which was discovered on a computer file in the home of *Al-Qa’ida* member Nazih al-Wadiah Raghie in Manchester, England during a police raid of his home on May 10, 2000.

⁴⁹ FM 34-60, 2-1 & 2-5.

nature, some of the more noticeable ones being the security education and counterintelligence awareness programs often utilized to enhance awareness of potential security risks involving espionage.⁵⁰ Another example of passive measures is the use of the polygraph to vet personnel in order to grant them access to specially compartmented or classified information.

Whereas passive security programs prevent hostile intelligence services from gaining physical or personal access to sensitive information from the inside, countermeasures on the other hand generally involve denying the adversary intelligence collector from being able to access potential information from the outside. An operational example of these countermeasures is the cover, concealment and deception (CC&D) operations that are employed to deliberately trick or impair the ability of an adversary imagery intelligence collection system. Another example is foreign contact reporting requirements. By enacting a requirement whereby officials with access to classified information must report all foreign contacts, the counterintelligence service can potentially eliminate the opportunity for clandestine recruitment efforts of the adversary. The creation of an entire sub-discipline known as *technical surveillance countermeasures* (TSCM), which was developed specifically as a way to mitigate the increasingly diverse array of foreign clandestine (technical) surveillance techniques, demonstrates that effective countermeasures are integral in neutralizing adversary intelligence operations. Ultimately, the evidence presented indicates that *neutralization operations* are dependent on the effective combination of both security programs and countermeasures in order to hinder hostile intelligence services in their stride to gain access to sensitive information.

Neutralization operations, although largely defensive and passive in nature can also utilize active measures, such as defensive collection operations. Defensive source operations, as they are known within DoD counterintelligence, are CI human source collection operations that are actively employed to diminish the effectiveness of adversary espionage efforts and to prevent terrorist attacks from being conducted. An example of this kind of defensive collection operation done by DoD counterintelligence components, are Counterintelligence Force Protection Source

⁵⁰ An example of one of the policy documents outlining these programs is the DoD Directive 5240.6 *Counterintelligence Awareness and Briefing Program*. (26 February 1986).

Operations (CFSO).⁵¹ These operations are twofold in nature, thwarting the espionage efforts of foreign intelligence services (FIS) and deterring or preventing terrorist attacks and/or FIS-sponsored sabotage from occurring. CFSO is a generic term that was devised as a means to clarify terminology between the four service components and as a way to integrate force protection needs into counterintelligence responsibilities.⁵² CFSOs are human source operations, normally clandestine in nature, conducted abroad that are intended to fill the existing gap in national level coverage, as well as satisfying the combatant commander's intelligence requirements. Other examples of counterintelligence collection that potentially provide support to *neutralization operations* are the screening and debriefing of non-tasked human sources, also called *casual* or *incidental* sources such as: walk-in's (individuals who volunteer information); unwitting sources (any individual providing useful information to counterintelligence, who in the process of divulging such information may not know they are aiding an investigation); defectors; enemy prisoners of war (EPW); refugee populations and expatriates; interviewees (individuals contacted in the course of an investigation); and official liaison sources.⁵³ All of these as mentioned earlier are potentially beneficial for counterintelligence use in *neutralization operations*, however some of these same sources also allow for their development into potential sources for aggressive exploitation as well.

b. Exploitation Operations

Exploitation operations are the more arcane and secretive measures of counterintelligence that give rise to its 'nefarious' reputation. These operations utilize many of the same sources of information and especially focus on exploiting the clandestine human and technical sources to the detriment of FIS and mitigate the threat

⁵¹ *FM 34-60*. Note: this term is used by all the Department of Defense counterintelligence components and is found in their respective manuals, directives and instructions.

⁵² *Ibid.*, 4-8.

⁵³ U.S. Army, Field Manual 34-17. *Counterintelligence Operations*. Washington, DC: Department of the Army. (28 February 1968). [hereafter referred to as: *FM 34-17*]. Although this much older version of the U.S. Army's counterintelligence manual has subsequently been superseded many times over (most recently by *FM 34-60*), it provides much more detail on certain subjects, to include in this case, the various possibilities of human sources.

posed by terrorists, both to the benefit of the U.S. In DoD circles *exploitation operations* fall under the category of “special techniques”, “CI special operations”, “offensive counterintelligence operations”, and “offensive counterespionage activities”, and due to their sensitive nature the specific details of this tradecraft are classified in their entirety.⁵⁴ Since other federal level documents that discuss these types of operations are also classified, it is at this point that unofficial open source publications are of particular use, as the only really useful information will come from intelligence reform literature. Other activities that fit within the scope of these offensive counterintelligence operations are: double agent operations, disinformation operations, and deception/counter-deception operations.

At the heart of *exploitation operations* is the objective to degrade the effectiveness of an adversary’s intelligence service or a terrorist organization. Principally this is done one of two ways, either by manipulating the adversary (FIS/or terrorist) in some manner or by disrupting the adversary’s normal operations. For FIS this means disrupting their collection capability, whereas with terrorists this means disrupting their attack capability. Disrupting an adversary’s normal pattern of operations is perhaps the easier of the two tasks to achieve. At least in terms of its metric, offensive counterintelligence operations that succeed in breaking up a clandestine network by arresting the persons involved or by exposing their actions – such as declaring diplomats found to be spying “*personae non gratae*” – demonstrate that disruption is quite measurable and effective against FIS if the right actions are taken.⁵⁵ The same can be said of measuring the effectiveness of offensive counterintelligence operations against terrorists; if the attacks do not occur due to the CI operation, they have obviously been disrupted.

⁵⁴However, for those with access, some of these documents are listed here for further reference: U.S. Army Regulation (S) AR 381-47 *U.S. Army Offensive Counterespionage Activities (U)*. (30 July 1990); DoD Directive S-5240.9 *Support to Department of Defensive Offensive Counterintelligence Operations*. (28 November 1989). DoD Joint Publication (S) JP 2-01.2 *Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations (U)*. (no date); Director of Central Intelligence Directive DCID 5/1 *Coordination of US Clandestine Foreign Intelligence Activities Abroad*.

⁵⁵ Roy Godson ed., *Intelligence Requirements for the 1980’s: Counterintelligence*. (Washington D.C.: National Strategy Information Center, 1980.), 30. [hereafter referred to as: Godson, *Counterintelligence*, pp.#]

By far, the more difficult task is manipulating the enemy, particularly over a long period of time.⁵⁶ Manipulation implies the use of deception and to deceive a wary opponent is an inherently complex task that requires the utmost knowledge of the adversary and of oneself. This is especially true when the target of that deception is both aware they are a target for deception and a practitioner of this craft themselves; such is the case with foreign intelligence services of other nations.⁵⁷ Terrorists on the other hand, although they engage in deception as a function of security⁵⁸ appear to be more prone to manipulation or deception by a well-placed adversary than are foreign intelligence services. This is in part due to the fact that many terrorist groups, whose members “often mistrust and fight among each other, disagree, and vary in conviction.”⁵⁹, are not as internally cohesive as foreign intelligence services, potentially leaving them more vulnerable to both deception and manipulation. This is where a detailed discussion of moles and double agents becomes necessary.

Moles and double agents are the bread and butter of *exploitation operations*, and truly put the “offense” in offensive counterintelligence operations. A *mole* is intelligence jargon for the penetration of an organization – a foreign government, a foreign intelligence service, or even a terrorist organization – by an adversary intelligence officer and usually refers to the intelligence officer himself/herself. Penetrating the intelligence service of an adversary or the ranks of a terrorist group is no easy task to be sure. It can be accomplished in at least several ways. One of the more difficult methods involves having the would-be-mole “dangled” – that is luring the adversary intelligence service (or terrorist group) to recruit the opposition’s clandestine intelligence officer who is posing as a “walk-in” (someone who voluntarily offers information) – in the hopes that the adversary will unknowingly take the bait.⁶⁰ Another method is to directly recruit an intelligence officer (or terrorist member) from within the

⁵⁶ Godson, *Dirty Tricks or Trump Cards*, 223.

⁵⁷ Godson, *Dirty Tricks or Trump Cards*, 192.

⁵⁸ Roy Godson and James J. Wirtz, eds., *Strategic Denial and Deception: The Twenty First Century Challenge*. (New Brunswick and London: Transaction Publishers, 2002), 138.

⁵⁹ Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*. (Washington, D.C.: RAND, 2002), 47.

⁶⁰ Godson, *Counterintelligence*, 32.

ranks of the adversary service (terrorist group) and having that officer (terrorist) maintain their normal duties while spying on their parent service (organization); this is also referred to as recruiting an “agent” or “defector in place”.

The discovery of an adversary intelligence officer⁶¹ who has succeeded in penetrating one’s own organization offers the penetrated intelligence service the possibility of “turning” this officer in order use him as a “double agent”. This may be extremely difficult to accomplish, and even if accomplished the real difficulty is maintaining control of this “turned asset”⁶². Controlling an enemy agent who has been turned is a many-faceted and complex exercise that essentially boils down to making certain that the agent’s new-found loyalty remains consistent, which means determining whether the “doubled” agent’s turning is genuine or false.⁶³ However, this process can be quite convoluted and fraught with uncertainty and suspicion. Where it concerns terrorist groups, a terrorist who betrays his organization can be thought of and run as a double-agent against the terrorist’s “parent” organization in much the same fashion as an intelligence officer from a foreign intelligence service. Therefore, for sake of ease, wherever double-agents are discussed the methodologies generally apply to activities conducted against terrorist groups as well.

One facet of the efforts to control a double agent operation is to ensure that the double agent is protected from discovery by the parent intelligence service; this is especially true in circumstances where the double agent is a defector-in-place. Another facet of this control, and arguably the more difficult one, is the need for the service running the double agent to carefully evaluate the intelligence the turned asset is providing in order to prevent the double agent from being turned back against them. Evaluating the intelligence provided by the double agent is crucial as a careful analysis of it can potentially provide insight into what the adversary intelligence service knows about the targeted service, this knowledge may include awareness of the doubling of the adversary’s agent. If the adversary service is indeed aware that their agent has been

⁶¹ The potential for a terrorist to penetrate a U.S. intelligence/counterintelligence organization is far less likely than an officer of a foreign intelligence service who attempts the same thing.

⁶² The use of the term “asset” is intelligence jargon, used primarily by human intelligence collectors, to denote the use of a human source as an intelligence asset.

⁶³ Christopher Felix. *A Short Course in the Secret War*. (Lanham: Madison Books Inc., 2001), 123.

doubled back against it, it can potentially turn this agent yet again, only this time the agent will be working for the parent service once more, now earning the new moniker of “triple agent”. This circumstance can be quite confusing, particularly in situations where an agent makes multiple turnings. One author on the subject succinctly describes this otherwise complicated process by saying: “In brief, once turned makes a double agent, twice turned makes a triple agent, and so on.”⁶⁴

Despite their apparent complexity and risk, double agent operations can be run with a relative degree of freedom from discovery if wisely conducted and selectively carried out. One way to minimize their risk is to ensure that upon discovery of a penetration of the host service, the adversary agent is kept unaware of his/her discovery, and slowly the host service must then curtail the mole’s access to information in a manner that does not arouse his/her suspicion, while at the same time he/she is fed erroneous information.⁶⁵ This surreptitious feeding of misinformation without the agent’s awareness back to the parent service can in essence “double” the agent without having to turn them through a more formal recruitment. A greater success could probably be achieved through “pitching” the enemy agent – that is, by directly asking the adversary to switch allegiances. If he accepts the pitch, the now “turned” agent is more likely to effectively feed misinformation back to his parent service. One reason this kind of double agent is potentially more effective is because as an insider he has an intimate understanding of his parent service that enables him to pin point and exploit its weaknesses more easily. However, conscientious betrayal of an adversary’s agent is quite possibly much more psychologically challenging on the part of the service handling him/her as a double agent. In this case, the intelligence service handling the agent must consider whether the double agent having turned once, might turn against them. This again harkens back to the issue of control, the limits of which are demonstrated in being able to distinguish between false and genuine betrayal and in the relative lapse in awareness of the service against which the double agent is being run.⁶⁶

⁶⁴ *Ibid.*

⁶⁵ Mark M. Lowenthal. *Intelligence: From Secrets to Policy*. (Washington D.C.: CQ Press, 2000), 102.

⁶⁶ Felix, 124.

Since determining loyalty and maintaining control over double agents is tricky at best, it is not hard to see how problematic this methodology can become. In fact, the potential for multiple turnings of agents and perhaps worse, the turning of one's own intelligence officers (especially those working within counterintelligence itself), poses a serious risk to any intelligence service wishing to employ these techniques. This may be the reason that triple-agent operations appear not to have been undertaken by U.S. counterintelligence in some espionage cases that have come to light in recent years, particularly among those involving high-level penetrations.⁶⁷ Although the arrest and prosecution of Aldrich Ames of the CIA and Robert Hanssen of the FBI, both of whom were senior counterintelligence officers in their respective agencies who volunteered to spy for the Russians, hardly qualifies as conclusive evidence that triple-agent operations were not attempted throughout the community writ large, these two cases suggest that *neutralization operations* may be the preferred method of handling adversary double agent operations vice the more aggressive exploitation of these potential triple-agent sources.

Putting aside the more problematic prospects of agents turned multiple times, other historical examples of successful long-term double agent operations such as Britain's Operation Double Cross, conducted in World War II that succeeding in turning most of Germany's agents, as well as the German Abwehr's Operation North Pole that succeeded in capturing and controlling the entire British undercover network in the Netherlands⁶⁸, suggest that these types of operations are indeed feasible. Therefore, despite the obviously very risky and extremely complex nature of double agent operations, the potentially quite lucrative intelligence windfall – the disruption or deception of an adversary service – makes them an inseparable component of *exploitation operations*.

D. THE TIMELESS NATURE OF COUNTERINTELLIGENCE FUNCTIONS

⁶⁷ Arthur S. Hulnick. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*. (West Port, Connecticut: Praeger Publishers, 1999), 94.

⁶⁸ Godson, *Dirty Tricks or Trump Cards*, 233, and Felix, 125.

The basic functions of counterintelligence appear to be a timeless set of skills and tasks that defines counterintelligence as a discipline. Although the threat environment has undoubtedly changed many times over since counterintelligence was first employed in the U.S. during the Revolutionary War, the core competencies as laid out above have changed little, if any in the intervening years.⁶⁹ To further substantiate this claim, one must look at the more recent roots of U.S. counterintelligence as found in the period just prior to and during World War II. It was during this era that counterintelligence started to become institutionalized as a separate and definitive practice of U.S. intelligence and is thus considered the origin of the modern U.S. counterintelligence establishment.⁷⁰ From this point on U.S. counterintelligence has changed only in so far as it has become multidisciplinary in nature. This multidisciplinary nature was the result of the need for counterintelligence to keep pace with modern technology that subsequently diversified the sources for intelligence. For example, by the time the Cold War began U.S. counterintelligence had already incorporated into its tradecraft intercepted adversary radio signals, under a program with the code name VENONA, which were used to identify and monitor the activities of clandestine Soviet agents operating within the U.S.⁷¹ This is but one example of how signals intelligence (SIGINT) collection began to aid counterintelligence investigations, which also demonstrated the need too to develop an operational capability within U.S. counterintelligence to counter adversary SIGINT operations. As the means hostile intelligence services used to target the U.S. began to diversify so too did U.S. counterintelligence diversify, evolving from a merely human-oriented, counterespionage effort, to a more broadly focused, multi-source *counterintelligence* effort.

The marriage of SIGINT and HUMINT, which is to say the use of both technical and human means in counterintelligence activity, would eventually give rise to further developments such as the aforementioned technical surveillance countermeasures that

⁶⁹ For more information on this refer to the work by Stephen F. Knott entitled *Secret and Sanctioned: Covert Operations and the American Presidency*. (New York and Oxford: Oxford University Press, 1996), which is an excellent source on American intelligence practices during the American Revolution which, among other things, describes counterintelligence efforts in quite good detail.

⁷⁰ Rafalko, 1.

⁷¹ *Ibid.*, Chapter 4 and Robert Louis Benson and Michael Warner. eds., *VENONA: Soviet Espionage and the American Response 1939-1957*. (Washington D.C.: Government Printing Office, 1996.), xix.

serve as technical means to enhance an otherwise purely human endeavor. Not surprisingly, this expansion of counterintelligence into a multidisciplinary element of intelligence has gotten greater since the end of the Cold War due to the seemingly exponential growth in technological advancements that continue to diversify the technical means of intelligence collection. As a result, counterintelligence must now not only contend with the threat posed by U.S. adversaries who use information systems to aid in conducting espionage, but the threat to the national infrastructure itself which includes numerous critical information systems.⁷² However, despite a changing technological environment and the subsequent need to diversify counterintelligence with respect to integrating and understanding these advanced technologies in order to develop new sources or collection methodologies, U.S. counterintelligence still appears to be relatively static in terms of its fundamental functions. Thus, counterintelligence, whether facing the “insider threat” posed by human spies or the “outsider threat” posed by both human agents and perhaps in the future “intelligent software agents”⁷³, must nonetheless still use its timeless set of functions.

Even in view of the events of September 11 that threw international terrorism to the forefront of American foreign and domestic policy, as well calling into question U.S. counterterrorism policies, this ostensibly “new threat” has few implications on the essential functions of counterintelligence as a discipline. Combating terrorism is not a new concept for the U.S. counterintelligence community as it has had a responsibility to expend some of its time and resources on this threat since at least the early 1980’s; albeit, like most other disciplines within the intelligence community, counterintelligence has not focused on terrorism until now. Preventing terrorist attacks from being conducted against U.S. interests becoming the primary mission of counterintelligence, this does not necessarily force a change in any of the core competencies. Rather, counterintelligence must merely begin to more readily incorporate terrorists as another target of its

⁷² U.S. Congress. Joint Economic Committee. *Security in the Information Age: New Challenges, New Strategies*. (Washington D.C.: GPO, 2002), 99-100. The specific article referred to by this citation is “Counterintelligence and Infrastructure Protection” and was written by John MacGaffin.

⁷³ Christopher D. Noble, *Espionage in Information Warfare*. (Carlisle, PA: U.S. Army War College, 2002). Available [online]: <http://carlisle-www.army.mil/usacsl/divisions/std/branches/keg/98TermII/espionage.htm>. The notion of artificial intelligence software agents is only one of many future possibilities in the ever developing world of cyber-warfare and cyber-espionage.

operations. Probably the best historical example of reforming and refocusing in light of a changing threat environment is found in the development of the previously discussed Counterintelligence Force Protection Source Operations (CFSOs). It is essential to remember that these CFSOs were specifically devised within the DoD counterintelligence components to provide intelligence on terrorist activity as a force protection measure as a result of the increasing threat of terrorism to U.S. forces abroad and that CFSOs generally employ the same fundamental skill set as other counterespionage activities. Therefore, in the midst of an ever-changing threat paradigm of various kinds of actors, counterintelligence has shown a remarkable stability in its operational practices up to the present day.

E. COUNTERINTELLIGENCE IN THE POST-SEPTEMBER 11 ERA

Having described the various functions of counterintelligence and organized them into a set of four essentially static *core competencies* that defines counterintelligence as a separate and unique discipline of intelligence, the task now is to delineate and assess the responsibilities of U.S. counterintelligence in order to determine whether or not it must be changed with regard to the threat environment that the U.S. currently faces. The precedent for reviewing counterintelligence responsibilities is based in part upon the ongoing debate concerning the Intelligence Community (IC) that is the result of the catastrophic attacks of September 11. The other reason counterintelligence responsibilities ought to be reassessed is the fundamental shift that occurred in the USG in the aftermath of September 11 with respect to its foreign and domestic policies. The primary aspect of this policy shift that directly concerns counterintelligence is the far greater attention that is generally being paid to the activities of hostile non-state actors and to transnational terrorists specifically. Although this policy shift has implications for counterintelligence in both the international and domestic arenas, the increased focus on domestic security issues within the U.S. suggests that domestic counterintelligence responsibilities must first be reassessed. This seems particularly true in light of the creation of the Department of Homeland Security (DHS), as well as the passing and implementation of the USA PATRIOT Act, both of which have domestic intelligence, and therefore counterintelligence, implications. Given this impetus, reassessing

counterintelligence responsibilities is quite appropriate. We will begin by outlining traditional counterintelligence responsibilities.

Modern American counterintelligence was established in order to combat the burgeoning threat of hostile intelligence activity being directed against the U.S. by various nation-states, which at the time of its inception, was primarily Germany. With World War II winding down and the Cold War just beginning, U.S. counterintelligence turned to focus its attention on the threat primarily coming from the Soviets and to a lesser extent on the intelligence services of the other communist states. Since the Soviet Union and her communist allies largely posed a military and/or a nuclear threat to the U.S., this was the focus of U.S. counterintelligence efforts as well. This paradigm would last up through the end of the Cold War. The post-Cold War period proved to be a transitional time for U.S. counterintelligence, whose almost singular focus on Russia gave way to a somewhat broader focus on a wider array of threats. The rise of terrorism in the 1970s and 1980s, which at the time was largely a state-sponsored phenomenon, gave counterintelligence an opportunity to broaden its horizons. From the time of the first Gulf War in Iraq in the early 1990s on, the hostile intelligence efforts of so-called ‘rogue nations’, such as North Korea or Iraq, came to dominate the efforts of U.S. intelligence in general and by extension counterintelligence as well. This period also saw an increasing focus on the threat of economic or industrial espionage coming from a variety of states, including other democratic and allied nations.⁷⁴

As can be seen from these examples, U.S. counterintelligence was organized principally as a way to confront the hostile intelligence efforts of other nations. Since the bulk of U.S. counterintelligence efforts have historically focused on countering the intelligence activities of communist and rogue nations, it would not be surprising to find that the relatively recent shift towards focusing counterintelligence against economic espionage, transnational (and non-state sponsored) terrorism, and international criminal enterprises have perhaps not had the same measure of success as these counterintelligence efforts have had against the more traditional, state-based intelligence adversaries. However, with the creation of a cabinet-level department that is tasked with preventing terrorist attacks on the American homeland as well as the loosening of

⁷⁴ For a more thorough discussion of this see the *Annual Report to Congress on Foreign Economic Espionage* series referred to earlier in this work.

restrictions on domestic intelligence collection as evidenced by the USA PATRIOT Act, the opportunity is ripe for U.S. counterintelligence to hone its skills in these areas as well.

Now that terrorism has been given such a high priority – it is effectively the FBI’s number one priority according to their own website⁷⁵ – U.S. counterintelligence might have the opportunity to devote a considerably greater amount of time and resources to aid domestic counterterrorism efforts. Nonetheless, in terms of its core functions and fundamental techniques, U.S. counterintelligence will likely have to change substantively little – if at all – to meet this threat. The only change that may be needed regards the “culture” of counterintelligence itself, something that does not necessarily lend itself to “imposed reform”. “Counterintelligence culture” is defined here as the distinct organizational behavior or the prevailing mindset of members within the counterintelligence community that essentially embodies the conventional wisdom of this unique intelligence discipline. The conventional wisdom of the counterintelligence community is simply that the threat to national security is primarily the intelligence services of other nations, which is essentially an outgrowth of its modern history. Thus, since U.S. counterintelligence has historically focused on targeting and thwarting the activities of state-based intelligence services, the shift in focus towards thwarting the activities of terrorists might be somewhat difficult to embed in the counterintelligence culture.

For example, it is unlikely that counterintelligence practitioners will give terrorists the same level of professional respect and credibility as they do state-based intelligence services. Likewise, they are even less likely to treat terrorists as a hostile intelligence threat in the same manner as foreign spies. The reasons these mindsets may be adopted are understandable. For one, terrorists are often accused of not behaving rationally or their activity is treated as merely being criminal. These perceptions may contribute to developing a false impression of terrorist activities as being unprofessional or incompetent, when this may in fact be untrue.⁷⁶ Assuming that they are treated as rational actors and more than just criminals, terrorists are often regarded as uneducated,

⁷⁵ For more information see: <http://www.fbi.gov/priorities/priorities.htm> [15 June 2003].

⁷⁶ Glazov, Jamie, “Symposium: Diagnosing Al-Qaeda,” *Frontpage Magazine*. 18 August 2003. Available [online]: <http://frontpagemag.com/articles/ReadArticle.asp?ID=9416> [20 August 2003]. This article provides a great discussion of the dangers of such a mindset towards terrorists.

lacking formal training, and as having limited resources. Some of these allegations are patently true, as both international terrorists and criminal organizations often do not have the resources, education or training as do the foreign intelligence service of a state. However, this line of reasoning still potentially discredits or underestimates terrorist capabilities.

Still another reason for this mentality is the fact that terrorist activities are not traditionally perceived as constituting a hostile intelligence threat like FIS activity that specifically targets U.S. secrets for collection. This statement, while grounded in truth, is perhaps misleading. Although the goals and aims of terrorists are quite different from that of states, which employ FIS to illicitly obtain sensitive U.S. information, terrorists nonetheless conduct intelligence collection to support their operations. Most terrorist intelligence collection could be categorized as employing open source methods; however some of their collection could also clearly be conducted in a covert manner as well. Pre-attack surveillance techniques are a good example of terrorist intelligence activity that is both open – as it must largely be conducted in open areas or public venues – and covert – wherein this activity is often disguised to make it appear as though it were innocuous in order to prevent discovery by an alert security apparatus. There is evidence to suggest too, that some terrorists employ clandestine techniques – primarily through the use of informants – to aid in their planning and conduct of terrorist attacks. The most recent example of this being the simultaneous attacks conducted by *Al-Qa'ida* in Saudi Arabia that apparently employed insider information, perhaps from within the Saudi National Guard itself, to facilitate their attacks against three western housing compounds in the vicinity of Riyadh.⁷⁷ Thus, counterintelligence as a culture may need to come to terms with respecting terrorist organizations on a professional level, particularly as evidence demonstrates that, while both international terrorists and criminal organizations do not necessarily pose a sophisticated intelligence threat of the same caliber as foreign intelligence services, they nonetheless pose a viable threat as a clandestine organization in general.

⁷⁷ Unattributed, "U.S. intelligence: Saudi military riddled by Al Qaida infiltrators", *World Tribune*. 14 May 2003. Available [online]: http://www.worthynews.com/zone.cgi?http://216.26.163.62/2003/ss_terror_05_14.html [20 May 2003].

Domestic counterintelligence is the one facet of U.S. counterintelligence that potentially needs the most consideration for reform. This is because it is within the domestic arena where counterintelligence and law enforcement responsibilities meet. In most instances the activities of terrorists and foreign spies are illegal, thus the responsibilities of law enforcement and counterintelligence coincide. But it is the techniques employed by counterintelligence and law enforcement that do not always coincide and thus friction occurs. Obviously, this is both an issue of operational practice and organizational structure, but this chapter will deal only with the former, not the latter. The organizational component to this argument will be dealt with in the following chapter.

The FBI is the lead agency responsible for dealing with hostile foreign intelligence activities conducted domestically inside the U.S. *Executive Order 12333* also allows other counterintelligence components to operate domestically, but since they nearly always operate under the auspices of the FBI the efforts of these components will largely not factor into this discussion.⁷⁸ Since the FBI has control over foreign counterintelligence (FCI) operations within the U.S. it should come as no surprise that its actions to combat hostile intelligence threats often employ law enforcement techniques. However, using law enforcement techniques when conducting a FCI operation – something perhaps antithetical to intelligence operations in general – may be somewhat problematic for at least several reasons.

For one, America is a democratic nation whose law enforcement agencies seek to bring criminals to justice through a due process of law that necessitates the use of restrictive legal procedures and rules of evidence in order to detain and prosecute a suspect without violating their rights.⁷⁹ Therefore being able to legally obtain and use evidence of criminal action or intent is of paramount importance yet may not be feasible when conducting an investigation against a foreign intelligence officer. This lack of

⁷⁸ U.S. President. *Executive Order*. “United States Intelligence Activities, Executive Order 12333,” Federal Register 46, no. 59941 (4 December 1981). Available [Online]: <http://www.fas.org/irp/offdocs/eo12333.htm> [20 February 2003]. [hereafter referred to as *EO12333*] However, the one notable (and frequent) exception to this rule of FBI as lead agency concerns the two military counterintelligence components that also serve the double-role of federal law enforcement agencies, the Air Force Office of Special Investigations (AFOSI) and the Naval Criminal Investigative Service (NCIS), who are given the lead over FCI operations along with arrest authority within the jurisdiction of their respective military facilities. See: Odom, 174.

feasibility may come in that the actual collection methods may not be considered legal or admissible in court. Yet, even if they were, the need to protect sources and methods of collection renders what is otherwise viable evidence unusable in most courts.⁸⁰

When considering the issue of using law enforcement agencies to conduct FCI operations the problem of organizational culture once again rises to the surface. Law enforcement as a distinct organizational culture is dominated by a criminal-catching, prosecution mindset that is in many ways incompatible with intelligence organizational culture.⁸¹ Whereas intelligence organizational culture, and particularly counterintelligence, thrives on secrecy, patience, and ambiguities, law enforcement prefers to categorize the world along clear-cut lines, where the “good guys” and the “bad guys” are a matter of black and white, not shades of gray.⁸² In terms of their general attitude and response with respect to the media, intelligence and law enforcement could hardly be more different. Where counterintelligence tends to shun publicity, law enforcement agencies appear to bask in the open coverage of their activities.⁸³ And finally, considering the intricate and convoluted nature of clandestine intelligence networks, the traditional law enforcement penchant for quick arrests is clearly counterproductive to developing a good understanding of adversary intelligence operations that require long term and painstakingly slow operations and investigations that stretch years at a time.⁸⁴

Based upon the evidence stated above, it would seem that law enforcement and counterintelligence are in fact incompatible. The limitations of certain techniques of law enforcement, from issues of admissibility of evidence to arrest authority, suggest that with regard to counterintelligence they obviously hamper the ability to employ the full range of options against adversary intelligence activity and perhaps terrorist activities as well. Whatever benefit was originally intended by establishing agencies that have the

⁷⁹ Hulnick, 101.

⁸⁰ *Ibid.*, 102

⁸¹ Hulnick, 101; Odom, 175; This is generally agreed upon by many within the intelligence community and noted as well among numerous authors writing on intelligence reform.

⁸² Godson, *Dirty Tricks or Trump Cards*, 75.

⁸³ Odom, 177.

⁸⁴ *Ibid.*, 178

dual-responsibilities of law enforcement and counterintelligence now appears to have been overridden by the disadvantages now arising from conflicts in both practice and culture between the two.

This assessment of counterintelligence has noticeably focused on the domestic aspects of U.S. counterintelligence seemingly neglecting counterintelligence activities abroad. The primary reason for this is because U.S. counterintelligence activity undertaken abroad is under the auspices of the CIA. Since the CIA does not have policing powers and because it is purely an intelligence organization, its foreign operations do not stir up the debate concerning law enforcement being meshed with counterintelligence. And since counterintelligence is essentially a specific kind of foreign intelligence endeavor⁸⁵ that is conducted abroad it is also sanctioned under *EO 12333*. This does not mean that the FBI and other federal law enforcement counterintelligence entities⁸⁶ do not have responsibility to conduct counterintelligence activities abroad, for they do. In fact, the FBI stations numerous special agents in embassies around the world as legal attaches whose geographic locations enable them to assist in counterintelligence operations conducted abroad.⁸⁷ The bottom line with counterintelligence activities abroad is that they do not substantially differ from counterintelligence conducted domestically except that they are free from many of the legal restrictions imposed on domestic counterintelligence organizations.

While some restrictions on intelligence collection directed against U.S. citizens apply overseas as well, intelligence oversight incidents occurring abroad rarely seem to get the same level of attention that problems involving combined law enforcement-counterintelligence endeavors in the domestic arena do.

The evidence presented demonstrates that the core competencies and basic functionalities of U.S. counterintelligence do not need to change regardless of the dynamic threat environment present today or the federal government's new policy focus

⁸⁵ U.S. Army, Regulation 381-12. *Subversion and Espionage Directed Against the U.S. Army (SAEDA)*. Washington, D.C., Department of the Army, (15 November 1993), 6. [hereafter referred to as *AR 381-12*].

⁸⁶ This specifically implies the DoD counterintelligence components with federal law enforcement powers, namely AFOSI and NCIS.

⁸⁷ Godson, *Dirty Tricks or Trump Cards*, 76. The CIA station chief in each embassy remains the principle authority over counterintelligence efforts conducted abroad, regardless of the presence of FBI legal attaches.

on terrorism. The only possible exception to this would be to take a closer look at counterintelligence analysis sources and methods to consider a greater inclusion of open source intelligence (OSINT), something that could be particularly useful as counterintelligence activities being conducted domestically appear to be increasing. However, this potential reform will be considered in the last chapter detailing the future of U.S. counterintelligence. In addition, counterintelligence culture may need to learn to embrace its new focus, as international terrorists and other hostile non-state actors may well prove to be as professional and dedicated foes as the traditional foreign intelligence services have been. Considering the complex issues inherent in the combination of law enforcement and counterintelligence responsibilities in the domestic arena U.S. counterintelligence must also decide whether or not it wants to change or leave this paradigm alone. In either case, whether separating counterintelligence from law enforcement or keeping the two combined, this problem and its potential solutions provides a segue to discussing the next most important aspect of counterintelligence reform, the structure of the counterintelligence community, which will be the subject of the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE COUNTERINTELLIGENCE COMMUNITY

A. INTRODUCTION

The analysis of counterintelligence up to this point has determined that while the threat environment may be changing this poses little challenge to U.S. counterintelligence, as counterintelligence is an essentially timeless function whose role and associated capabilities require only minimal reform to offset its deficiencies in practice. Therefore, the analysis must turn to focus on another aspect of this misunderstood discipline of intelligence, the structure of the U.S. counterintelligence community. The organizational design of the U.S. counterintelligence community has been chosen for analysis for a number of reasons. For one, organizational issues have repeatedly been the subject of discussion in terms of Intelligence Community reform, but have not often included counterintelligence. While this could be interpreted as meaning the U.S. counterintelligence community does not need restructuring, it suggests alternatively that reorganizing counterintelligence has merely been overlooked. Secondly, in spite of numerous government commissions that have recommended, among other things, to organizationally reform the IC, few if any of these recommendations have been implemented. However, there are two other factors that are really at the crux of the issue of why the U.S. counterintelligence community needs reorganization. The first of these factors concerns the ongoing debate over the organizational divide that exists between foreign and domestic counterintelligence operations. The second factor is linked to the first, in that it concerns the mixing of law enforcement and counterintelligence in the same organizations that conduct domestic counterintelligence operations. Each of these factors will be explained in further detail in the following paragraphs.

The issues concerning the foreign-domestic split and the law enforcement-counterintelligence overlap in many ways revolve around two federal agencies, the Central Intelligence Agency (CIA) and the Federal Bureau of Investigations (FBI), as they constitute the two principle U.S. counterintelligence agencies. The primacy of both agencies is seen in the FBI's role as the lead domestic counterintelligence agency and the CIA as the lead agency for counterintelligence conducted abroad. It is not surprising,

then, that problems of the foreign-domestic divide and the law enforcement-counterintelligence overlap have most noticeably emerged at this organizational intersection. However, regardless of the primacy of either agency, the counterintelligence organizations of the armed forces must be included in this discussion as well. Since these military counterintelligence organizations also have an operational role in conducting counterintelligence both domestically and abroad it is imperative they be included in any discussion involving community-wide organizational reforms. It should be noted at this point that the counterintelligence community is a much broader array of organizations than may be apparent. Rather than a small community made up of a few national level agencies, the counterintelligence community is really a mix of various offices, departments and agencies that are spread all throughout the federal government. Therefore, the reality is that the foreign-domestic divide and the organizational overlap of counterintelligence and law enforcement affect more than just the CIA and FBI. In fact, problems of counterintelligence are problems that will undoubtedly, if left unchecked, negatively impact every organization within the IC. Incidents such as the penetration of the Defense Intelligence Agency by a Cuban agent or the compromise of U.S. nuclear weapons information from the Department of Energy's Los Alamos lab demonstrate this point.⁸⁸ This is not to say that these specific incidents were necessarily counterintelligence failures caused substantially by organizational issues. Rather these counterintelligence failures clearly illustrate that counterintelligence is a community-wide endeavor, one whose failings will not necessarily be solved by addressing the problems found between one or two agencies.

As outlined in the first chapter the attacks of September 11, 2001 have catapulted the issues of Intelligence Community reform to the forefront yet with a discussion of counterintelligence noticeably lacking. Yet, as we have noted, the 9/11 attacks are symptomatic of a much older and obviously unresolved issue in the Intelligence Community, the foreign-domestic divide. This longstanding problem, and the associated problem of combining law enforcement and counterintelligence responsibilities under

⁸⁸ For more information on these specific incidents refer to the Wen Ho Lee Affidavit, ____, and the Ana Bellen Montes Avidit and Indictment. Two internet sites are particularly helpful in researching thies specific incidents as they have both compiled a variety of related documents and new articles on these cases (and others): the Federation of American Scientists (FAS), <http://www.fas.org/> and the CI Centre, <http://www.cicentre.com/>

one agency, harkens back to the earliest efforts to organize modern American intelligence and counterintelligence during the World War II era. It was immediately prior to WWII, in 1939 when President Franklin Delano Roosevelt gave the FBI the primary responsibility for counterespionage.⁸⁹ About two years later, FDR gave William Donovan, as head of the precursor organization to the CIA, the Office of Strategic Services (OSS), the responsibility for coordinating “...all forms [of] intelligence including offensive operations...”, which meant both “positive” and counterintelligence operations that were to be conducted abroad.⁹⁰ It appears that FDR may have arbitrarily, for political reasons, doled out the specific responsibilities each agency would have. Unfortunately, the problems that this piecemeal approach to organizing U.S. intelligence created have persisted up to the present day, particularly where it concerns counterintelligence.⁹¹ Therefore this analysis is not only necessary, it is long overdue.

However, before addressing the above issues and in order to frame this analysis of the counterintelligence community in the proper light, a discussion of how counterintelligence benefits from strict control over its operations is imperative. Thus, the next section will deal directly with the pertinence of centralizing U.S. counterintelligence operations. Following this discussion, the next sections will outline the various organizations that make up the U.S. counterintelligence community along with the overall community structure.

B. CI OPERATIONS REQUIRE CENTRALIZATION

Counterintelligence, in order to be successfully carried out, requires strong central control. Centralizing counterintelligence is predicated on the need to maintain both secrecy and security in counterintelligence operations. Counterintelligence operations seek to penetrate adversary organizations – and with regard to foreign intelligence services this means penetrating their intelligence network – in the hopes of learning the adversary’s capabilities, intentions, and most importantly what the adversary knows about U.S. intelligence operations. As is perhaps obvious, the value in penetrating an

⁸⁹ Persico, 17 & 35.

⁹⁰ *Ibid.*, 91.

⁹¹ Persico, 16,

adversary's organization, and especially its secret operations, is that it allows U.S. counterintelligence to gain an insider perspective into the enemy's operations, providing the most reliable means of determining the adversary's capabilities and intentions.⁹² However, the greater value of counterintelligence operations is not that they provide knowledge about an adversary so much as they provide leverage over that adversary. Secret knowledge of what an adversary secretly knows about U.S. intelligence operations is that leverage.

This concept is somewhat convoluted and perhaps requires some further explanation. So, when an adversary is unaware that U.S. counterintelligence knows what the adversary secretly knows about U.S. intelligence, this gives counterintelligence an advantage over the adversary, in terms of manipulating them. If this adversary is indeed ignorant of the penetration they are very susceptible to deception and manipulation, as U.S. counterintelligence can selectively feed them intelligence that will play to the adversary's bias and knowledge of U.S. intelligence. Over time, U.S. counterintelligence can use this conduit to sow disinformation in an attempt to influence or secretly manipulate the adversary's actions in a way more favorable to U.S. interests.⁹³ However, this leverage although undeniably advantageous, is quite fragile and perishable because it is only remains an advantage when this knowledge is kept secret from the adversary. This is where security becomes relevant to counterintelligence.

Security in counterintelligence operations is primarily achieved by restricting the dissemination of knowledge concerning these most-secret of operations. However, it should be mentioned too that restricting dissemination of operational information is not a measure solely employed to protect counterintelligence operations; this is a recognized standard practice for protecting intelligence operations of all sorts. This means that counterintelligence must limit access to the details of CI operations to those personnel who have a demonstrably imperative need to know. The protection this affords is obvious: the fewer people who know, the fewer opportunities for these operations to be compromised. It is upon this principle of compartmentalization, also referred to as "need to know", where centralization of operations finds its basis. The potential for the

⁹² Felix, 121.

⁹³ *Ibid.*

inadvertent (or intentional) compromise of sensitive intelligence sources, in this case a counterintelligence penetration, is significantly lessened if an organization can maintain strict control over their operations. This is most easily achieved by centralizing these kinds of operations under one organization that has a very narrow and vertical chain of command.

The intent of this section was to show the crucial need to maintain both secrecy and security of current and future counterintelligence operations. It is obvious that this particular approach singularly highlighted the merits of centralization. However, in order to demonstrate the benefits of centralization more fully, an assessment of how U.S. counterintelligence is left vulnerable by its current structure is needed. Before this analysis can be conducted, the U.S. counterintelligence community must first be outlined.

C. THE KEY PLAYERS & SUPPORT ORGANIZATIONS

1. The Five Key Players

More than all the others, two organizations in particular dominate U.S. counterintelligence: the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA). Along with these two, the Department of Defense counterintelligence components are the only other organizations that conduct counterintelligence operations.⁹⁴ While the FBI and the CIA are easily the most recognizable components – and therefore historically the most dominate forces within the counterintelligence community – the Department of Defense is the next most visible contributor to U.S. counterintelligence as it hosts three counterintelligence organizations: the Air Force’s Office of Special Investigations (AFOSI), the Army’s counterintelligence branch under the Intelligence and Security Command (INSCOM), and the Navy’s Criminal Investigative Service (NCIS). Despite the noticeable and important role that these five organizations play they only constitute the operational core of the U.S. counterintelligence community. In fact, the community is a much broader and more diverse conglomeration of organizations that largely fulfill a non-operational support role to U.S. counterintelligence efforts both abroad and domestically.

⁹⁴ Godson, *Counterintelligence*, 35.

2. CI Support Organizations

These support organizations, which all have counterintelligence responsibilities of varying types and degrees, can be broken down into two general categories: *direct support* and *indirect support* organizations. *Direct support* organizations are defined here as those organizations that support the counterintelligence community through their policymaking functions or those organizations, which by virtue of their position, provide unique counterintelligence support to the greater Intelligence Community. Foremost among the direct support organizations is the Office of the National Counterintelligence Executive (NCIX), which serves as the primary interagency steering group. This organization was set up under the Clinton Administration to provide coordinated, national-level, strategic direction and policy guidance to the various components of the U.S. counterintelligence community.⁹⁵ As such NCIX is responsible for developing the *National Threat Identification and Prioritization Assessment* and the *National Counterintelligence Strategy*, by leveraging the expertise of both the private and public sectors, in order to promulgate these guiding documents to the various members of the counterintelligence community.⁹⁶ NCIX is staffed by members from the following organizations: the CIA and FBI; the Departments of Defense, State, Energy, and Justice; along with representatives from the Joint Chiefs of Staff (JCS) and the National Security Council. Together these organizations also make up the National Counterintelligence Policy Board.⁹⁷ The National Counterintelligence Board of Directors that is chaired by the Director of the FBI and is made up of the Deputy Secretary of Defense, the Deputy Director of the CIA, and a senior Department of Justice representative oversees NCIX.⁹⁸

⁹⁵ White House fact sheet - *The PDD on CI-21: Counterintelligence for the 21st Century*. Available [online]: <http://www.fas.org/irp/offdocs/pdd/pdd-75.htm>. [hereafter referred to as *The PDD on CI-21: Counterintelligence for the 21st Century*]. NCIX came into existence during the Clinton Administration in January 2001 via Presidential Decision Directive (PDD) 75 effectively absorbing the responsibilities of its predecessor organization, the National Counterintelligence Center (NACIC). The bulk of the information available on NCIX is located on its homepage on the internet: <http://www.ncix.gov/>

⁹⁶ *Ibid.*

⁹⁷ *Ibid.*

⁹⁸ *Ibid.*

There are three other organizations that clearly fall into this direct support category as well, the Department of Energy (DOE), the Department of State, and the National Security Agency (NSA). Each of these organizations is listed as being among the 15 organizations that make up the Intelligence Community (IC),⁹⁹ further substantiating their role as counterintelligence *direct support* organizations is the fact that each of these organizations is also a part of the National Counterintelligence Policy Board.¹⁰⁰ The Department of Energy's Office of Counterintelligence is the primary office charged with protecting America's nuclear secrets.¹⁰¹ Its most important duty is to maintain security through access control and to provide investigative support to the operational counterintelligence components, which is primarily the FBI, in the event that sensitive nuclear information is compromised.¹⁰²

The U.S. State Department's specific role in this endeavor, in addition to being one of the IC members that make up the staff of NCIX, is to supply policy oversight and coordination with the other 14 members of the Intelligence Community on counterintelligence issues.¹⁰³ The State Department additionally contributes to U.S. counterintelligence efforts by way of its Bureau for Diplomatic Security, otherwise known as the Diplomatic Security Service. The Diplomatic Security Service is responsible for Visa and Passport control, and therefore fraud investigations, a tool that has been instrumental in identifying suppliers of false documentation to numerous entities hostile to the U.S.¹⁰⁴

The National Security Agency also maintains an Office of Counterintelligence that is directly responsible for identifying and minimizing threats to the U.S. Signals

⁹⁹ U.S. Central Intelligence Agency, *A Consumer's Guide to Intelligence*. (Washington D.C.: Office of Public Affairs, 2002), 32.

¹⁰⁰ *The PDD on CI-21: Counterintelligence for the 21st Century*.

¹⁰¹ U.S. Department of Energy. *Department of Energy (DOE) FY2001 Presidential Budget Request for the Office of Counterintelligence*. (Washington D.C.: GPO, 2001). Available [online]: www.cfo.doe.gov/budget/01budget/_otherdef/counter/counter.pdf. The DOE's Office of Counterintelligence was only recently established in February 1998 as a result of Presidential Decision Directive (PDD) 61 which set counterintelligence apart as an independent office that reports directly to the Secretary of Energy.

¹⁰² See: DOE's Chicago Operations Office for Counterintelligence webpage: http://www.ch.doe.gov/insidech/org_offices/oci/WhatWeDo/index.htm

¹⁰³ *A Consumer's Guide to Intelligence*, 19.

¹⁰⁴ The Diplomatic Security Service webpage describes this nicely, see: <http://www.state.gov/m/ds/>

Intelligence (SIGINT) community. In keeping with this role, the NSA has been designated by presidential directive to act as the executive agent for interagency Operational Security (OPSEC) training to ensure the safety and security of all forms of government related information not classified or otherwise restricted.¹⁰⁵ As such, the NSA maintains and oversees the work of the Interagency OPSEC Support Staff (IOSS) that is staffed by members from the NSA, CIA, FBI, DoD, and even the General Services Administration.¹⁰⁶ In addition to these roles and responsibilities, the NSA is also a leading provider of intelligence specifically used by the counterintelligence community to identify hostile intelligence efforts being conducted against U.S. interests, such as noted by the now-declassified VENONA program.¹⁰⁷

Another office is found within DoD's Defense Intelligence Agency (DIA), the Counterintelligence and Security Activity, which, as a subordinate office of the Directorate of Administration (DA), "...serves as the focal point for issues on counterintelligence and for assessments of the threat posed by foreign intelligence activities".¹⁰⁸ In addition to this office, the Defense Security Service, responsible for conducting personal security investigations, has been set up as a way to free the other operational DoD counterintelligence entities from the burden of personnel screening and background checks, which although clearly an essential task, is quite resource intensive.

Indirect support organizations are any other national level government organizations that maintain an office specifically dedicated to counterintelligence and those that directly interface with other national level counterintelligence agencies, which would primarily be the FBI, on counterintelligence investigative matters.¹⁰⁹ Although many of these would likely be considered "minor contributors" among the major players

¹⁰⁵ The information was derived from the website of the IOSS and can be found at the following link: <http://www.ioass.gov/html/about.htm>

¹⁰⁶ *Ibid.*

¹⁰⁷ Robert Louis Benson and Michael Warner. eds., *VENONA: Soviet Espionage and the American Response 1939-1957*. (Washington D.C.: Government Printing Office, 1996.), xix.

¹⁰⁸ This quote comes from the website of "the United States Intelligence Community" which appears to be an official IC overview and guide set up and maintained by the CIA. The quote is found on the page entitled: *Organization of the Defense Intelligence Agency* available [online]: http://www.intelligence.gov/1-members_dia_org.shtml

¹⁰⁹ *EO12333* specifically outlines the responsibility for the IC member organizations other than the CIA to liaise and coordinate their counterintelligence investigation matters with the FBI. Further research reveals that all the counterintelligence offices of these other CI organizations, some of which are non-IC organizations, defer to the FBI in accordance with the stipulations put forth in *EO12333*.

in the counterintelligence community, the support they provide nonetheless helps ensure the security of sensitive U.S. programs, information and technologies. Although many offices, departments and agencies could well fit under this rubric, the following list of organizations provides a representative sample.

One example is the NRO, which is the United States' lead agency in developing, operating and maintaining its diverse array of reconnaissance satellites. This office provides support to the counterintelligence community through its Office of Counterintelligence by identifying information, technology and programs potentially at risk from foreign intelligence with respect to U.S. satellite reconnaissance capabilities.¹¹⁰ The recent case of Brian Regan demonstrates the extremely important role that the NRO's Office of Counterintelligence plays in protecting one critical portion of America's sensitive reconnaissance operations (SRO). Regan, a retired Air Force Master Sergeant and former NRO employee, was convicted of conspiracy to commit espionage on behalf of China and Iraq after he removed over 20,000 pages of classified documents from an NRO office.¹¹¹ Another example is the National Imagery and Mapping Agency¹¹² (NIMA) that is the leading provider of imagery intelligence (IMINT) and cartographic support to the USG and IC writ large. NIMA also provides support to the counterintelligence community especially in terms of assisting domestic law enforcement and counterterrorism efforts, albeit on a very limited basis.¹¹³ Interestingly, while the Department of Homeland Security is certainly an indirect supporter of the counterintelligence community by virtue of its position as the central "clearing house" for domestic intelligence analysis particularly via its Information Analysis and Infrastructure Protection (IAIP) section, counterintelligence is not listed among its responsibilities, nor does there appear to be an office devoted to counterintelligence liaison.¹¹⁴ Other

¹¹⁰ For more information see their website: <http://www.nro.gov/index1.html>

¹¹¹ Jerry Markon, "Spy buried secret data stashes in state parks," *The Washington Post*. 31 July 2003. Available [online]: <http://www.azcentral.com/news/articles/0731spy31.html> [01 August 2003].

¹¹² NIMA is in the process of having its name officially changed through Congress to the National Geospatial-Intelligence Agency (NGA) to reflect its leading role in the development of an ostensibly new-found intelligence discipline of geospatial intelligence.

¹¹³ This is as stated on their website with respect to NIMA support to government customers, see: <http://www.nima.mil/ocrm/nima/govt.html>

¹¹⁴ The organizational chart provided by DHS as well as all of the publicly available information on

examples of organizations that provide indirect support to U.S. counterintelligence include the Defense Threat Reduction Agency, The Coast Guard Investigative Service, and the U.S. Treasury Department. Each of these organizations has a responsibility to coordinate, liaise or in the case of the CGIS, conduct preliminary investigations of a counterintelligence nature while informing the FBI and other appropriate counterintelligence organizations in order to maintain national level involvement on cases deemed of value by these agencies. Organizations such as these that provide indirect support to the CI form the outer layer of the U.S. counterintelligence community.

D. OUTLINING THE COMMUNITY STRUCTURE

Merely listing the organizations involved in CI may suggest a counterintelligence capability that needs little restructuring. However, given the importance of centralization, when one considers the fact that few of the different organizations that make up the counterintelligence community are formally connected to one another, one can be sure that community structure needs reassessing. It would be useful at this point to look at a couple of organizational diagrams that depict the general structure of the counterintelligence community. These two diagrams, *Figure 1* and *Figure 2* show two different representations of the various organizations and structuring of authority, as they currently exist within the counterintelligence community:

DHS suggests that no role with respect to counterintelligence was ever specifically considered for the Department of Homeland Security. However it still seems reasonable to assess that DHS would provide an indirect role in supporting U.S. CI by virtue of its intelligence analysis and production that focuses on domestic terrorism, something that would be of interest to CI officers and therefore very likely passed on to them.

Figure 1. -- Major Components of the U.S. CI Community

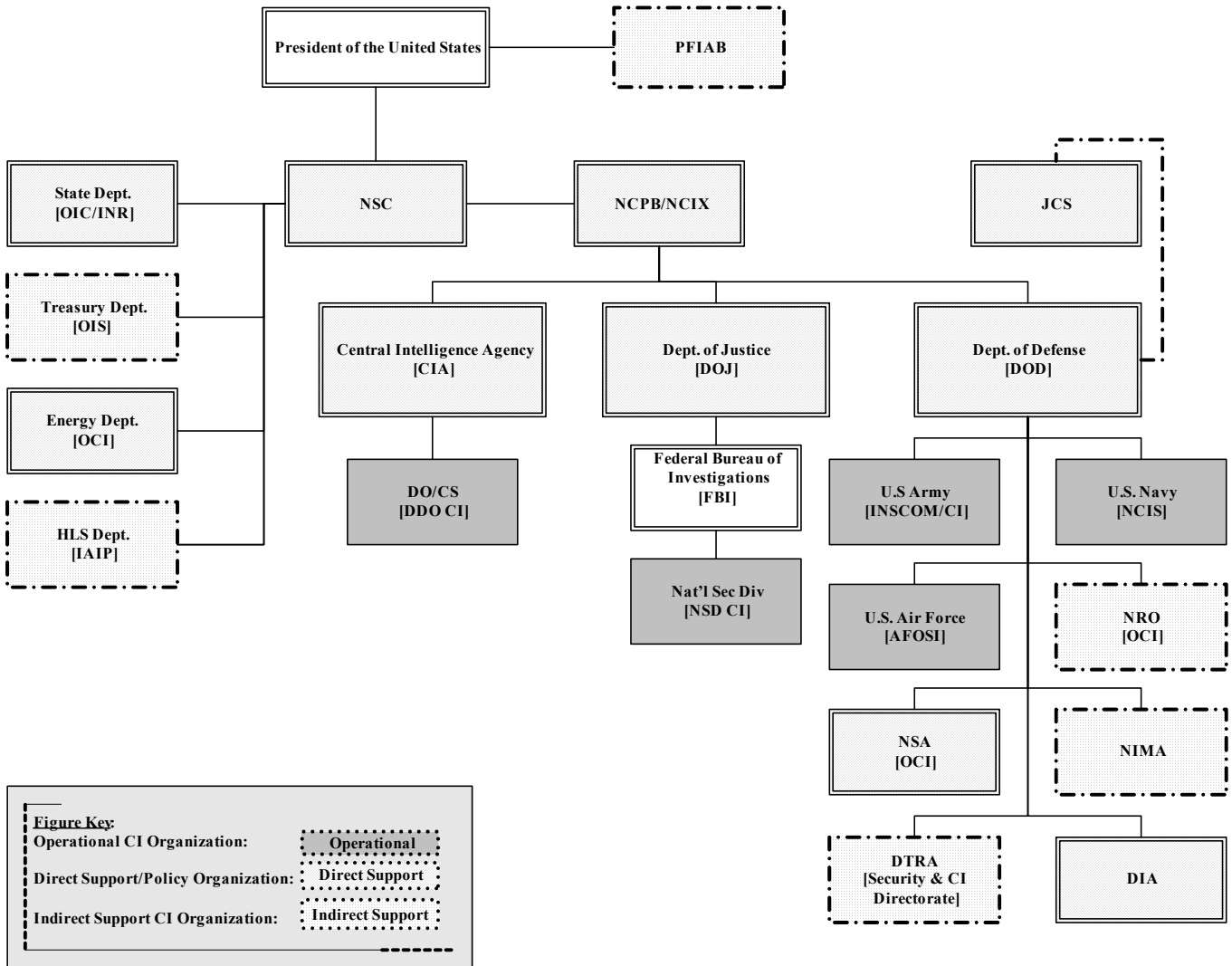


Figure 1. Major Components of U.S. CI Community.

Figure 2. -- Executive U.S. CI Structure [PDD-75]

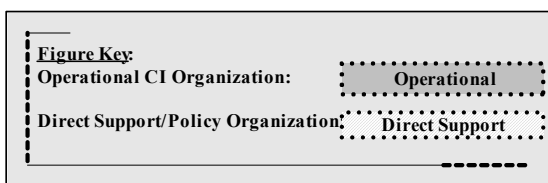
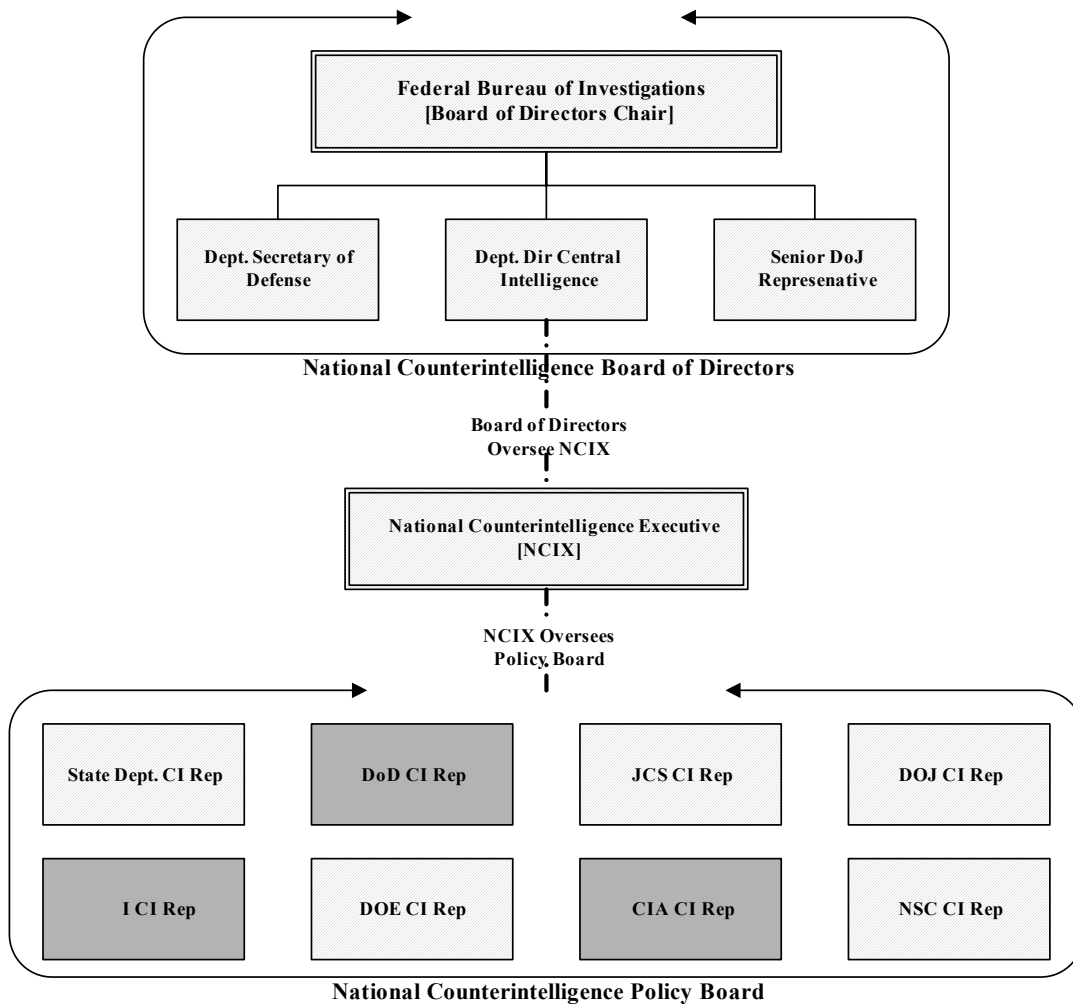


Figure 2. Executive U.S. CI Organization [PDD-75].

A couple of observations are in order about these two diagrams:

1. Overall Decentralization

Figure 1 shows the numerous organizations that constitute the U.S. counterintelligence community, which includes the operational, direct support and indirect support counterintelligence organizations. *Figure 1* suggests a decentralized counterintelligence community. That the U.S. counterintelligence community is decentralized is not really surprising, as it merely reflects the overall decentralization of the Intelligence Community. However, it is this decentralization that is the core problem U.S. in counterintelligence.

As a consequence of this decentralization, U.S. counterintelligence appears to be a disparate grouping of cabinet-level departments, independent agencies and “offices of counterintelligence” housed in various organizations which share few, if any, formal ties to one another. The Department of Defense illustrates this point well as it does not legally or structurally fall under the authority of either the FBI or CIA.¹¹⁵ And, except where the operations of the DoD counterintelligence components – that is, NCIS, AFOSI, or Army CI – cross over into the specific “jurisdiction” of either the FBI in domestic settings or the CIA in foreign settings, these service-specific assets are operationally under the control of their individual armed service command structures. Even internally the DoD counterintelligence apparatus is decentralized with the individual service counterintelligence components almost completely disconnected. Primarily this is because the counterintelligence services of each of the individual military branches are beholden to no one save their parent service – and since at least two of these counterintelligence organizations are “outside the chain of command”¹¹⁶ and directly

¹¹⁵ The organizational diagram showing the Department of Defense underneath or subordinate to the FBI & CIA is merely illustrative of the relative subordination and coordination of strategic, foreign or domestic level operations that involve cooperation and liaison with one of the two agencies.

¹¹⁶ Both the Air Force Office of Special Investigations (AFOSI) and the Navy’s Criminal Investigative Service (NCIS) are outside the normal operational forces chain of command, each one operating as unique

answerable only to the secretaries of their respective services, this makes the connection between these disparate entities all the more tenuous.

2. Centralized Executive Authority

In fact looking at the executive-level decision making component of the U.S. counterintelligence community found in *Figure 2* reveals an organizational design that is in direct contrast to that shown in *Figure 1*. *Figure 2* differs in that it depicts U.S. counterintelligence in a seemingly more centralized arrangement than the overall community appears to be when looking at it in *Figure 1*. This diagram reflects the USG attempts under the Clinton administration to reform U.S. counterintelligence in response to a number of embarrassing and very damaging espionage cases that surfaced in the 1990's, the most notable of these cases being the betrayal of two counterintelligence officers, Aldrich Ames (CIA), and Robert Hanssen (FBI), on behalf of the Russian intelligence services.¹¹⁷ This reform is embodied in the Presidential Decision Directive 75 (PDD-75), which created the aforementioned NCIX in May 2001.¹¹⁸ In an effort to give the NCIX more legitimate control of the community, PDD-75 requires NCIX to make efforts to centralize the budgeting issues within the community by "...working with the DCI's Community Management Staff", to "...review, evaluate, and coordinate the integration of CI budget and resource plans of, initially, the DOD, CIA and FBI".¹¹⁹ However, it is uncertain if this coordination really amounts to actual control over the budget of each of the various operational components mentioned.

The extent of control that NCIX has over any one organization or group of organizations within the counterintelligence community is hard to determine. Although NCIX was set up to serve as the focal point in the community for guidance and direction, it only has the power to publish the national strategy. The limits of NCIX control over the

and independent service who answers to their respective service secretaries. Interestingly, both of these organizations are also distinct and separate from the main intelligence component of their respective services.

¹¹⁷ The Honorable Richard Shelby, "Intelligence and Espionage in the 21st Century", *Heritage Lectures*, no. 705, (18 May 2001): 2, 3-5. Available [online]: <http://www.heritage.org/Research/NationalSecurity/HL705.cfm> [10 August 2003].

¹¹⁸ *The PDD on CI-21: Counterintelligence for the 21st Century*.

¹¹⁹ *Ibid.*

budget for counterintelligence and the fact that it is not given operational control over any of the agencies, specifically those conducting CI operations, leaves one wondering if NCIX has much influence or provides real leadership beyond writing strategy and policy documents for the community. However, the fact that this high-level and well placed organization even exists, means that the counterintelligence community potentially has a ready made central authority that need only be given the operational and budgetary control it requires in order to exercise this essential power.

E. HIGHLIGHTING THE FLAWS IN DESIGN

This section will now focus on the flaws in this decentralized community design. The problems of this decentralization organization arise from its foreign-domestic split, the unnecessary overlap among a multiplicity of organizations, and the placement of domestic counterintelligence operations in federal law enforcement agencies. In order to demonstrate the flaws in the current CI organization, a third organizational diagram has been provided. In fact, this third organizational diagram, *Figure 3*, is arguably the most important of the different graphic depictions of the community in that it represents how the operational arm of U.S. counterintelligence is organized. More than anything else *Figure 3* demonstrates a simultaneous structural divide and operational overlap in the organization of the operational counterintelligence components. Directly following this diagram are three separate sections that analyze the problems to structuring U.S. counterintelligence in this fashion.

Figure 3. -- Structural Divide & Overlap in U.S. Operational CI Organization

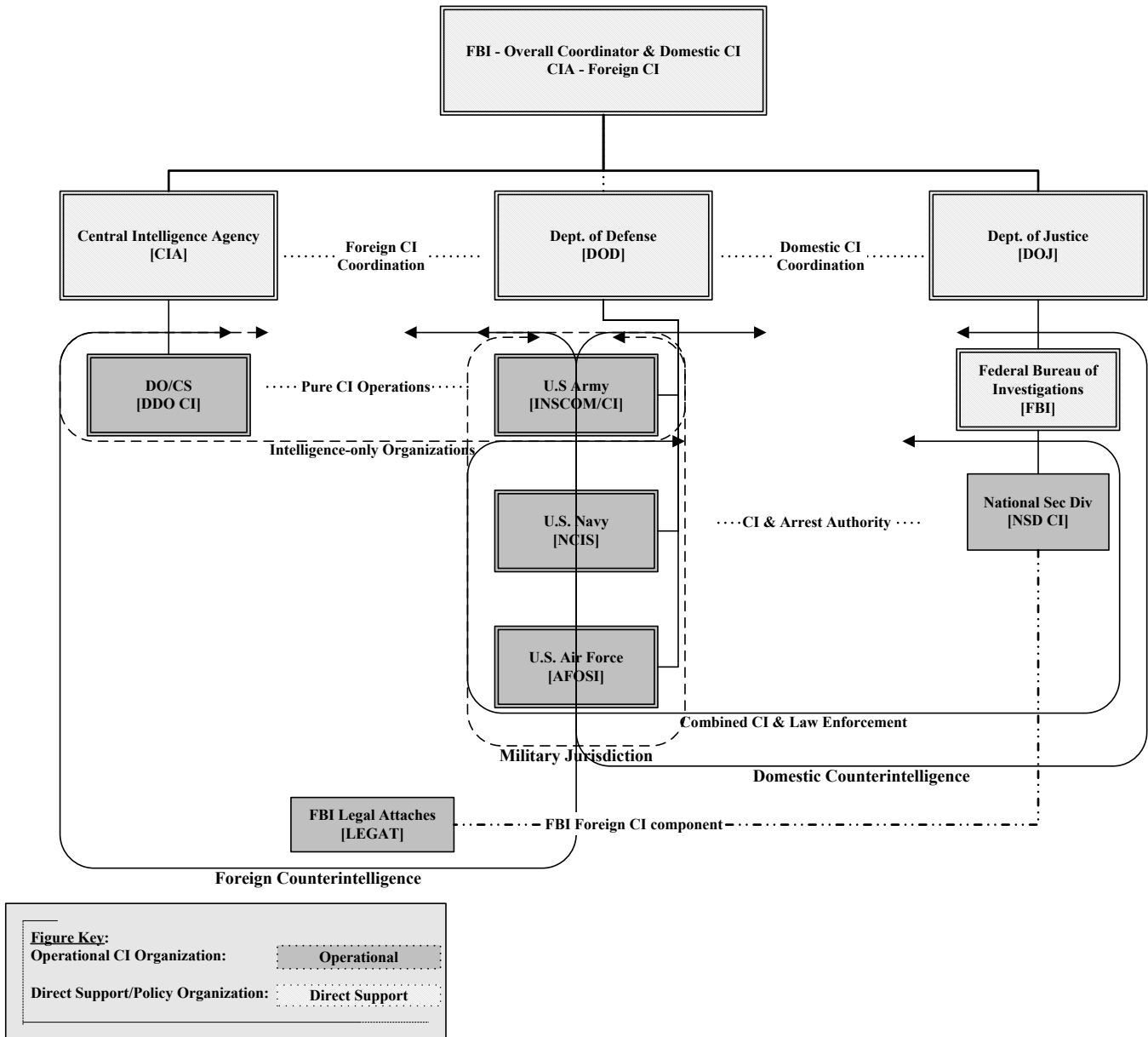


Figure 3. Structural Divide and Operational Overlap in CI Organizations

1. The Foreign-Domestic Divide

The structural divide in counterintelligence is the organizational outgrowth of the often-debated concepts of U.S. intelligence practices: the distinction made, on the one hand, between foreign and domestic intelligence operations and, on the other, between law enforcement operations and intelligence operations. The primary reason the conceptual and operational distinctions are made is to protect the civil liberties of the American public. Thus, the rules that govern the conduct of domestic security (law enforcement) and foreign intelligence operations are different. Essentially these rules concern the employment of intrusive means of detection or surveillance to monitor persons suspected of posing a threat along with the use of certain methods of attaining information (or evidence) in the course of conducting criminal investigations or during intelligence gathering operations. And, although in many cases the tactics, techniques and procedures employed by both law enforcement and intelligence could well be the same, the fact is the U.S. has decided it is unwilling to do to its own citizens what it is willing to do to foreigners.

Taking this discussion one step further, it is worth noting that some of these methods, when employed in one kind of operation may in fact be ineffective, antithetical, or even illegal if utilized during a different type of operation.¹²⁰ Among others, *intelligence collection* and *arrest authority* are salient examples of methods whose employment may work and are legitimate in one kind of operation, but are neither legal nor effective in another. For example, while the ability to monitor and arrest an individual conducting espionage within the U.S. is both a legal and an effective means for the FBI to thwart hostile intelligence activities domestically, the same rules and means to thwart this kind of activity do not necessarily apply to the CIA.¹²¹ Likewise, the tactics employed by the CIA overseas do not necessarily translate easily to the FBI. This is because the actions of the CIA are limited by the scope of their mission: (1) to gather foreign intelligence abroad, (2) to conduct counterintelligence operations abroad in order to protect the U.S. and perhaps surprisingly, (3) to conduct counterintelligence operations

¹²⁰ Odom, 174.

¹²¹ *EO12333*, 1.8 (a) & (c).

domestically to protect themselves.¹²² In addition to this, the CIA is given more latitude in its intelligence collections means, some of which may be antithetical (i.e. breaking laws of foreign countries in order to gather intelligence) as well as illegal to the law enforcement mission of the FBI.¹²³

This discussion of the differences in tactics and techniques between law enforcement and intelligence agencies highlights the American predilection for guaranteeing the rights of its citizens through the constitutional system of checks and balances and a separation of powers; this is especially important when considering the government's control of its security and intelligence services. In practical terms this separation is meant to mitigate the potential for the federal government to create a so-called "counterintelligence state", a situation in which the state uses its intelligence and security apparatuses as the primary means to repress its citizens and to quash dissent.¹²⁴ Given America's open, democratic society that is allowed through debate to question the policies of the federal government, the chance for this kind of abuse of power is unlikely. However, some would dispute this claim, arguing that in the aftermath of September 11 we have experienced an increase in government secrecy, a broader expansion of surveillance and intelligence gathering powers, and an erosion of checks and balances, particularly between the Legislative [Congress] and the Executive Branches of government.¹²⁵ Regardless of whether or not one agrees that the U.S. government is steadily gaining more latitude with respect to employing the intelligence domestically, the fact remains that limiting the control any one branch of government (or any one agency's) has over intelligence has been the primary motivation for dividing U.S. intelligence into many parts.

¹²² It may surprise some to learn this fact, as the CIA is generally understood to have no charter or authority to conduct intelligence operations domestically. These domestic counterintelligence operations are done to safeguard both CIA facilities and personnel within the U.S. However, these operations are not conducted unilaterally, but rather through coordination with the FBI.

¹²³ *Ibid.*, 1.8 (a), 1.14(a)-(e).

¹²⁴ J. Michael Waller, *Secret Empire: The KGB in Russia Today*. (Boulder: Westview Press, 1994), 13; while this specific usage of the notion of a "counterintelligence state" is taken from Waller's work, it seems that the Russians actually coined this term where it first appears in the work by John J. Dziak, *Chekisty: A History of the KGB*. (Lexington: Lexington Books, 1988).

¹²⁵ A report that does a fine job of outlining the five major areas where basic U.S. citizen rights are ostensibly being eroded as a consequence of 9/11 and the subsequent War on Terror is entitled: *Imbalance of Powers: How Changes to U.S. Law & Policy Since 9/11 Erode Human Rights and Civil Liberties*. (Washington D.C.: Lawyers Committee for Human Rights, 2003),

This division to limit control is clearly visible within the counterintelligence community. The organizational separation of the operational entities along the lines of foreign and domestic operations is the most visible aspect of this fact. Another, perhaps less obvious aspect of the attempt to limit control over U.S. intelligence assets is the operational overlap of law enforcement and counterintelligence. The first facet concerns the distinction made between foreign versus domestic intelligence collection, wherein the CIA as the leading foreign intelligence service is barred from operating against U.S. persons inside the United States except with the strict approval and coordination of the FBI.¹²⁶ It is precisely these two facets of the decentralized design of U.S. counterintelligence that should be reconsidered in light of the persistent issues and problems that this has created.

Ultimately, this concept of dividing intelligence capabilities between foreign and domestic organizations, essentially led to the creation of a counterintelligence community that is not only decentralized, it is “stove piped,”¹²⁷ and lacks good communication and cooperation. For example, in practice this foreign-domestic distinction, and its subsequent organizational separation, necessitates a “hand-off” be made between the CIA and FBI¹²⁸ when an intelligence or counterintelligence operation transitions from a foreign to a domestic setting. And unless tight coordination is maintained between the two organizations during this crucial phase it seems that this structural design has a limited utility particularly when dealing with transnational threats. A recent example of this kind of situation is found in looking at the case of the September 11 attacks. Although this case concerns counterterrorist and human intelligence operations specifically, this example is still quite useful since the tactics, techniques and procedures are essentially the same for counterintelligence activity involving human source operations. The recently released *Report of the Joint Inquiry into the attacks of September 11, 2001* notes that both the CIA and the FBI had identified and tracked individuals who would ultimately participate in the group of 19 hijackers who flew commercial airliners

¹²⁶ EO12333.

¹²⁷ For a good discussion of this notion of “intelligence pipelines” and the problem of “stove piped” intelligence, see: Lowenthal, 58.

¹²⁸ Making “hand off’s” of terrorist or hostile intelligence collector information must be made between all operational counterintelligence components, this includes the armed service counterintelligence organizations as well.

into the World Trade Center towers and the Pentagon on September 11.¹²⁹ The CIA, for its part had identified two of the *Al-Qa'ida* operatives Khalid Al-Mihdhar and Nawaf Al-Hazmi, and tracked them to Malaysia where they ostensibly met with other *Al-Qa'ida* members in January 2000 to discuss plans for the September 11 attacks.¹³⁰ However, once these individuals left Malaysia and entered the U.S., the CIA failed to notify the FBI of the arrival of two foreigners suspected of having ties to international terrorists. The CIA also failed to place their names on any of the various terrorism watch lists that it should have.¹³¹ The FBI likewise had an opportunity to share crucial information with the CIA and failed to do so. Not only had the FBI run a long-time informant who ended up becoming the roommate of both Al-Mihdhar and Al-Hazmi, but FBI agents had also identified an individual named Omar Al-Bayoumi, who was supporting the activities of the two soon-to-be hijackers, someone suspected of being a clandestine intelligence officer for the Saudi Arabian government.¹³² However, the FBI did not give either of these crucial pieces of intelligence to the CIA. As a result of the lack of solid communication, both agencies failed to conduct a seamless “hand off”. This failure contributed to and facilitated the surprise attacks on September 11, 2001.

2. Unnecessary Overlap

This second section deals with the problem of overlap as a consequence of the U.S. counterintelligence community’s decentralized structure. This particular problem has a couple of manifestations, the first of which is a logical byproduct of the foreign-domestic split wherein the FBI, a federal law enforcement agency, was given responsibility for domestic counterintelligence. This combines two very distinct functions in one organization: law enforcement and counterintelligence. The second section covers another facet of this overlap, the potential for duplication of efforts and decreased

¹²⁹ U.S. Congress, Senate and House. Permanent/Select Committees on Intelligence. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 with additional views*. 107th Cong., 2d sess., 2002 [hereafter referred to as *Report of the Joint Inquiry*, pp.#].

¹³⁰ *Ibid.*, 12-13.

¹³¹ *Ibid.*, 13.

¹³² *Report of the Joint Inquiry*, 174.

security as a result of multiple, separate counterintelligence organizations conducting operations.

a. Combining Law Enforcement and Counterintelligence

The first problematic facet of this overlap concerns the combination of law enforcement and counterintelligence under one organization, wherein the FBI serves not only as the leading federal law enforcement agency, but the leading domestic counterintelligence agency as well. The FBI, however, is not the only counterintelligence agency that has arrest authority, for two of the three military counterintelligence organizations – NCIS and AFOSI – are also federal law enforcement agencies.¹³³ Although organizationally speaking, law enforcement and counterintelligence are not strictly divided, as is evidenced by these three organizations, the conduct of counterintelligence operations are nonetheless separate activities from law enforcement operations and as such are governed by different rules.¹³⁴ However, organizationally consolidating both counterintelligence and law enforcement operations into the same agency has created the problem of a divide focus. Any agency that has more than one core mission or focus is potentially likely to devote more time, attention and resources to one mission area over another, the one it deems to be the priority. In the case of the FBI, the priority has traditionally been its law enforcement mission, and not surprisingly, the counterintelligence division has suffered as a result.¹³⁵ This is because of the 28,000 people employed by the FBI, only one quarter of them are specifically employed in an intelligence related function, and not all of them counterintelligence.¹³⁶ Additionally, it seems that on a professional level, special agents working counterintelligence have not been afforded the recognition for their efforts in the same manner that their fellow agents

¹³³ Of note, the U.S. Army is not included in this list as a result of the Church Committee hearings. In the aftermath of these debilitating hearings, the Army separated the two functions by creating a federal law enforcement agency, the Criminal Investigative Division (CID), and moving the counterintelligence function back under the control of the operational chain of command of U.S. Army intelligence, specifically the Intelligence and Security Command (INSCOM).

¹³⁴ *EO12333*.

¹³⁵ *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*. (New York: Markle Foundation, 2002), 20-21. [hereafter referred to as *Markle Report*, pp.#].

¹³⁶ *Markle Report*, 70.

working on traditional criminal matters have; in fact one special agent viewed this situation as being so bad that he referred counterintelligence as the “bastard stepchild” of the FBI.¹³⁷ Therefore, whenever discussing the utility of combining counterintelligence functions within law enforcement agencies the challenges posed by a divided focus should factor into these discussion.

b. Multiplicity of Organizations

The second problem of operational overlap with regard to counterintelligence is the potential to develop a duplication of effort. A duplication of effort could take a number of forms, but essentially given that there are five operational counterintelligence organizations in the U.S. CI community, it seems reasonable that at least two situations could occur: (1) the five separate CI organizations (or at least two of them) could conduct operations targeting the same adversary organizations, and (2) these same organizations could all unwittingly use the same clandestine intelligence sources. This overlap in operations, while it could possibly benefit the counterintelligence efforts against an adversary, is on the whole undesirable when weighing the potential costs against the potential benefits.

On the one hand conducting multiple, yet separate operations against the same adversary could be beneficial by providing different and unique insights into the organization. Another potential benefit resulting from a situation where an adversary organization is penetrated multiple times by separate U.S. counterintelligence agencies is the enhanced security it affords to at least some of the different operations. For example, in a case where the security forces of a penetrated organization detect and subsequently neutralize one clandestine penetration or intelligence network, this same organization is unlikely to uncover all penetrations.¹³⁸ This can potentially lead to the penetrated organization falsely believing it has successfully rooted out the traitors from within itself. As a consequence the adversary organization may only change those security practices

¹³⁷ *Joint Inquiry Report*, 335.

¹³⁸ That is, unless of course all of the counterintelligence organizations involved employ the same specific tradecraft. However, this tradecraft – the tactics, techniques and procedures employed by the counterintelligence officers – would have to be very unique or unusual enough to warrant it becoming an

that are determined to have specifically allowed the penetration to occur and once these changes are completed the organization may let down its guard to a degree. This in turn allows the other counterintelligence organizations to continue running their clandestine networks, and probably more securely than ever. But, despite these potential benefits, there are downsides to multiple counterintelligence agencies working against the same adversary organizations, particularly in the absence of close cooperation and good communication between them. These potential downsides and pitfalls that result from multiple CI organizations operating will be discussed in the following paragraphs.

One problem associated with having multiple CI organizations conduct operations is the potential for multiple organizations to use the same individual as a clandestine source of intelligence. This problem can manifest itself in a number of ways but essentially revolves around determining where an agent's loyalty lies in order to maintain control of him and the potential for an agent in such a situation to deceive U.S. counterintelligence. Each issue will be dealt with in turn.

The first issue concerns establishing control over an agent in the employ of more than one counterintelligence agency. As eluded to before, controlling an agent means ensuring the source's loyalty to his/her handler¹³⁹ and by extension, of course, to the counterintelligence organization overall. Keep in mind that one aim of counterintelligence is to thwart or exploit the efforts of adversary intelligence collectors. This means counterintelligence organizations will attempt to recruit individuals who are members of an adversary intelligence service, especially those working as clandestine case officers¹⁴⁰ or counterintelligence officers. Given that an adversary intelligence/counterintelligence officer is trained to recruit agents and deceive his/her enemies, this makes controlling such an individual tricky at best. Add to this already tricky situation a source that is discovered to be working for more than one "master" (more than one CI organization), and determining this source's loyalty becomes a complex task. In fact, under such circumstances determining who the agent is really loyal

indicator of a specific organization's operations.

¹³⁹ The term "handler" and "case officer" are law enforcement/intelligence jargon for an intelligence/counterintelligence officer who recruits and/or acts as the facilitator of a recruited individual in order to handle the passing of intelligence from the recruited source to the intelligence organization.

¹⁴⁰ see above reference (40).

to may be an exercise in futility, for it is doubtful that any organization is actually controlling this “asset”. Ultimately, if such a determination cannot be made, then the counterintelligence organization could terminate this agent’s employment thus nullifying any potential (future) damage.

The real danger in this kind of situation is if the source is discovered to be a “dangle”¹⁴¹ – an adversary intelligence officer who falsely betrays his parent organization in order to deceive and penetrate the recruiting service. Of course this discovery implies learning of this mole’s other allegiances. If, on the other hand a mole maintains duplicity and remains undiscovered by any of the counterintelligence organizations he/she has penetrated then these organizations would be extremely vulnerable to deception. And since moles are trained intelligence officers, this makes the deception that much more damaging as they are likely very capable of effectively feeding disinformation back to their handlers. Therefore, what U.S. counterintelligence really risks by having multiple organizations conduct counterintelligence operations is being deceived through multiple channels by a trained adversary.

Although one of the main roles of counterintelligence is to prevent penetration by an adversary, the ultimate objective is to guard against enemy deception.¹⁴² However, in a situation where multiple CI organizations are, unawares, employing the same source, there is a greater potential to successfully deceive U.S. counterintelligence as there are more channels to attempt (and succeed at) this deception. While multiple CI organizations could potentially limit a source’s deception by being able to vet the source and verify this source’s reporting with other CI organizations, this would require close cooperation and communication between these organizations. It is uncertain however, given the current structure of the U.S. counterintelligence community, whether a multi-organizational vetting process could be accomplished. Thus, it seems

¹⁴¹ A dangle is a clandestine intelligence officer of a hostile intelligence service who is purposely allowed to be recruited by an adversary service with the full knowledge of his/her parent organization in order to facilitate the penetration of that adversary intelligence service. They are said to be “dangled” like bait, which means they are placed in the sight of the adversary intelligence service in such a way to make the officer appear to be a prime candidate for recruitment.

¹⁴² Alternatively, having a member of a terrorist organization potentially working for more than one U.S. organization can achieve the same basic objective of deception, but to different ends. In this case, it is probably to confuse about the timing, nature or locations of an impending terrorist attack.

having multiple counterintelligence organizations conduct operations potentially poses an unnecessary risk of deception to U.S. counterintelligence overall.

F. FINAL ASSESSMENT: COUNTER-INTELLIGENT STRUCTURE

The U.S. counterintelligence community has been described above in the following ways: overall decentralized, centralized executive authority, divided, and overlapped. All of these different descriptions were provided to give one a sense of how the U.S. counterintelligence community is shaped and organized. Looking at those descriptions alone one would be compelled to conclude that the community is if anything, complex and incoherent. This does not appear to be far off the mark. The structural form that the community takes looks as if it is more of an accidental arrangement than a thoughtful design. Unfortunately, the result of this is a counterintelligence community that cannot function as effectively until the problems and issues that were highlighted are addressed and fixed.

It seems there are three dangers to U.S. security that emerge by having the counterintelligence community structured in an overly decentralized fashion: (1) having counterintelligence operations divided along foreign-domestic lines means that the CI organizations involved are likely to fail to effectively communicate or sufficiently coordinate their efforts to facilitate the “handoff” needed to continuously track transnational foreign threats, such as terrorists or spies, (2) combining law enforcement with counterintelligence potentially means a divided focus, limited resource and methods of operation that are potentially antithetical to one another, and lastly (3) multiple organizations potentially allow a duplication of effort as well as multiple avenues for deception to emerge. Principally this danger is in the form of moles feeding disinformation to the U.S. counterintelligence community through multiple clandestine channels. Thus, on balance it seems that U.S. counterintelligence would benefit from a higher degree of centralization.

THIS PAGE LEFT INTENTIONALLY BLANK

IV. COUNTERINTELLIGENCE REFORM: THE WAY AHEAD

A. INTRODUCTION

The two areas analyzed in the earlier chapters were counterintelligence functions and counterintelligence organization. The last two chapters concluded that the structure of the counterintelligence community was the only aspect that needed substantial reform, this chapter seeks to lay out an approach to that reform. This chapter will build upon the basic assumptions and assessments derived from the earlier chapters, and will propose some measures of reform specifically in terms of restructuring the counterintelligence community to resolve the problems the current structure poses.

B. ORGANIZATIONAL REFORM

Organizational reform for the U.S. counterintelligence community is long overdue. As the third chapter concluded, the U.S. counterintelligence community is dysfunctional at best. U.S. counterintelligence is a hodge-podge grouping of culturally distinct organizations – law enforcement, intelligence, military, and civilian – whose structural design rests on the separation of foreign and domestic operations. This structural design appears to be an accidental result of the piecemeal approach taken to organizing U.S. intelligence over at least the last fifty years.¹⁴³ Although there are a multitude of factors that contributed to this dynamic, clearly the constitutional and legal constraints placed on policing and intelligence work, which emphasize civil liberties and the right of the individual over the ability of the state to invade the privacy of its citizens for the sake of security, are the primary ones that led to this simultaneously divided and overlapping structure. Thus, as a result of these and other, factors, U.S. counterintelligence is in disarray: its constituent organizations are parochial, its operations are overlapping, it shares no common intelligence database and perhaps worst of all, lacks clear, unified guidance and strategic direction from a single authority.

¹⁴³ *Aspin-Brown Commission*, 47.

The following sections will provide some potential solutions to these organizational issues. The first proposal is to create a single counterintelligence agency that would be the only organization given the responsibility and authority to conduct offensive counterintelligence operations. The other part of this proposal is to leave intact the rest of the non-operational components of the counterintelligence community – the support organizations that are spread throughout the IC. This essentially means maintaining the preliminary investigative and analytical functions within these offices and continuing to let these offices work as a networked structure. The second proposal is to centralize counterintelligence reporting. This means creating a single, unified intelligence and threat information database specifically for counterintelligence, to which each counterintelligence organization can contribute intelligence garnered in the course of its duties. The third proposal is to suggest expanding the current network of direct and indirect support counterintelligence organizations by creating offices of counterintelligence at all levels of government, federal, state, and local as well within the private sector. These proposals, while exploratory in nature and certainly not all-inclusive, might provide a roadmap towards reorganizing the U.S. counterintelligence community.

1. Centralized Operations, Distributed Support

It has been observed that operationally the U.S. counterintelligence community suffers from a lack of cohesion. This lack of cohesion is manifested in at least two ways: (1) there are five counterintelligence organizations – two national level agencies and three military service counterintelligence components – that all individually and separately conduct offensive counterintelligence operations, and (2) there is no central counterintelligence authority that controls the operations of these organizations or their budgets. This situation leaves the U.S. as at risk from penetration by foreign powers, whether terrorist or spies. One potential solution to this situation is centralizing counterintelligence operations. However, in order to be effective this centralization must resolve both issues of multiple organizations and a lack of central control.

The centralization of U.S. counterintelligence must begin with the issue of separate counterintelligence organizations with operational responsibilities. Since the analysis in Chapter 3 determined that numerous counterintelligence organizations with operational authority leaves the U.S. counterintelligence community vulnerable to penetration through multiple avenues, it seems the best way to counteract this threat is to reorganize counterintelligence into a single organization. Most importantly, this single organization would be the only U.S. counterintelligence agency that has an operational responsibility or capability. This reorganization would essentially remove the operational counterintelligence component from the CIA, the FBI, and the three military services. At the same time however, this reorganization would not altogether dismantle the analytical and investigative counterintelligence capability of any of these five organizations. Although this issue will be dealt with more thoroughly in the following paragraphs, it should be noted that in order to facilitate the preliminary investigative and analytical capabilities of each parent organization, the existing counterintelligence agencies or offices will need to remain intact and in place.

Some clarification should be provided at this point concerning the operations for which the new counterintelligence organization will be responsible. Essentially the new national-level counterintelligence agency would have the specific and singular authority to conduct counterintelligence operations that employ the more intrusive and clandestine tradecraft used to thwart adversary intelligence operations. Primarily this counterintelligence tradecraft – the diverse array of tactics, techniques and procedures used to deceive or deny the adversary intelligence collector – refers only to those methods used to conduct *neutralization* and *exploitation operations* as outlined earlier in Chapter 2. As demonstrated in Chapter 2, counterintelligence can be broken down into two basic functions: (1) identifying and assessing the threat posed by hostile intelligence services or terrorist organizations and (2) exploiting the adversary intelligence or terrorist operations to the advantage of the U.S. It is this second function that logically gives rise to both types of counterintelligence operations, *neutralization* and *exploitation*.¹⁴⁴ Although these two operations only constitute half of the core competencies, it should be

¹⁴⁴ See: Chapter 2, Section B. The Functions of Counterintelligence for a more detailed discussion of this.

remembered that all of the core competencies are employed concurrently in conjunction with one another. However, it is only the last core competency *exploitation operations* that should be centralized under the control of one operational authority.

This means that all of the functions that fall under the rubric of *neutralization operations* should be left within the various counterintelligence organizations. These functions are resident within both the *direct* and *indirect support* counterintelligence organizations that were discussed in detail in the third chapter. In essence this means that the responsibility and authority to conduct the other less sensitive functions of counterintelligence, ones that do not employ clandestine tradecraft that are potentially subject to compromise or deception, can and should be left within the existing counterintelligence organizations. Counterintelligence investigations, specifically those conducted for reasons of treason, espionage, spying, subversion and sedition, as well as the various analytical functions, such as making threat and vulnerability assessments are all examples of counterintelligence functions that are unlikely to compromise the sensitive sources and methods employed by U.S. counterintelligence to its adversaries.¹⁴⁵ The reason that counterintelligence investigation methods are unlikely to compromise sources is because the techniques employed are overt and based on standard investigative practices that are employed by a wide variety of investigating bodies. Analytical products, such as vulnerability assessments, also employ overt and commonly used scientific and academic methods for producing them. In fact, unless investigative reports or analytical assessments contain information that specifically discusses or alludes to a covert method for obtaining that information, then neither of these types of activities is likely to tip-off an adversary to penetration by a counterintelligence service.

There is also a reasonable argument for allowing the CI support organizations to retain the more sensitive functions of *neutralization operations*: the capability and authority to conduct defensive or low-level source operations. Defensive or low-level source operations are similar in nature to the more sensitive and clandestine offensive counterintelligence operations, in that they are essentially networks of human intelligence

¹⁴⁵ *FM 34-60*, Appendix A and *MCWP 2-14*, 7-17 through 7-30. Both the Army and Marine Corps CI manuals provide detailed descriptions of these techniques demonstrating that while these techniques are both greatly beneficial and generally non-sensitive as they are overt, ethical and legally-constrained methods of detecting and deterring espionage and other hostile or illicit intelligence activities.

assets providing a source of information to the respective organizations for defensive and force protection purposes.¹⁴⁶ But, the conduct of defensive/low-level source operations would need to be strictly regulated by the central counterintelligence agency to ensure that these operations do not cross over into the jurisdiction of the national-level agency. One way to prevent an overlap between these operations and the offensive operations under the control of the central agency, would be to institute a reporting requirement whereby each CI organization seeking to employ an individual as an intelligence source solely for defensive purposes would be required to inform the central agency of this development to include the details of the individual to be employed. In addition to this reporting requirement, another way to mitigate the possibility of overlap would be to limit the conduct of defensive/low-level source operations to the immediate geographic area surrounding the facilities under the purview of each organization. This would force these CI organizations to focus on developing assets that provide indicators of suspicious activities targeting the organization in the immediate vicinity. This is a technique that is currently used by the military counterintelligence organizations that in essence extends the eyes and ears of security beyond the fences of military bases and is apparently very useful. By allowing CI support organizations to run source-operations only within the immediate vicinity of their facilities and instituting a reporting requirement would greatly diminish the chances for such operations to overlap with those of the central counterintelligence agency. This is because these requirements both prevent these operations from developing beyond their intended purpose and prevents the inadvertent employment of the same source by two different organizations, the risk of which was thoroughly discussed in the third chapter.

In addition to the above-mentioned reasons, it would behoove U.S. counterintelligence to leave these particular capabilities resident within the parent organizations because doing so allows the counterintelligence professionals in those positions to keep a pulse on the organization. This is the insider advantage. The benefit that insiders – a counterintelligence professional who is a member of the parent organization – have is their ability to establish a background picture, or otherwise stated a

¹⁴⁶ These operations could potentially provide indications of hostile intelligence activity as much as the threat of terrorist activity that could be targeting a facility. For more information refer to Chapter 2, Section 2 a. *neutralization operations*, where these operations were discussed in greater detail.

sense of what is normal for that organization. This internal perspective is crucial for detecting anomalies, or indications that suggest the organization may be targeted for collection and potentially penetrated by a hostile intelligence collector. Without a resident counterintelligence capability it is very difficult to detect deception or root out moles from within the organization as these anomalies only become apparent when a sense of what is normal – the pattern of day-to-day activities – is somehow disrupted.¹⁴⁷ Further evidence to support this proposal is found by noting the operational requirement for U.S. counterintelligence to conduct threat and awareness briefings of both public and private sector organizations that are potentially at risk from hostile intelligence collection activities, and or those who may be the target of terrorist attacks.¹⁴⁸ These programs demonstrate the need to make the employees of any given organization aware of the potential for hostile intelligence activity directed against them from foreign or internal sources. In addition it also keeps employees more alert for any suspicious indicators that suggest a terrorist group is targeting the organization. This in turn shows how vital an internal counterintelligence capability is in helping to detect and deter foreign operations, whether spies or terrorists. A relevant example of this kind of capability and its associated programs, are the annual counterintelligence threat awareness briefings conducted by the Department of Energy's Office of Counterintelligence that are also made publicly available via the internet.¹⁴⁹ Of note, the most recent briefings provide awareness training on suspicious indicators of both hostile intelligence and terrorism operations.¹⁵⁰ By leaving these organizations intact as such, this would create a virtual network of counterintelligence support organizations distributed throughout the IC who could work to provide investigative and analytical support to the community as a whole, and the operational center specifically.

¹⁴⁷ Godson, *Counterintelligence*, 218.

¹⁴⁸ Within the Department of Defense these programs are governed under DoD Directive 5240.6 *Counterintelligence Awareness and Briefing Program* (Washington, D.C.: GPO, 26 February 1986). However, DoD agencies are not the only ones who conduct these kinds of programs, with the best example being the Department of Energy's *Counterintelligence Awareness Guide* (Washington, D.C.: GPO, 2000). Available [online]: http://www.nnsi.doe.gov/C/Courses/CI_Awareness_Guide/Threat.htm [12 April 2003], that is unclassified and promulgated via the internet to its constituent offices throughout the country.

¹⁴⁹ U.S. Department of Energy. Office of Counterintelligence. *2002 Counterintelligence Awareness Briefing*. (Washington, D.C.: GPO, 2002). Available [online]: http://www.nnsi.doe.gov/S/init/SSB2003/Counterintelligence_Awareness_03-19-02.ppt. [hereafter referred to as *DOE CI Awareness Briefing*].

¹⁵⁰ *DOE CI Awareness Briefing*

Returning to the centralization of operations, it is critical to remember that the reason for removing the CI operational capability from the five aforementioned agencies is the very sensitive nature of *neutralization* and *exploitation* operations. Thus, these functions must be placed under the direct supervision of one controlling authority. It is important to note that only the most sensitive counterintelligence functions, the offensive counterintelligence operations that are conducted using penetrations, moles, double-agents, dangles and the like, should be centralized under the control of one national-level agency. This means that aside from the overt activities of investigations and analysis, the rest of the counterintelligence offices would not be allowed to conduct these kinds of operations.

Although this proposal may sound radical, the call to centralize counterintelligence operations is not new or a result of the events of 9/11. It is true that 9/11, along with the recent revelations of spies being caught within our intelligence services, provide a reason to discuss such a proposal. The case of 9/11, as discussed earlier in the third chapter, provides a cogent example of the need for one agency to run counterintelligence operations that are not restricted by limitations due to geography. For instance, if there had been only one agency that was allowed to run counterintelligence operations and that organization was allowed to conduct surveillance and track Nawaf al-Hazmi and Khalid al-Mihdhar around the globe and most importantly as they crossed into America, then the linkages these individuals had to *Al-Qa'ida* might not have been missed and their activities domestically would have been taken for what they were, planning for a terrorist attack. However, in reality there were at least two different organizations tracking these two individuals, the CIA and FBI, and both were limited to tracking the two *Al-Qa'ida* operatives on the basis of their location (foreign or domestic). Since neither organization adequately coordinated with the other at the crucial point when al-Hazmi and al-Mihdhar crossed over into the U.S., the FBI missed the linkages between these individuals and *Al-Qa'ida* and ultimately their domestic activities did not receive the attention they should have. Had the FBI known that both al-Hazmi and al-Mihdhar were linked to *Al-Qa'ida* and thus potentially terrorists, it is possible that they would have been arrested, much as their alleged fellow co-conspirator Zacarias Massaoui was

arrested in Minnesota, and that this could have disrupted the 9/11 plot.¹⁵¹ However, the case of 9/11 is just one example of a problem that has long been recognized by some analysts and policy makers but has yet to be solved.¹⁵² Unfortunately, the organizational challenge remains.¹⁵³

Interestingly, in the often divergent analyses of Intelligence Community re-organization that have occurred in the past two years largely as a result of September 11 the discussion of U.S. counterintelligence organization is quite unified. The relatively few authors and analysts that have discussed counterintelligence, both those within the community, as well as those outside it, are unanimous in their agreement that U.S. counterintelligence organization and operations suffer from a lack of coherence and centralized direction.¹⁵⁴ Some of these authors cite issue of incompetence in the various organizations in conducting counterintelligence.¹⁵⁵ Other authors cite reasons of a divided mission focus on the part of the FBI as a reason to centralize U.S. counterintelligence operations into a singular organization.¹⁵⁶ One suggestion offered by some of these authors is to strip counterintelligence from the FBI and create a separate domestic intelligence agency. While the reasons for doing so may differ, ranging from FBI incompetence in intelligence work in general, to issues of a divided mission focus, the authors all generally agree that some new agency, whether a domestic intelligence agency (that would seem to have both “positive” and counterintelligence roles) or a strictly counterintelligence agency, need be established to correct past deficiencies and to

¹⁵¹ Bill Gertz, *Breakdown: How America's Intelligence Failures Led to September 11*. (Washington, D.C.: Regnery Publishing Inc., 2002), 196-206. An excellent discussion of Zacarias Massaoui's arrest on the suspicion that he was a terrorist and had ties to Usama Bin Ladin are found in an excerpt of the letter by FBI Special Agent Coleen Rowley to FBI Headquarters provided by Gertz in one of his appendices that outlines the headquarters failure to adequately address the Massaoui case which, in the opinion of Special Agent Rowley, could have potentially unraveled the 9/11 plot before it happened.

¹⁵² Godson, *Counterintelligence*, 218-222.

¹⁵³ *Ibid.* Chapter 7, entitled, *Counterintelligence Organization and Operational Security in the 1980's* in its entirety, from pp. 210-257, provides an excellent discussion of the shortfalls in U.S. counterintelligence organization as it was recognized in the 1980's, and in many ways provided the theoretical underpinnings for this thesis.

¹⁵⁴ These authors', some of whose works have been variously cited throughout this thesis, form a representative sample of the most vocal advocates of counterintelligence reform and are provided here for comparison: William Odom, Mark Riebling, Siobhan Gorman (National Journal), Gordon Cordera (Jane's), Sen. Richard Shelby, John Hamre, John McGaffin and Robert David Steele.

¹⁵⁵ Steele, *The New Craft of Intelligence*, 22-23. Odom, 178; *Joint Inquiry Report*, 402.

¹⁵⁶ Gertz, 99-100; 168.

ensure future success.¹⁵⁷ One author, retired Army General and former National Security Agency director William Odom, argues that not only should the FBI be stripped of this responsibility, but so should the CIA in order to create a single “National Counterintelligence Service.” Yet, he curiously leaves the counterintelligence components of the three military services out of this consolidation process.¹⁵⁸ However, not all of these authors agree that the FBI or CIA need be stripped of their counterintelligence capabilities, nor do they all agree as to what exact form a new domestic intelligence agency should take – some advocate creating an organization along the lines of Britain’s domestic security service, MI-5, while others suggest this model is not applicable.¹⁵⁹ While disagreements are evident in these discussions, a unifying thread nonetheless remains: U.S. counterintelligence organization in its current form is the primary reason for the ineffectiveness of its operations.

There have been some official efforts to rectify these shortfalls. The aforementioned PDD-75 and its offspring, NCIX, are the clearest examples of these efforts.¹⁶⁰ However, as noted earlier NCIX does not appear to have the “teeth” it needs to dictate policy for the community as a whole. Unfortunately, while it seems to be a well-intentioned attempt to give U.S. counterintelligence a focal point for guidance and direction, PDD-75 does not appear to give NCIX control over operations and probably limited control, at best, over the budget, the two most important aspects of organizational control.¹⁶¹ Despite the fact that NCIX has been charged to develop and maintain a centralized strategy for the U.S. counterintelligence community,¹⁶² without operational or budgetary control over the various offices and agencies that make up the community,

¹⁵⁷ Odom, 170; Gorman, “FBI, CIA remain worlds apart”; Mark Riebling, “Getting Smart: Three steps toward a more intelligent intelligence community,” *National Review*. 20 July 2002;

¹⁵⁸ Odom, 183.

¹⁵⁹ Robert Bryan, et al., “America Needs more Spies,” *The Economist*. 10 July 2003. Available [online]: http://www.economist.com/world/na/displayStory.cfm?story_id=1907776 [12 July 2003].

¹⁶⁰ *The PDD on CI-21: Counterintelligence for the 21st Century*.

¹⁶¹ *Ibid.* Although there is a section within PDD-75 that discusses NCIX’s responsibility with respect to the budget that states, “*The Office, working with the DCI’s Community Management Staff, will review, evaluate, and coordinate the integration of CI budget and resource plans of, initially, the DOD, CIA and FBI.*”, it is uncertain what amount of actual control this coordination actually has over the budget.

¹⁶² This was discussed earlier in Chapter 3, C. Organizational Outline of the Community, 2. Centralized Authority.

NCIX is unlikely to effect much change in the community's practices. Worse, NCIX is in no position to accomplish the centralization of operations that is needed to ensure security of the USG, the Intelligence Community or the private sector.

On balance, it seems that advocates for counterintelligence reform are pushing for the centralization of counterintelligence – both in operations and organizations, while at the same time it appears that the USG has done little substantively to address these issues. The creation of the NCIX, while evidence of the federal government's concern for counterintelligence failings, is a limited endeavor at best that itself appears unable to change what are essentially deeply rooted organizational problems. However, these problems will likely be fixed only with the creation of a centralized counterintelligence organization that handles operations, and the continuing presence of numerous counterintelligence support organizations distributed throughout the community to facilitate the investigative and analytic functions so critical to the success of this intelligence discipline.

2. Centralized CI Reporting

This next proposal concerns the need for a centralized repository for counterintelligence reporting. Counterintelligence, in order to be truly effective, relies on a comprehensive picture of the various threats posed to the United States, whether state or non-state actor, spy or terrorist. This means counterintelligence reporting from the military, intelligence, and law enforcement communities must be incorporated into this single database. This means all types of counterintelligence reporting derived from all different means must be included as well. The bulk of the data in this repository should be in the form of raw and unanalyzed intelligence but should also include counterintelligence analysis products and vulnerability assessments that could potentially benefit any organization having access to this database. Thus, this database can serve as a means of passing intelligence indications and warning (I&W) as well as facilitating long term assessments and deep analysis of issues pertinent to the counterintelligence community writ large.

This centralized database, while needed to help develop coherence between the separate CI organizations as well as ensuring that counterintelligence analysis products and vulnerability assessments are comprehensive as possible, is also potentially problematic. In order for this centralized database to be as comprehensive as it should be, it needs to contain counterintelligence reporting concerning both external and internal threats. This is where the database potentially becomes a problem because the rules for disseminating and allowing access to each kind of reporting differ. This requires some further discussion.

The reason that these rules differ is based on the relative sensitivity of each kind of reporting. In terms of counterintelligence reporting concerning external threats, the widest possible dissemination is definitely warranted and necessary. Disseminating external threat reporting broadly ensures that all the organizations with access to this database will be informed and aware of suspicious and potentially hostile activity targeting their organization. The only limitation to disseminating such information is in the event U.S. counterintelligence adopts a more devolved community structure involving state and local authorities; this gives rise to issues of classification and giving state and local authorities access to restricted national security information. However, this potential problem will be discussed a little further in the following section.

Disseminating counterintelligence reporting that concerns internal threats faces a similar, yet different problem. Placing counterintelligence reporting that discusses general trends in or observations of suspicious indicators, which may be indicative of internal penetration, is not problematic in itself. The problem is in giving broad access to counterintelligence reporting that concerns threats internal to a particular organization. Counterintelligence reporting that discusses specific organizations being internally targeted, or worse, those that discuss individuals under investigation for suspicious activity, can potentially “tip-off” or alert an adversary who may have access to the database. Once warned, an adversary could then curtail or stop all such activity in order to “fall below the radar screen” helping them to evade security. Essentially, this means wide dissemination of counterintelligence reporting that discusses the details of suspicious indicators within a particular organization is likely to hinder an investigation into such activity. An example of this can be found in reading the Department of Justice

report that discusses the shortfalls in the investigation conducted into the treasonous activities of Robert Philip Hanssen, the FBI counterintelligence officer indicted for spying on behalf of Russia for nearly 20 years.¹⁶³ In this report by the Office of the Inspector General on FBI security practices it is noted that Hanssen was given broad access to a classified database that contained sensitive reporting on a wide variety of counterintelligence operations for which Hanssen had no specific need-to-know.¹⁶⁴ As well, the report noted that Hanssen was able to use his access to this same database as a way to determine whether or not any of his treasonous activities had become suspicious or had otherwise come to the attention of internal security personnel. Specifically access to this database allowed Hanssen to conduct searches for reports that may have contained his name or cited the locations of his drop sites where he would pass on his stolen information to the Russians; this essentially allowed Hanssen to monitor for signs of an investigation being conducted against him.¹⁶⁵ Thus, because the FBI failed to properly compartmentalize its sensitive reporting database it not only allowed Hanssen to compromise a broad array of extremely classified counterintelligence operations, it also hindered FBI efforts to detect and investigate Hanssen's activities.

Therefore, in order to make this database both useful and secure, access to the different kinds of reporting will need to be limited to those organizations that have the proper clearance and need-to-know. With respect to external threat reporting, this will be given the widest dissemination possible; with the possible exception of certain state, local or private sector entities that will be discussed in more detail later. Counterintelligence reporting on internal threats that is general in nature and does not contain any information regarding a particular organization or individual under investigation may be disseminated widely as well. What must be guarded most closely, however, are specific indications of penetration into particular organizations or information that identifies a specific individual; such information must be restricted to only those who may be conducting an

¹⁶³ U.S. Department of Justice, Office of the Inspector General, *A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen*. (Washington, D.C.: GPO, 2003). [hereafter referred to as: *OIG Report*, pp.#]

¹⁶⁴ *Ibid.*, 23 & 25.

¹⁶⁵ *OIG Report*, 23.

investigation or those conducting an offensive operation against an identified threat. Even with these limitations, this database will still provide a useful CI tool.

3. The Devolved Counterintelligence Community

One purpose of this section is to suggest that the “federalized” paradigm of counterintelligence is perhaps an outmoded concept that must be replaced by a more “devolved” model of counterintelligence. The first notion, the “federalized counterintelligence paradigm,” is an analytical framework that describes the current structure of the U.S. counterintelligence community specifically, but is one that could generally apply to the IC as a whole. The “federalized paradigm” is essentially the traditional concept of U.S. counterintelligence as a singularly federal government responsibility. The second notion, the “devolved counterintelligence paradigm,” is also an analytical framework, one that will attempt to describe an alternative view of how to structure the counterintelligence community. The “devolved paradigm” is a new concept that suggests counterintelligence is no longer only a federal responsibility, but a collective federal, state and municipal (local) responsibility.

The third chapter demonstrated specifically the need to centralize counterintelligence offensive operations. This injunction to centralize operations did not include CI support functions, however. This suggests that the counterintelligence offices scattered throughout the USG and in the IC specifically should not be dismantled but left in place. This is because the purpose of these CI organizations is to support offensive CI operations by conducting preliminary investigations as well as making counterintelligence analyses and threat assessments on their particular organization. This distributed effort by these CI support organizations allows the centralized counterintelligence operations agency to direct its efforts (i.e. no wild goose chases) and to focus on conducting its offensive operations. In addition it seems U.S. counterintelligence efforts would benefit from as much investigative and analytical support as possible. This is in part because counterintelligence concerns more than just USG organizations, as private sector commercial entities are also targeted, as well as the obvious fact that counterintelligence benefits from more “eyes and ears”, which gives

them more opportunities to detect indicators of suspicious or hostile activity. Therefore, U.S. counterintelligence must not only leave the federal level support organizations in place, it must add the state and local dimensions to their efforts as well.

a. State and Local Counterintelligence offices

This first step towards reorganizing counterintelligence and devolving it from the federal government level is to establish a central counterintelligence office at every other level of government: state, county, and municipal. In addition to this central office, counterintelligence offices should be set up in every major governmental department or agency that has a distinct or potential counterintelligence role. These departments and agencies could include those involved in commerce, law enforcement, emergency management services, as well as port and transit authorities. While this list is not all inclusive, it is representative of those departments or agencies within these state and local governments that could find themselves the target of hostile intelligence collection or terrorist activities and could greatly benefit from having an organic counterintelligence capability. It should be remembered that these counterintelligence offices will only be responsible for conducting analysis to identify real or potential vulnerabilities as well as conducting inquiries and preliminary investigations into suspicious activity and suspected threats. These counterintelligence offices would not have authority to conduct full-blown investigations¹⁶⁶ nor any of the previously discussed counterintelligence operations that fall under the rubric of *neutralization* or *exploitation* operations and are the purview of the new national-level counterintelligence operations agency. In any case, such a CI support network has great potential to spread the burden currently placed on the Federal counterintelligence community, which try as it might, will not pick-up on every indicator, or run down every lead or investigate every anomaly, which could potentially point to a spy or terrorist attempting to infiltrate the U.S.

¹⁶⁶ The only obvious exception to this would be the counterintelligence section of a police agency. Even then issues of intelligence oversight and respecting civil liberties would have to be thoroughly addressed and laws solidified up front before any such capability could really become operationally functional.

b. Encouraging Private Sector Participation

Although these efforts apply to the private sector as well, no such endeavor can be imposed upon the American business community. Programs such as the FBI'S ANSIR, which is used to liaise with and provide information to private corporations and businesses that are a potential target for hostile intelligence collection, is one way to continue to influence the private sector to take threat of espionage, and to a lesser extent, terrorism more seriously. It would behoove these private sector organizations to liaise and network more broadly with their counterparts in both the business community as well as the government, whether federal, state, or local. However, in order for this to be effective, each organization within the business community would have to set-up an internal office devoted to counterintelligence-related activities as well. Specifically these offices would help identify industrial espionage efforts or even the threat of terrorism posed to businesses.

c. The LA TEW as a model for devolving U.S. Counterintelligence

Although these recommendations to establish a devolved and collaborative approach to investigative and analytical counterintelligence support may be precedent setting in regards to U.S. counterintelligence,¹⁶⁷ such endeavors have already been undertaken for counterterrorism, especially in the wake of the September 11 attacks. One of the earliest and best examples in developing a counterterrorism support network that pre-dates 9/11 is the Los Angeles Terrorism Early Warning Group (TEW).¹⁶⁸ The TEW was established in 1996 in order to monitor trends and potentialities that may result in terrorist threats or attack within Los Angeles County.¹⁶⁹ The TEW was founded for two

¹⁶⁷ To the author's knowledge there does not appear to be any historical example or case where U.S. counterintelligence functioned in such a distributed, networked and collaborative fashion.

¹⁶⁸ In addition to these references the author visited the LA TEW on a number of occasions in 2002 in support of research for this thesis, to include attending a couple of monthly meetings, getting a tour of the LA Emergency Operations Bureau where the TEW is located, and interviewing one of the co-founders Sgt. John Sullivan. During one such trip the author was given the opportunity to accompany LA County Sheriff's Department officers assigned to the TEW to a number of other collaborative working group sessions on terrorism throughout the LA area that demonstrate the now extremely interconnected nature of these once disparate agencies.

¹⁶⁹ *Towards a National Strategy for Combating Terrorism*. Second Annual Report of the Gilmore Commission. (Washington, D.C.: GPO, 15 December 2000), G-5. Available [online]:

primary reasons: (1) the Los Angeles metropolitan area is a confluence of over 88 jurisdictions and has at least 42 separate law enforcement agencies, and (2) because the information flow between local responding agencies and the national intelligence community was exceptionally poor.¹⁷⁰ Therefore, in order to break down the barriers between national-level and local-level agencies as well as to distribute the burden sharing among these agencies in a more organized manner, the TEW was created to serve as an Indications and Warning (I&W)/Net Assessment center that utilized open source intelligence to research and assess emerging terrorist threats and attacks.¹⁷¹ The core participants of the TEW include: the LA County Sheriff's Department, the LA Police Department, the LA County Fire Department, the LA County Department of Health Services, and the FBI. It has many other cooperating agencies, but includes not only the various law enforcement and emergency management services spread throughout the greater metropolitan area, but military service components as well.¹⁷²

Thus, it can be observed from the example of the LA TEW that such a collaborative endeavor for counterintelligence is not out of the realm of possibility. Certainly the growing awareness of the threat posed by terrorists, especially in the post-9/11 timeframe, has spurred this cooperation further. An effort of this scope would definitely benefit the counterintelligence community, in much the same way that it has benefited the counterterrorism community. And noticeably too, the TEW model provides a cogent example of a real world interagency endeavor that allows for the timely sharing of intelligence across boundaries otherwise difficult to traverse.

C. CONCLUSION

1. Potential Problems & Benefits of Devolving Counterintelligence

Although this new “devolved paradigm” can solve the old problems created by having U.S. counterintelligence be a divided and singularly federal government

<http://www.rand.org/nsrd/terrpanel/terror2.pdf> [10 March 2003].

¹⁷⁰ *Ibid.*

¹⁷¹ Arquilla and Ronfeldt, *Networks and Netwars*, 125; *Towards a National Strategy for Combating Terrorism*, G-5.

¹⁷² Arquilla and Ronfeldt, *Networks and Netwars*, 124.

responsibility, it is likely to generate some problems of its own. But, this new counterintelligence structure also potentially provides some ancillary benefits not specifically intended as well. On balance, the model is more beneficial to U.S. counterintelligence than the current structure.

One potential problem with a devolved structure is the issue of cooperation and standardization. Since the federal government will not have sole responsibility or control over the counterintelligence activities of the state and local authorities, this may cause problems in cooperation between the counterintelligence offices at these different levels of government. A lack of standardization in training, techniques, and information systems are all potential problems that will hinder this interagency approach to counterintelligence. The training, education and professionalization of counterintelligence personnel could greatly differ from one region, state or locality to the next. This could potentially create problems in communication and cooperation between these separate offices. However, having some differences in the actual techniques employed in conducting investigations, analysis or in making assessments could be a benefit derived from a lack of standardization. In a devolved system, each organization could pursue different approaches. Over time, “best practices” would emerge that other organizations could copy.¹⁷³

Another issue associated with not having standardization in these various counterintelligence offices is the problem of having different information systems by which each counterintelligence office communicates with its counterpart across other levels of government. However, by having collaborative working group sessions that involve the counterintelligence professionals from the different offices meeting one another physically would be one way to work around the information systems issue. But solving the systems issue is crucial if the community is really going to function optimally, especially in regards to accessing the centralized database. This discussion of the centralized database gives rise to an additional problem: the fact that most state and local authorities are not normally given access to classified national security information. Obviously, like the information systems issue, this must be resolved if the counterintelligence community is going to work in a collaborative fashion across levels

¹⁷³ Steele, *The New Craft of Intelligence*, 23.

of government. But then the issue of giving state and local authorities access to classified information is potentially more easily solved, as it really only requires broadening the vetting (background investigations) process for individuals seeking employment in this career field.

Thus, it can be observed that on balance, while this devolved model may give rise to new challenges for the counterintelligence community, the majority of these problems are either mitigated by ancillary benefits or can be solved with a little time, effort or creativity. Therefore there is good reason to adopt this model as the new standard for U.S. counterintelligence.

2. Concluding Remarks

In conclusion it seems U.S. counterintelligence would benefit by re-centralizing the operational components currently resident in the CIA, FBI, AFOSI, NCIS, and within Army's INSCOM into one executive-branch agency. This would greatly limit problems in counterintelligence that are due to: failing to monitor and track transnational threats, being exploited and deceived by foreign spies through multiple channels, as well as providing a more focused and tailored offensive response to penetrations of the U.S. whether from foreign intelligence services or international terrorists. This centralized effort can only succeed if the rest of the counterintelligence community operates effectively as a distributed analytical and investigative support network to these offensive operations. In addition, secure and effective offensive counterintelligence operations require access to a fused intelligence database, one that includes both external threat reporting as well as internal reporting. The existing network of counterintelligence offices that includes all of the offices already established within the federal government should be devolved to include the state and local levels as well. And finally, the new devolved CI community should support and encourage the private sector to be an active participant in securing the U.S. from foreign threats. The culmination of these efforts is likely to see a counterintelligence community that is more capable of detecting, deterring and exploiting the broad array of threats it faces in the years to come.

LIST OF REFERENCES

1. Arquilla, John and David F. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica and Washington, D.C.: RAND, 2001.
2. Arquilla, John and David F. Ronfeldt, eds., *The Advent of Netwar*. Santa Monica and Washington, D.C.: RAND Corporation, 1996.
3. Benson, Robert Louis and Michael, Warner, eds., *VENONA: Soviet Espionage and the American Response 1939-1957*. Washington, D.C.: Government Printing Office, 1996.
4. Best, Jr., Richard A. *Homeland Security: Intelligence Support*. Library of Congress, Congressional Research Service (CRS) Report for Congress, Order Code RS21283, Washington, D.C.: Government Printing Office, 2003.
5. Bunker, Robert J. ed. *Non-State Threats and Future Wars*. London and Portland: Frank Cass & Company, 2003.
6. Conrad, Rachel, "Chinese arrests raise concern over technology exports." *Naples Daily News*. 23 January 2003. Available [online]: <http://www.naplesnews.com/03/01/business/d885278a.htm> [25 January 2003].
7. Davis, Paul K. and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*. Washington, D.C.: RAND, 2002.
8. Doyle, Charles, *Terrorism: Section by Section Analysis of the USA Patriot Act*. Library of Congress, Congressional Research Service (CRS) Report for Congress, Order Code RL312200, Washington, D.C.: Government Printing Office, 2001.
9. Dziak, John J. *Chekisty: A History of the KGB*. Lexington: Lexington Books, 1988.
10. Felix, Christopher [James McCargar]. *A Short Course in the Secret War*. 4th ed. Lanham: Madison Books Inc., 2001.
11. Gertz, Bill. *Breakdown: How America's Intelligence Failures Led to September 11*. Washington, D.C.: Regnery Publishers Inc., 2002.

12. Glazov, Jamie, "Symposium: Diagnosing Al-Qaeda," *Frontpage Magazine*. 18 August 2003. Available [online]: <http://frontpagemag.com/articles/ReadArticle.asp?ID=9416> [20 August 2003]
13. Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action & Counterintelligence*. Washington, D.C. and London: Brassey's, 1995.
14. _____, ed. *Intelligence Requirements for the 1980's: Counterintelligence*. Washington, D.C.: National Strategy Information Center, 1980.
15. Godson, Roy and James Wirtz, eds. *Strategic Denial and Deception: The Twenty First Century Challenge*. New Brunswick and London: Transaction Publishers, 2002.
16. Gorman, Siobhan, "FBI, CIA remain worlds apart," *National Journal*. 01 August 2003. Available [online]: <http://www.govexec.com/dailyfed/0803/080103nj1.htm> [06 August 2003]
17. Gray, Colin S. "Thinking Asymmetrically in Times of Terror," *Parameters*. (2002): 5-14.
18. Gunaratna, Rohan. *Inside Al-Qaeda: Global Network of Terror*. Washington, D.C.: Columbia University Press, 2002.
19. Herrington, Stuart A. "Reviving DoD Strategic Counterintelligence: An Appeal to the 'NCIX'," *American Intelligence Journal*. 20, nos. 1 & 2, (2001): 35-40.
20. Hulnick, Arthur. *Fixing the Spy Machine: Preparing American Intelligence for the 21st Century*. West Port: Praeger Publishing, 1999.
21. *Imbalance of Powers: How Changes to U.S. Law & Policy Since 9/11 Erode Human Rights and Civil Liberties*. Washington, D.C.: Lawyers Committee for Human Rights, 2003.
22. Knott, Stephen F. *Secret and Sanctioned: Covert Operations and the American Presidency*. New York and Oxford: Oxford University Press, 1996.
23. Lesser, Ian ed., *Countering the New Terrorism*. Santa Monica and Washington, D.C.: RAND, 1999.
24. Lichtblau, Eric, "Ex-Agent Gets Some Immunity in Spy Case." *New York Times*. 1 May 2003. Available [online]: <http://www.nytimes.com/2003/05/01/politics/01SPY.html> [01 May 03].
25. Lind, William ed., "The Changing Face of War: Into the Fourth Generation," *Military Gazette*. October 1989.

26. Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press, 1999.
27. Markon, Jerry, "Spy buried secret data stashes in state parks," *The Washington Post*. 31 July 2003. Available [online]: <http://www.azcentral.com/news/articles/0731spy31.html> [01 August 2003].
28. John Miller, Michael Stone and Chris Mitchell, *The Cell: Inside the 9/11 Plot, and Why the FBI and CIA Failed to Stop It*. New York: Hyperion, 2002.
29. Noble, Christopher D. *Espionage in Information Warfare*. Carlisle: U.S. Army War College, 2002. Available [online]: <http://carlisle-www.army.mil/usacsl/divisions/std/branches/keg/98TermII/espionage.htm> [10 June 2003].
30. Odom, William. *Fixing Intelligence for a More Secure America*. New Haven: Yale University Press, 2003.
31. Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage -2002*. Washington, D.C.: NCIX, 2003.
32. Olson, James M. "A Never Ending Necessity: The Ten Commandments of Counterintelligence", *Studies in Intelligence*. 46, no. 11 Washington, D.C.: U.S. Central Intelligence Agency, 2001.
33. Rafalko, Frank J., ed., *A Counterintelligence Reader, Volume II: Counterintelligence in World War II*. Washington, D.C.: National Counterintelligence Center, 1999.
34. Richelson, Jeffery T. *Foreign Intelligence Organizations*. Cambridge: Ballinger Publishing Co., 1988.
35. Riebling, Mark. *Wedge: From Pearl Harbor to 9/11: How the Secret War Between the CIA and FBI Has Endangered National Security*. New York: Simon & Schuster, 2002.
36. Sawyer, Ralph D. and Meichung Sawyer. *The Tao of Spycraft: Intelligence Theory and Practice in Traditional China*. Boulder and Oxford: Westview Press, 1998.
37. Shelby, Richard, "Intelligence and Espionage in the 21st Century", *Heritage Lectures*, no. 705, 18 May 2001. Available [online]: <http://www.heritage.org/Research/NationalSecurity/HL705.cfm> [10 August 2003].

38. Steele, Robert D. *The New Craft of Intelligence: Personal, Public, & Political*. Oakton: OSS International Press, 2002.
39. _____. *On Intelligence: Spies and Secrecy in an Open World*. Oakton: OSS International Press, 2001.
40. Unattributed, "U.S. intelligence: Saudi military riddled by Al Qaida infiltrators", *World Tribune*. 14 May 2003. Available [online]: http://www.worthynews.com/zone.cgi?http://216.26.163.62/2003/ss_terror_05_14.html [20 May 2003].
41. U.S. Army, Field Manual 34-17. *Counterintelligence Operations*. Washington, D.C.: Department of the Army, 28 February 1968.
42. _____, Field Manual 34-60. *Counterintelligence*. Washington, D.C.: Department of the Army, 3 October 1995.
43. U.S. Central Intelligence Agency, *A Consumer's Guide to Intelligence*. Washington, D.C.: Office of Public Affairs, 2002.
44. U.S. Congress, Senate. *Commission on the Roles and Capabilities of the United States Intelligence Community*. Washington, D.C.: Government Printing Office, 1996.
45. _____, Senate and House. Permanent/Select Committees on Intelligence. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 with additional views*. 107th Cong., 2d sess., 2002.
46. _____, Joint Economic Committee. *Security in the Information Age: New Challenges, New Strategies*. Washington, D.C.: Government Printing Office, 2002.
47. U.S. Department of Defense, DoD Directive 5240.6 *Counterintelligence Awareness and Briefing Program*. Washington, D.C.: Government Printing Office, 26 February 1986.
48. _____, DoD Directive 5105.67 *Department of Defense Counterintelligence Field Activity (DoD CIFA)*. Washington, D.C.: Government Printing Office, 19 February 2002.
49. U.S. Department of Energy. *Department of Energy (DOE) FY2001 Presidential Budget Request for the Office of Counterintelligence*. Washington, D.C.: Government Printing Office, 2001. Available [online]:

- www.cfo.doe.gov/budget/01budget/_otherdef/counter/counter.pdf [15 August 2003].
50. U.S. Department of Justice. Office of the Inspector General. *A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen*. Washington, D.C.: Government Printing Office, August 2003. Available [online]: <http://www.usdoj.gov/oig/special/03-08/final.pdf> [01 September 2003].
 51. U.S. Federal Bureau of Investigation, *Attorney General Guidelines for Foreign Intelligence Collection and Foreign Counterintelligence Investigations*. Washington, D.C.: Government Printing Office, 18 April 1983. Available [online]: <http://cryptome.sabotage.org/fbi-guide.htm> [10 January 2003].
 52. U.S. Marine Corps, Marine Corps Warfighting Publication 2-14. *Counterintelligence*. Washington, D.C.: Headquarters of the Marine Corps, 5 September 2000.
 53. U.S. President. *Executive Order*. "United States Intelligence Activities, Executive Order 12333," Federal Register 46, no. 59941 (4 December 1981). Available [Online]: <http://www.fas.org/irp/offdocs/eo12333.htm> [20 February 2003].
 54. _____. *Presidential Decision Directive 39*. "U.S. Counterterrorism Policy," Washington, D.C.: Government Printing Office, 21 June 1995. Available [Online]: <http://www.ojp.usdoj.gov/odp/docs/pdd39.htm> [01 September 2003].
 55. Van Creveld, Martin. *The Transformation of War*. New York: Simon & Schuster, 1991.
 56. Waller, J. Michael. *Secret Empire: The KGB in Russia Today*. Boulder: Westview Press, 1994.
 57. Wannal, W. Raymond, "Undermining Counterintelligence Capability," *International Journal of Intelligence and Counterintelligence*. 15 (2002): 321-329.
 58. White House fact sheet - *The PDD on CI-21: Counterintelligence for the 21st Century*. Available [online]: <http://www.fas.org/irp/offdocs/pdd/pdd-75.htm> [10 May 2003].

THIS PAGE LEFT INTENTIONALLY BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. David Tucker
Naval Postgraduate School
Monterey, California
4. James Russell
Naval Postgraduate School
Monterey, California
5. Captain Robert Simeral
Naval Postgraduate School
Monterey, California
6. Captain Steven Ashby
Naval Postgraduate School
Monterey, California
7. John Sullivan
LA Terrorism Early Warning (TEW) Group
Los Angeles, California
8. Rusty Capps
The Center for Counterintelligence and Security Studies
Alexandria, Virginia
9. Robert David Steele
Open Source Solutions, Inc.
Oakton, Virginia
10. David Jimenez
Texas Association of Crime & Intelligence Analysts
El Paso, Texas