AU/ACSC/121/2001-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

INTELLIGENCE OVERSIGHT REVISITED:

DOES CONUS BASE SECURITY REQUIRE A CHANGE?

by

Victor J. Valdez, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col David J. Wallace

Maxwell Air Force Base, Alabama

April 2001

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01APR2002	N/A	-

Title and Subtitle Intelligence Oversight Revisited: Does CONUS Base Security Require a Change?	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Valdez, victor J.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Air Command and Staff College Air University Maxwell AFB, AL	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 53	

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Tables

Page

Preface

I chose this topic because of my personal experiences during my career. I served as a terrorism analyst monitoring the terrorist threat in the US and I performed counterintelligence collections overseas and in the CONUS. I wanted to explore two questions. Is there a new terrorist threat environment and does it warrant modifying the sacrosanct intelligence oversight rules. I believe it is important to continue to examine how the US military performs its counterintelligence mission and how can it be improved.

I wish to thank my Faculty Research Advisor, Lt Col David J. Wallace, USAF, for his patience and support during the writing of this paper. His understanding of my personal obstacles helped me complete this project.

AU/SCHOOL/NNN/2001-04

Abstract

This paper examined the changes in the terrorist threat in the United States (US) and questioned if these changes warrant a revision of intelligence oversight (IO) limitations on military counterintelligence (CI) agencies in order to provide greater security for military bases. The paper demonstrated that the terrorist threat in the United States increased. Using the Department of Defense (DoD) methodology to assess terrorist threat level and applying publicly available information, the terrorist threat in the US should be assessed as Medium. Most terrorism experts agree there will be a terrorist attack in the US in the future. Even taking into account the objections of the General Accounting Office, most experts agree that a terrorist group will employ weapons of mass destruction, probably in the US and possibly against the military. These two assumptions demonstrated that the risks of failing to prevent a terrorist attack are greater than ever.

Terrorist will target military installations and personnel because they are visible symbols of American power. installation commanders must protect their bases from a terrorist attack. The installation commander's mission to protect their base is facilitated by a robust antiterrorism program, which includes an effective CI capability. Military CI agencies have the responsibility to warn commanders of potential terrorist attacks. When CI organizations operate in the US and collect information on possible terrorist threats, they must conduct their activities in accordance with intelligence oversight guidelines. Intelligence oversight rules were created to regulate when

and what type of information could be collected on US persons. The rules were designed to protect American civil liberties from excessive government intrusion.

Given the importance of detecting and preventing a terrorist attack, the current IO guidelines do restrict some CI collections. Primarily, the current IO guidelines do not address domestic terrorism. The rules should include provisions to collect on US persons reasonably believed to be involved in domestic terrorism. Also, the rules should allow for full utilization of open source intelligence (OSINT). A revision of IO rules should remove any ambiguity on what OSINT is collectable and retainable. Nearly all public information is available via the Internet, either for free or for a fee. The revised IO rules should address if CI agencies can do some type of "data mining" from the Internet to collect information on US persons and under what conditions. The IO rules were established long before the Internet technology was in place and should be revised to account for the technology. This approach will best prepare the military counterintelligence agencies to perform their tasked missions and provide warnings of possible terrorist attacks.

Chapter 1

Introduction

> *No matter how high the aims predicated by terrorist, their activities are always criminal, always destructive, throwing human kind back to a time of lawlessness and chaos, provoking internal and international complications, contradicting the goals of peace and progress.*
>
> —Andrei Sakharov[1]

This paper will examine changes in the terrorist threat in the United States and question if these changes warrant a revision of intelligence oversight limitations on military counterintelligence agencies in order to provide greater security for military bases. Many experts agree the United States (US) terrorist threat has changed in three ways. First, the US terrorist threat (domestic and international) is higher than in previous decades. This belief is characterized as the greater likelihood that a terrorist act will occur in the future. Second, terrorists will seek to inflict mass casualties. Finally, terrorists may employ chemical, biological, radiological, or nuclear (CBRN) weapons. CBRN weapons are also referred to as weapons of mass destruction (WMD). These changes in the terrorist threat will impact the security of military bases in the United States.

Terrorist will target military installations and personnel because they are visible symbols of American power.[2] This was demonstrated in 1983 when the Marine barracks in Beirut, Lebanon, was attacked. It was demonstrated in 1996 when the Air Force dormitory at Khobar Towers, Saudi Arabia, was bombed. It was demonstrated in 1997 when the Federal Bureau of

Investigations (FBI) thwarted a planned attack on Fort Hood, Texas. Most recently, it was demonstrated in 2001 when the USS Cole was bombed in the Port of Aden, Yemen. Given this history, installation commanders must protect their bases from a terrorist attack.

The installation commander's mission to protect their base is facilitated by a robust antiterrorism program, which includes an effective counterintelligence (CI) capability. Military CI agencies have the responsibility to warn commanders of potential terrorist attacks.[3] When CI organizations operate in the US and collect information on possible terrorist threats, they must conduct their activities in accordance with intelligence oversight guidelines. Intelligence oversight rules were created to regulate when and what type of information could be collected on US persons. The rules were designed to protect American civil liberties from excessive government intrusion. This paper will question if the increased terrorist threat justifies a modification or revision of existing intelligence oversight limitations on CI agencies.

Design

There are four assumptions that must be tested to justify lessening intelligence oversight rules on military CI agencies. The first assumption is the terrorist threat in the US has increased. That is, there is a greater possibility a terrorist attack will occur than in previous decades. The second assumption is that the nature of the terrorist threat has changed. Specifically, the nature of the target or the type of weapon employed has changed. Third, military CI agencies are hindered in their collection and dissemination of terrorist threat intelligence under current intelligence oversight guidelines. Finally, military CI agencies will be better able to provide warnings of terrorist attacks if intelligence oversight rules are modified. There are inherent limitations in testing these assumptions.

There are two limitations inherent in this study. One limitation is the difficulty in assessing a terrorist threat level. The process for assessing the terrorist threat is addressed in Chapter 3. However, one key problem to note is the inability to accurately understand the terrorist's intention. While some terrorist like Usama Bin Laden will openly advocate attacking American interest, others are more secretive. Yet, knowing the terrorist's intention is key to assessing the threat level. The second limitation is the subjective nature of the topic. Most of the terrorism experts offer subjective opinions. There is little objective input when determining future terrorist attacks.

Research Methodology

The research methodology employed for this paper entailed review and analysis of primary and secondary sources, both historical and contemporary. Primary sources included, but were not limited to, presidential executive orders; Congressional records; DOD, Joint Staff, and United States Air Force (USAF) directives, instructions and reports. Secondary sources used included various professional, scholarly, and journalistic articles concerning terrorism and counterterrorism options.

Notes

[1] Quoted in Statement of Honorable William H. Webster, former Director Central Intelligence Agency and former Director Federal Bureau of Investigations, in House, *The Future of U.S. Antiterrorism Policy: Hearing and Markup of H. Res. 118 to Condemn the Release by the Government of Malta of Convicted Terrorist Mohammed Ali Rezaq before the Subcommittee on International Security, International Organizations and Human Rights,* 103rd Cong., 1st Sess., 1993: 61.

[2] Joint Pub (JP) 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 1998, II-10.

[3] Ibid, V-1.

Chapter 2

Background

> *The collection and computerization of information by government must be tempered with an appreciation of the basic rights of the individual, of his right to privacy, to express himself freely and associate with whom he chooses.*
>
> —Senator Samuel J. Ervin, Jr.[1]

Before examining the four assumptions necessary to change intelligence oversight rules, it is important to understand the origin of the limitations and to know the current rules. While these rules apply to all Department of Defense (DoD) personnel, they are aimed at intelligence, counterintelligence, and intelligence-related activities. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IO)) is charged with the management and oversight of this program.

Origin of Intelligence Oversight Limitations

The Department of Defense, as well as other US Government agencies, operates under intelligence oversight rules to protect the civil rights of individuals and to ensure previous civil rights abuses are not repeated. During the 1960s and early 1970s, the military intelligence community (including counterintelligence units) violated the civil rights of Americans. The military intelligence community treated legitimate political expression as a threat to national security. By the early 1970s, the military intelligence community had accumulated massive

amounts of information on Americans – based primarily on their political views.[2] These abuses began with an initial desire to protect military forces.

The military's civil rights violations originated during the 1960s with the need for pre-deployment intelligence before assisting civil authorities.[3] The civil rights and anti-Vietnam War movements led to "significant civil demonstrations."[4] Civil authorities requested military assistance to restore order. The Army was designated executive agent for providing aid to civilian authorities. Even by today's standards, it is understandable that military units needed and requested pre-deployment intelligence before assisting civil authorities. Since they were charged with helping restore order, the military commanders need to know who was causing the civil unrest and what threats faced their troops. These are legitimate concerns. According to the ATSD(IO)'s web site, the "mission creep" began at this point.[5] The Army began collecting required force protection information when the FBI was unable to provide meet their needs. "Eventually, DoD intelligence personnel were using inappropriate clandestine and intrusive means to collect information on the legitimate political positions and expressions of US persons, accumulating that information in a nationwide data bank, and sharing that information with law enforcement authorities."[6]

The scope of the abuse is best illustrated by listing some of the worst activities of the military intelligence during this period. ATSD(IO)'s web site list the following activities to highlight this point:

> Military counterintelligence special agents established, maintained, and disseminated files on civil rights activists and organizers.
>
> Counterintelligence special agents penetrated organizations such as the "Resistors in the Army" and the "Friends of Resistors in the Army" and recruited members of these organizations as informers. These organizations posed no foreign threat.

> So called "dissidents", actually US persons who were exercising their First Amendment rights, were placed under surveillance and their movements were observed and recorded.
>
> Radio communications of civil rights and anti-war demonstrators were intercepted by military intelligence personnel.
>
> Using media cover, military counterintelligence special agents infiltrated the 1968 Democratic National Convention in Chicago.
>
> Information collected by Defense elements was routinely transferred to civilian law enforcement authorities without evidence of criminal activity or relevance to the law enforcement missions of the receiving authorities.[7]

When the scope of these activities became public, Congress evaluated the degree of abuse by the military. In 1971 and 1974, the US Senate's Subcommittee on Constitutional Rights reported tens of thousands of card files and dossiers of potential "dissidents" were kept on file by Military Intelligence. The committee also reported "fifty-four federal agencies operated no fewer than 858 databanks that contained more than a billion separate records on American citizens. Eighty-four percent operated without any explicit legal authorization, and fewer than 33 percent of them notified citizens that they were collecting information about them."[8] As a result of congressional oversight, the DoD restricted the future surveillance of US persons, destroyed existing files, and developed an oversight mechanism to monitor intelligence oversight.[9]

Current Intelligence Oversight Rules

DoD intelligence agencies are governed two key Intelligence Oversight documents, Presidential Executive Order 12333 and DoD Directive 5240.1-R.[10] Executive Order 12333, United States Intelligence Activities, 4 December 1981, recognized that "timely and accurate' intelligence is important to national security.[11] However, EO 12333 added several restrictions to

prevent abuses by the intelligence community. Specifically, as related to terrorism, the following rules apply:

> 2.3 Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General … Those procedures shall permit collection, retention and dissemination of the following types of information:
>
> (a) Information that is publicly available or collected with the consent of the person concerned;
>
> (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;
>
> (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations[12]

DoD Directive 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, December 1982, implements EO 12333 and provides similar guidance. According to DoDD 5240.1-R the following guidance is provided regarding the counterintelligence collection and terrorism:

> Procedure 2 – Collection of Information about United States Persons.
>
> C. Types of information that may be collected about United States persons. Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories:
>
> 1. Information obtained with consent.
>
> 2. Publicly available information. Information may be collected about a United States person if it is publicly available.
>
> 4. Counterintelligence. Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:

a. persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.

11. Threats to Safety. Information may be collected about a United States person when the information is needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations.[13]

While other definitions are listed in the Glossary, it is important to clarify what a US person is considered. According to DoDD 5240.1-R, a "United States person" means: (1) A United States citizen; (2) An alien known by the DoD intelligence component concerned to be a permanent resident alien; (3) An unincorporated association substantially composed of United States citizens or permanent resident aliens; or, (4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person.[14]

Notes

[1] Quoted in "Mission and History: Assistant to the Secretary of Defense (Intelligence Oversight)", on-line, Internet, 7 February 2001, available from http://www.dtic.mil/atsdio/mission.html.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Charles J. Sykes, "Beware the Brave New World," *Hoover Digest*, 2000 No. 2, n.p.; on-line, Internet, 12 February 2001, available from http://www-hoover.stanford.edu/publications/digest/002/sykes.html.

[9] As a side story, the author was stationed with an Army Warrant Officer assigned to Army Military Intelligence. The MI soldier recounted that his first assignment in MI, during the 1970s, was spent destroying files on US persons. According to the MI soldier, he spent two years on this task.

Notes

[10] "Welcome to the Intelligence Oversight Office", on-line, Internet, 7 February 2001, available from http://www.dtic.mil/atsdio/welcome.html.

[11] Executive Order 12333, United States Intelligence Activities, 4 December 1981.

[12] Ibid.

[13] DoD Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982.

[14] Ibid.

Chapter 3

The Changing Terrorist Threat

> *America will become increasingly vulnerable to hostile attack on our homeland, and our military superiority will not entirely protect us…Americans will likely die on American soil, possibly in large numbers.*
>
> —The United States Commission on National Security/21st Century[1]

The terrorist threat in the United States has changed due to the higher probability of a terrorist attack, the nature of the target, and the possible use of weapons of mass destruction. Almost every source consulted agreed the terrorist threat in the United States has changed for the worse for one or all of these reasons. Hence, the first two assumptions of the author's argument (increased terrorist threat and changed nature of the terrorist threat) can be demonstrated to be valid.

Increased Terrorist Threat

FBI data, three separate commissions, and the recent arrest of a terrorist support the argument the United States faces a higher terrorist threat. A review of FBI data for the past twenty years revealed several interesting trends on terrorist activity in the United States (Table 1). First, the number of terrorist incidents since 1982 decreased until it hit zero in 1994. After 1994, the number of incidents has gradually increased. Second, the number of terrorist incidents prevented remained relatively stable for most of the period and significantly increased in the last couple of years. The terrorist attacks and the terrorist incidents prevented include both domestic

and international terrorism. For the latest year available, the FBI reported all 5 terrorist incidents and all 12 prevented incidents were attributed to domestic terrorists.[2] Three commissions concurred with the FBI data and assessed the terrorist threat will increase.

Table 1. Terrorist Activity in the United States

Year	Terrorist Incidents	Incidents Prevented
1982	51	3
1983	31	6
1984	13	9
1985	7	23
1986	25	9
1987	9	5
1988	9	3
1989	4	7
1990	7	5
1991	5	5
1992	4	0
1993	12	7
1994	0	0
1995	1	2
1996	3	5
1997	2	20
1998	5	12

Source: House, *The Future of U.S. Antiterrorism Policy: Hearings and Markup of H. Res. 118 To Condemn the Release by the Government of Malta of Convicted Terrorist Mohammed Ali Rezaq before the Subcommitte on International Security, International Organizations and Human Rights*, 103d Cong., 1st sess., 1993, 277, and Department of Justice, *Terrorism in the United States, 1998* (Washington, D.C.: Federal Bureau of Investigations, 1998), 6.

In the last three years, three commissions were chartered to examine some aspect of the terrorist threat and all three commissions assessed an increased threat. The Department of Defense chartered one commission and Congress chartered the other two. In 1998, the Secretary of Defense chartered the United States Commission on National Security/21st Century (USCNS/21) to evaluate how the world will likely evolve over the next 25 years, to suggest a US national security strategy to deal with that world, and to propose government structures and

processes to enable the U.S. government to implement that strategy.[3] As part of the USCNS/21 process, the commission concluded, "America will become increasingly vulnerable to hostile attack on our homeland, and our military superiority will not entirely protect us."[4] The Congressional commissions arrived at similar conclusions.

Two Congressional mandated commissions assessed a greater likelihood of terrorist attacks against the United States, occurring in the United States. Section 591 of the Foreign Operations, Export Financing, and Related Programs Appropriations Act, 1999, established The National Commission on Terrorism.[5] The National Commission on Terrorism concluded international terrorist would attack the US within our borders and act out of a hatred of the US.[6] Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, echoed this assessment during testimony before the Senate Select Committee on Intelligence. Vice Admiral Wilson stated, " The terrorist threat to the US will grow as disgruntled groups and individuals focus on America as the source of their trouble."[7] A second Congressional commission on combating terrorism stated in its December 2000 report, "The potential for terrorist attacks inside the borders of the United States is a serious emerging threat … a terrorist attack on some level within our borders is inevitable …."[8] Unfortunately, a recent event supports the commissions' assessments.

The December 1999 arrest of Ahmed Ressam highlights the reality of the terrorist threat in the United States and that Usama Bin Laden remains a deadly adversary. Ahmed Ressam is an Algerian who was living in Canada prior to his arrested on 14 December 1999. Ressam was arrested at the US/Canadian border at Port Angeles, Washington. He was in possession of 130 pounds of bomb making material in his car. The subsequent investigation disclosed Ressam belonged to a terrorist sleeper cell of Usama Bin Laden's Al Qaeda organization. He was entering the US to conduct terrorist attacks during the millennium celebrations. Ressam's

probable target was Seattle's New Year celebration at the Space Needle.[9] Former National Security Advisor Samuel R. Berger stated, "One thing we learned from the Ressam case is that there is an increasing vulnerability here, that there are people here in the US that have connections to these groups … the possibility of Bin Laden activating other as yet unidentified cells for attacks is a the center of the threats we face over the next few years."[10] It becomes evident from this case that Usama Bin Laden remains a threat to the United States.

Figure 1 Usama Bin Laden

Usama Bin Laden has publicly proclaimed his intention to attack the United States and the US Government believes Bin Laden will strike again. On 23 February 1998, Bin Laden issued a "fatwa" stating, "it was a religious duty for all Muslims to wage war on U.S. citizens, military and civilian, anywhere in the world."[11] George J. Tenet, Director of Central Intelligence, stated before the Senate Select Committee on Intelligence, "Usama Bin Ladin is still foremost among these terrorists, because of the immediacy and seriousness of the threat he poses. Everything we have learned recently confirms our conviction that he wants to strike further blows against America. Despite some well-publicized disruptions, we believe he could still strike without additional warning."[12] Although many accept this view, at least one analyst cautioned against mistaking vulnerability for a threat.

Michael A. Wermuth of the Rand Corporation warned Congress not to mistake vulnerability for a threat. Wermuth stated, "The United States will always be vulnerable in almost limitless ways. We are an open society, with relatively open borders to foreign visitors. The length of our borders and the sheer amount of commerce and tourism that floods through our ports each day, makes it virtually impossible to detect every agent or device that a terrorist may try to bring into our country. But just because we are vulnerable in any number of ways, does not necessarily mean that a current threat exists to exploit that vulnerability."[13] Wermuth's advice is sound, but does not dispute the higher terrorist threat level.

Using the information presented above and using the DoD terrorism threat level matrix, the terrorism threat level in the United States should be assessed as Medium. Appendix A contains the full DoD methodology for assessing the terrorism threat level. According to Joint Pub 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, a Medium terrorist threat is characterized by the "presence" of terrorist groups, the "capability" of terrorist groups to conduct attacks, and a "history" of terrorist attacks.[14] Figures 2 and 3 disclose the presence of international and domestic groups that are present in the United States. These groups may pose a terrorist threat. The Medium threat level does not require an "intention" to attack. Nevertheless, given the statements by Bin Laden, it can be argued that there is an existing intention to conduct terrorist activity. Of course, the primary counter argument to this assessment is the security environment in the United States. JP 3-07.2 defined "security environment" as "The internal political and security considerations that impact on the capability of terrorist elements to carry out their operations."[15] It becomes a subjective question whether the US security environment is sufficient to deter or prevent a terrorist attack.

Figure 2 International Terrorist Groups Represented in US[16]

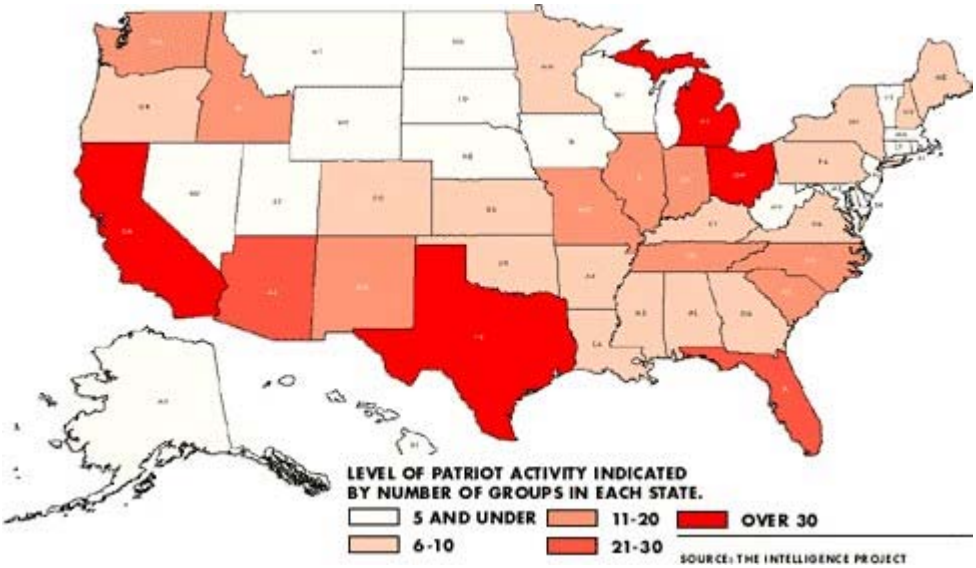

Figure 3 Militia Groups in the US[17]

Changed Nature of the Terrorist Threat

In addition to the increased terrorist threat, the nature of the threat changed by a greater tendency to inflict mass casualties and the greater likelihood of employing weapons of mass destruction. Whether the target is the American military or civilians, terrorists have demonstrated a willingness to inflict mass casualties. Even using a conventional weapon, the FBI identified a trend in terrorist activity toward more large-scale incidents designed for maximum destruction, terror, and media impact. Such attacks, even if fewer place more Americans at risk.[18] Both international and domestic terrorists have chosen this option, e.g. World Trade Center and Oklahoma City bombing. The National Commission on Terrorism identified the same trend in their report. The Commission highlighted the arrest of Ressam and his planned attack of Seattle's New Year's celebration.[19] An estimated 50,000 people were expected to attend that celebration before it was cancelled.[20] Terrorist will be able to inflict mass casualties easier if they used WMD.

The FBI, CIA, and DoD assess a growing willingness by terrorist to use WMD. Referring to Table 1, of the12 acts of domestic terrorism prevented in the United States during the 1998, two prevented terrorist acts involved the planned use of biological toxins.[21] The FBI reported the following regarding WMD cases (Table 2):

> "WMD cases--primarily those dealing with attempted procurement or threatened use of chemical, biological, and nuclear/radiological materials--increased steadily since 1995, rising from 37 in 1996 to 74 in 1997, to 181 in 1998. Threatened release of biological agents, such as anthrax or Bubonic plague, has become the most prevalent component of this disturbing trend. Threatened use of biological agents accounted for more than half of the WMD cases in 1998. By mid-1998, anthrax—also known as Bacillus Anthracis--had emerged as the agent of choice in WMD hoaxes."[22]

Table 2. WMD Investigations Opened by FBI

Type of Investigation	1997	1998
Nuclear	25	29
Chemical	20	23
Biological	22	112
Missile	2	1
Unknown	5	16

Source: Department of Justice, *Terrorism in the United States, 1998* (Washington, D.C.: Federal Bureau of Investigations, 1998), 14.

Concurrent with FBI statistics, two recent US Government reports echoed the warning of terrorist WMD use. As part of the USCNS/21 process, the commission concluded, "States, terrorists, and other disaffected groups will acquire weapons of mass destruction and mass disruption, and some will use them. Americans will likely die on American soil, possibly in large numbers."[23] In January 2001, the then-Secretary of Defense signed his *Proliferation: Threat and Response* report. The report identified the US vulnerability to WMD and the interest of Bin Laden to pursue this capability. The report stated, "The possible acquisition or use of NBC materials by terrorists, inadequate security of NBC materials, and threats to agriculture and livestock are some of the issues that greatly concern the United States and its allies."[24] The report also identified Bin Laden's interest in pursuing a WMD capability. Bin Laden's interest in NBC materials has been noted since the early 1990s and, in 1999, Bin Laden made public statements defending the right of the Muslim community to pursue WMD capabilities.[25] The US intelligence agencies supported this assessment.

Both the CIA and DIA leaders recently testified to Congress that terrorist will use WMD against the US. Director Tenet testified:

> "Mr. Chairman, we remain concerned that terrorist groups worldwide continue to explore how rapidly evolving and spreading technologies might enhance the lethality of their operations. Although terrorists we've preempted still appear to be relying on conventional weapons, we know that a number of these groups are

> seeking chemical, biological, radiological, or nuclear (CBRN) agents. We are aware of several instances in which terrorists have contemplated using these materials. Among them is Bin Ladin, who has shown a strong interest in chemical weapons. His operatives have trained to conduct attacks with toxic chemicals or biological toxins. HAMAS is also pursuing a capability to conduct attacks with toxic chemicals."[26]

Vice Admiral Wilson concurred with Director Tenet's assessment and told Congress, "The potential for terrorist WMD use will increase over time, with chemical, biological, and radiological agents the most likely choice."[27] However, unlike the previous assumption, there is disagreement on the threat of terrorist use of WMD.

The two arguments against terrorists use of WMD are the terrorists lack the capability to overcome the obstacles involved with these weapons and the terrorists prefer conventional weapons. Norman J. Rabkin, Director for National Security Preparedness Issues, General Accounting Office, presents the most pervasive argument against terrorists using WMD. Rabkin argues the executive or legislative branch may be getting an exaggerated view of the terrorist threat. Specifically, the CIA indicated "it was relatively easy to for terrorist to produce and use CBRN agents."[28] Rabkin countered that claim. He stated there were "significant technical and operational challenges" that terrorist had to overcome before employing chemical or biological agents.[29] These obstacles included specialized knowledge for manufacturing, designing an effective delivery device, difficulty in obtaining chemical or biological components, and assuming personal safety risks when no vaccines or antidotes exist. The GAO provided Congress the visual aid in Figure 4 to depict the "stages and obstacles that terrorist would face in developing, producing, weaponizing, and disseminating chemical and biological materials."[30] The failure of the Aum Shinrikyo group supports Rabkin's opinion.

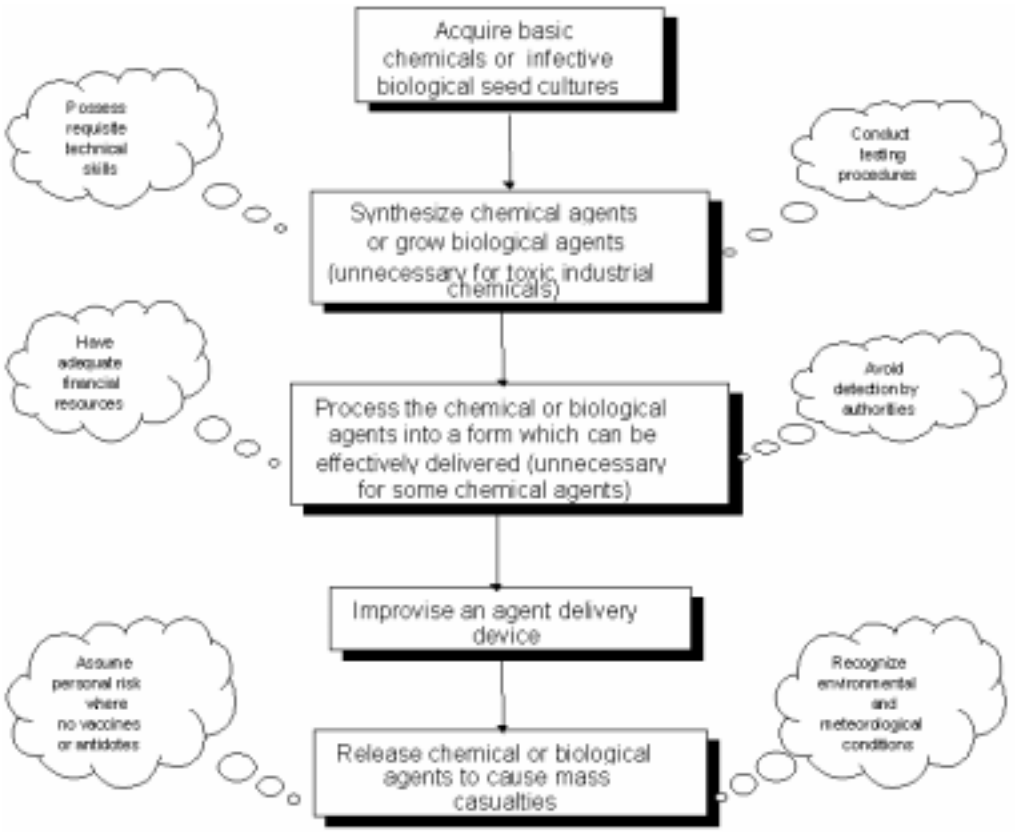

Figure 4 Stages for Terrorist to Conduct Chemical and Biological Terrorism and Obstacles to Overcome

The failure of the Aum Shinrikyo group, with its vast resources, supports the argument that terrorist groups do not have the capability to employ WMD. To date, only nation-states have succeeded in weaponizing CBRN weapons.[31] The Aum Shinrikyo group attempted to use CBRN weapons to produce mass casualties and failed. A report for the United States Air Force Counterproliferation Center reported the Aum Shinrikyo group had over 1 billion dollars in assets and top scientist from Japan and Russia. Despite these advantages, they failed to produce the results they sought.[32] The National Commission on Terrorism summed up the groups failures in its report, "The group used scores of highly skilled technicians and spent tens of millions of dollars developing a chemical attack that killed fewer people than conventional explosives could have. The same group failed totally in a separate attempt to launch an anthrax

attack in Tokyo."[33] Perhaps, because of examples like Aum Shinrikyo, terrorist groups prefer conventional weapons.

Terrorist groups prefer conventional weapons because they are easier to acquire, easier to handle, easier to use, and can still produce mass casualties. The FBI considers the WMD threat lower than "the threat from conventional terrorist tactics, such as bombings, shootings, and kidnappings, which remain the preferred method to carry out attacks."[34] Michael Wermuth makes the point that not only is the capability lacking from non-state sponsored domestic terrorist groups to use WMD, but also there is no intelligence on an intention to employ these weapons.[35]

The counter arguments to the terrorist use of WMD are legitimate concerns but not convincing. The CIA stated they know of international terrorist groups, especially Bin Laden's Al Qaeda, seeking to obtain a WMD capability. The FBI data demonstrates a dramatic increase in the number of investigations of WMD cases. Many of these cases proved to be hoaxes, but not all. Wermuth pointed out the US Government is preoccupied with planning for the worse-case scenario, countering a vulnerability instead of the threat. There is sufficient information publicly available to indicate a terrorist threat does exist and involves the possible use of WMD. "It is only a matter of time before US military forces will encounter terrorist use of WMD."[36]

A Constant Terrorist Threat

There remains one constant terrorist threat regardless of the threat level or the type of weapon employed; the American military will remain a favored terrorist target. Terrorist will target military installations and personnel because they are visible symbols of American power, interest, and influence.[37] There were two significant attacks against US military forces in the past five years: the bombing of the USS Cole (Figure 5) in the Port of Aden in October 2000 and

the bombing of the US Air Force dormitory at Khobar Towers (Figure 6) in Saudi Arabia in 1996. Both attacks demonstrated the US military continues to be targeted by terrorist. In both attacks, it can be argued the terrorist sought mass casualties. The terrorist threat to the US military remains valid in the continental US (CONUS) also.

Figure 5 USS Cole

Figure 6 Khobar Towers

The US military has been and remains a terrorist target in the United States. To date, the attacks have not been on the scale of the USS Cole or Khobar Towers. The DoD suffered from a variety of smaller terrorist attacks in the 1970s and 1980s. These incidents included attacks by

Puerto Rican independence groups and Plowshare peace movements. In 1997, for the first time, domestic right-wing extremists targeted and attempted an attack against a U.S. military installation in the United States.[38] In July 1997, the FBI thwarted an attack on Fort Hood, Texas, being planned by right-wing extremists who apparently believed US military installations were being used as training facilities for United Nation (UN) forces preparing to take over the United States. Bradley Glover, a self-proclaimed militia Brigadier General, anticipated an "engagement" with UN troops, which he believed were stationed at Fort Hood. The FBI advised the DoD of the planned assault, and on July 4, 1997, Glover and co-conspirator Michael Dorsett were arrested approximately 40 miles southwest of Fort Hood. Warranted searches of Glover's truck and Dorsett's home revealed explosive devices, explosive components, a homemade firearm silencer, assault rifles, pistols, chemicals, ammunition, body armor, camouflage clothing, and a copy of the Militia Soldiers Operations Handbook.[39] It is logical to assume future attacks against the US military will occur.

This chapter demonstrated the author's first two assumptions of his argument are valid. The terrorist threat level has increased. There is a greater chance of a terrorist attack in the United States. There is also a strong possibility that terrorist will seek mass casualties during their attack. One probable method for terrorist to achieve mass casualties is for them to employ WMD. "The combination of unconventional weapons proliferation with the persistence of international terrorism will end the relative invulnerability of the U.S. homeland to catastrophic attack. A direct attack against American citizens *on American soil* is likely over the next quarter century."[40] Finally, the US military will remain the favored target of a future military attack and should expect an attempt in the CONUS.

Notes

[1] U.S. Commission on National Security/21st Century, Phase I Report, *New World Coming: American Security in the 21st Century*, 15 September 1999, 4; on-line, Internet, 10 February 2001, available from http://www.nssg.gov/Reports/NWC.pdf.

[2] Department of Justice, *Terrorism in the United States, 1998* (Washington, D.C.: Federal Bureau of Investigations, 1998), 1.

[3] U.S. Commission on National Security/21st Century, Phase III Report, *Roadmap for National Security: Imperative for Change*, 15 February 2001, v, 130; on-line, Internet, 10 February 2001, available from http://www.nssg.gov/PhaseIIIFR.pdf.

[4] USCN/21, Phase I Report, 4.

[5] "There is established a national commission on terrorism to review counter-terrorism policies regarding the prevention and punishment of international acts of terrorism directed at the United States. The commission shall be know as 'The National Commission on Terrorism'". The National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (Washington, D.C.: Government Printing Office, 2000), 49-50; on-line, Internet, 18 March 2001, available from http://w3.access.gpo.gov/nct.

[6] Ibid, iv.

[7] Statement of Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, in Senate, *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*, 106th Cong., 2nd sess., 2 February 2000, 24.

[8] Robert Holzer, "Threats to US Homeland Loom Larger: Terror Attacks, Emergencies Test Pentagon, Civil Response," *Defense News*, 15 January 2001.

[9] Josh Meyer, "Border Arrest Stirs Fear of Terrorist Cells in US," *Los Angeles Times*, 11 March 2001.

[10] Ibid.

[11] Department of Defense, *Proliferation: Threat and Response* (Washington, D.C.: Office of the Secretary of Defense, January 2001), 62.

[12] Statement of George J. Tenet, Director of Central Intelligence, in Senate, *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*, 106th Cong., 2nd sess., 2 February 2000, 12.

[13] Statement of Michael A. Wermuth, in House, *Combatting Terrorism: Assessing Threats, Risk Management, and Establishing Priorities: Hearings before the Subcommittee on National Security, Veterans Affairs, and International Relations*, 106th Cong., 2nd sess., 26 July 2000, n.p.

[14] Joint Pub (JP) 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 1998, V-7 to V-8.

[15] Ibid, V-7 to V-8.

[16] Slide obtained from Joint Forces Lesson 535 slide show, Air Command and Staff College, 15 February 2001.

[17] Ibid.

[18] Senate, *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*, 105th Cong., 2nd sess., 1998, 29.

[19] The National Commission on Terrorism, iv, 3.

[20] Meyer, 1.

[21] DOJ, *Terrorism, 1998*, 1.

[22] Ibid, 12-13.

Notes

[23] USCNS/21, Phase I Report, 4.
[24] DoD, *Proliferation*, 61.
[25] Ibid, 62.
[26] Tenet, 12-13.
[27] Wilson, 24.
[28] Statement of Norman J. Rabkin, Director for National Security Preparedness Issues, National Security and International Affairs Division, GAO, in House, *Combatting Terrorism: Assessing Threats, Risk Management, and Establishing Priorities: Hearings before the Subcommittee on National Security, Veterans Affairs, and International Relations*, 106th Cong., 2nd sess., 26 July 2000, n.p.
[29] Ibid.
[30] Ibid.
[31] The National Commission on Terrorism, 4.
[32] Lansing E. Dickinson, *The Military Role in Countering Terrorist Use of Weapons of Mass Destruction*, The Counterproliferation Papers, Future Warfare Series No. 1 (Maxwell AFB, AL: Air University, September 1999), 3.
[33] The National Commission on Terrorism, 4.
[34] DOJ, *Terrorism, 1998*, 14.
[35] Wermuth, n.p.
[36] Dickinson, 37.
[37] Joint Pub (JP) 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 1998, II-10, and Wilson, 24.
[38] DOJ, *Terrorism, 1998*, 19-20.
[39] Ibid, 19-20.
[40] USCNS/21, Phase III Report, viii.

Chapter 4

The Counterintelligence Role in Antiterrorism

> *Intelligence and counterintelligence are the first line of defense in an antiterrorism program.*
>
> —JP 3-07.2[1]

The US military will continue to face a terrorist threat from both international and domestic terrorist in the United States. Domestic terrorists have demonstrated a desire to attack US military installations in the United States. International terrorists have demonstrated the ability to attack US military installations and personnel overseas. The terrorist threat places a responsibility on the CONUS installation commander to protect their installation through appropriate antiterrorism (AT)/force protection (FP) measures. Force protection involves more than reducing base vulnerabilities. Every CONUS military installation is vulnerable in some manner. Yet, "vulnerability" does not equal "threat". The key for the installation commander is to take the appropriate measures to reduce vulnerabilities given the local terrorist threat. The installation commander must have *intelligence* on the terrorist threat to fulfill their mission. This is the role of the local counterintelligence (CI) unit on base.

Counterintelligence Collection Mission

Components of DoD Counterintelligence

Each military service is directed to maintain a counterintelligence capability. The Service Secretaries are directed to ensure "a capability exist to collect, receive, evaluate from a Service perspective, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack."[2] This mission falls on the Service counterintelligence agencies. These agencies are the Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), and US Army Intelligence and Security Command. Within the Air Force, AFOSI is the only organization authorized to conduct counterintelligence activities and operations.[3]

Counterintelligence Requirements

The DoD is responsible for protecting its own personnel and installations, regardless of their location.[4] By Executive Order, the Secretary of Defense must protect the security of Department of Defense installations, activities, property, information, and employees by appropriate means.[5] In the CONUS, the Service Secretaries through the Services are responsible for AT/FP at all Service installations.[6] Installation commanders implement AT/FP measures to protect their personnel and installation. A key component of the installation commander's AT program is an effective counterintelligence capability.

It is DoD policy that CI activities be undertaken to detect, assess, exploit, and counter or neutralize terrorist activities.[7] Joint Doctrine further supports this position. "The role of intelligence and counterintelligence is to identify the threat, provide advance warning, and disseminate critical intelligence in a usable form for the commander. Additionally, counterintelligence provides warning of potential terrorist attacks and provides information for

CT operations."[8] The installation commander is evaluated on how well they integrated CI into their AT program.

A key component of the installation commander's AT program is the local vulnerability assessment, which includes a local threat assessment by the CI organization. The local threat assessment ensures the CI organization collects and disseminates available terrorist threat information to the commander. The CI agency has a standard list of information requirements (IR) to focus their collection effort. The IR list is a compilation of key data the commander needs to protect his or her installation from a terrorist attack. Table 3 is a list of IRs found in JP 3-07.2. However, the one key IR not included on the list is "intention". The commander needs to know the intentions of the terrorist group.

Table 3. Information Requirements

Organization, size, and composition of group
Motivation
Organization's long- and short-range goals
Religious, political, and ethnic affiliations
International and national support; e.g., moral, physical, financial
Recruiting methods, locations, and targets; e.g., students
Identity of group leaders, opportunist, and idealists
Group intelligence capabilities and connections with other terrorist groups
Sources of supply and support
Important dates
Planning ability
Internal discipline
Preferred tactics and operations
Willingness to kill
Willingness for self-sacrifice
Group skills (demonstrated or perceived); e.g., sniping, demolitions, etc.
Equipment and weapons (on-hand and required)
Transportation (on-hand and required)
Medical support availability
Means and methods of command and control
Means and methods of communicating to the public

Source: Joint Pub (JP) 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 1998, V-6.

The CI agency has a responsibility to collect this type of information on known or suspected terrorist groups operating near or with access to a military installation. Per Executive Order 12333, United States Intelligence Activities, military CI agencies will "Conduct counterintelligence activities in support of Department of Defense components outside the United States in coordination with the CIA, and within the United States in coordination with the FBI pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General."[9] The coordination with the FBI in the United States does not mean the CI agency should rely solely on the FBI to provide the information. One reason the DoD cannot rely solely on the FBI is because the GAO reported in 1999 that the FBI has not "captured in a formal, authoritative, written assessment" terrorist threats domestically, from both foreign and domestic sources.[10] Still, the FBI is the lead agency for combating terrorism in the US. There must be a close cooperation between the FBI and military CI agencies. However, the directed responsibility of the DoD to protect its own personnel and installations means the military CI agencies have a responsibility to collect against the IRs listed in Figure 3, even in the CONUS. The lack of intelligence on terrorist groups operating in the CONUS is a threat to the DoD.

CONUS Limitations

Military counterintelligence agencies are hindered in their collection of information requirements by existing intelligence oversight guidelines. As discussed in Chapter 2, all intelligence activity (including counterintelligence) in the United States is guided by intelligence oversight (IO). The IO guidelines hinder CI collections in two ways. First, IO rules do not make any mention of domestic terrorism. The CI collection is limited to US persons who have connections to a foreign government or international terrorism. The planned attack against Ft. Hood in 1997 demonstrated there is a current domestic terrorist threat against the US military.

Current rules do not allow CI agencies to collect information on potential domestic threats until after the group has committed a criminal act. In practical terms, that means the CI agency can collect the information after the group has carried out an attack against the DoD. Again, these restrictions do not apply to US Persons associated with international terrorist groups. The FBI reports there are members of several international terrorist groups (Lebanese Hizballah, Egyptian Al-Gamat Al-Islamiya, and the Palestinian Hamas) present in the United States who could support terrorist operations in this country.[11] (See Figure 2). Because these US Persons are tied to know international terrorist groups, the FBI and DoD can collect information on them.

The second reason the current IO rules hinder CI collection is because they do not account for the available open source information available today. The current IO rules are 20 years old. They rules state the CI agency can collect information that is publicly available. Some may interpret this to mean publicly available information about international terrorist only. This requires clarification. Concurrently, the amount and type of information readily available today through the Internet is staggering. Joint Pub 3-07.2 states open-source information is a primary source of information for counterintelligence.[12] Yet, there are still restrictions against collecting information off the Internet, even though it is publicly available. There has to be an established investigative interest, i.e., probable cause, established before a CI agency can monitor that medium.[13]

The intelligence oversight rules, in their current format, hinder the collection and dissemination of terrorist threat information by omitting the domestic terrorist threat and not adequately addressing the open source information available. The DoD has a directed responsibility to protect itself from a terrorist attack. The military CI agencies are key components of this mission. Operating under the current IO rules, the CI agencies may not be

able to collect against the necessary information requirements and assist the local commander in their AT/FP program. Hence, the third assumption of the author's argument is valid.

Notes

[1] Joint Pub (JP) 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 1998, x.

[2] Ibid, V-3 to V-4.

[3] Air Force Policy Directive (AFPD) 71-1, *Criminal Investigations and Counterintelligence*, 1 July 1999, 1.

[4] JP 3-07.2, viii.

[5] Executive Order (EO) 12333, United States Intelligence Activities, 4 December 1981, para 1.11.h.

[6] DoDD 2000.12, *DoD Antiterrorism/Force Protection (AT/FP) Program*, 13 April 1999, para 5.9.1.

[7] DOD Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982, para 4.1.

[8] JP 3-07.2, V-1.

[9] EO 12333, para 1.11.d.

[10] Statement of Michael A. Wermuth, in House, *Combatting Terrorism: Assessing Threats, Risk Management, and Establishing Priorities: Hearings before the Subcommittee on National Security, Veterans Affairs, and International Relations*, 106th Cong., 2nd sess., 26 July 2000, n.p.

[11] Senate, *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*, 105th Cong., 2nd sess., 1998, 29-30.

[12] JP 3-07.2, x.

[13] Senate, *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*, 105th Cong., 2nd sess., 1998, 86-88.

Chapter 5

Improved Counterintelligence Capability

> *Some terrorists hope to provoke a response that undermines our Constitutional system of government. So US leaders must find the appropriate balance by adopting counterterrorism policies which are effective but also respect the democratic traditions which are the bedrock of America's strength.*
>
> —The National Commission on Terrorism[1]

Intelligence oversight rules should be revised to improve military counterintelligence organizations ability to collect intelligence in face of the greater terrorist threat and still protect American civil rights. At no time does the author or any consulted source recommend doing away with intelligence oversight. The rules are in existence because civil rights must be protected and past abuses of civil rights did occur. However, after operating under the current intelligence oversight rules for over two decades, it is time for a revision to the rules in light of the new environment.

Need for Greater Intelligence Capability

There was one constant theme disclosed during the research for this paper – the need for a better intelligence capability. Almost every official report and all testimony before Congress on this issue called for an increased human intelligence capability. The rationale for the call for greater intelligence is to develop actionable information prior to a terrorist attack. In 2001, two commissions called for greater human intelligence. The USS Cole Commission offered the

following advice in January 2001 after reviewing the Oct 2000 terrorist attack on the USS Cole, "We, like other commissions before us, recommend the reprioritization of resources for collection and analysis, including human intelligence and signal intelligence, against the terrorist…Furthermore, an increase in counterintelligence (CI) resources dedicated to combating terrorism and development of clearer CI assessment standards is required."[2] A month later the final report of the US Commission on National Security made the following recommendation, "The intelligence community should emphasize the recruitment of human intelligence sources on terrorism as one of its highest priorities, and ensure that existing operational guidelines support this policy."[3] Testimony before Congress echoed these recommendations.

The call for better intelligence is not a recent phenomenon and is recommend after most terrorist attacks. After the attack on the World Trade Center bombing, former Ambassador-at-Large for Counterterrorism L. Paul Bremer testified to Congress, "it is absolutely vital that we continue our efforts to have timely and actionable intelligence in the field, and it is one of the more difficult fields to get good intelligence that I am aware of."[4] During the same hearings, former CIA and FBI director William H. Webster stated, "It is important that our intelligence in this area not be shrunk but expanded as the need requirements (sic). The use of informant and undercover agents has proved extremely valuable in this country."[5] Given the stated importance of intelligence, especially human intelligence, there is a strong argument to improve the capabilities of the military counterintelligence agencies.

Revising Intelligence Oversight

Argument For Revising Intelligence Oversight

Counterintelligence agencies are tasked to provide difficult to obtain intelligence on the terrorist threat to local commanders. The National Commission on Terrorism reported, "Obtaining information about the identity, goals, plans, and vulnerabilities of terrorists is extremely difficult. Yet, no other single policy effort is more important for preventing, preempting, and responding to attacks."[6] Vice Admiral Wilson also captured the difficult nature of the terrorist organization as an intelligence target, "The characteristics of the most effective terrorist organizations—highly compartmented operations planning, good cover and security, extreme suspicion of outsiders, and ruthlessness—make them very hard intelligence targets."[7] Admitting the difficulty in collecting information on terrorists, any restrictions that limit the ability of the military counterintelligence agencies should be carefully reviewed.

Intelligence oversight rules should be reviewed to determine what changes can be made that allow greater capabilities to the military CI agencies and still protect American civil rights. Raphael Perl, Congressional Research Service, summed up this balancing act when he testified before Congress, "In the United States addressing terrorist threats and government responses often involves tension between–or balancing of –civil liberties and effective detection of, and response to terrorist threats or acts."[8] The best synopsis of the argument to ease collection restriction and balance civil rights comes from Michael Wermuth of the Rand Corporations. Wermuth provided the following testimony:

> "I am acutely aware of the potential for over-zealousness, for government over-reaching, for the ostensible justification for intrusive efforts that could trample on the civil liberties of our citizens, as well as those from or in other countries. But I am equally as convinced that, with proper planning, with oversight from the Congress and other entities with responsibilities to ensure the appropriateness and

> legality of government actions, we can and must move forward on a broad front, to ensure that everything that can be done – within the boundaries of our Constitutional protections – is being done to protect our citizens, our property, indeed our very way of life, from potential perpetrators of terrorist acts…It is true that the well-established civil rights and liberties of U.S. persons must be protected as part of that process. It may well be true that certain laws and guidelines need to be reviewed, collaboratively between the Executive and Legislative Branches – perhaps even with some scholarly judicially-based input – to determine if minor modifications or adjustments are in order. In my view, we can make improvements without even raising the suggestion that our government is attempting to be more intrusive. As an example, if current laws and guidelines prevents the FBI or other law enforcement agencies from collecting (even with appropriate judicial oversight) and analyzing information on a single individual terrorist – the "lone wolf" in FBI jargon – such as the "Unabomber," Theodore Kaczynski, then perhaps some tweaking of the rules may be in order. I am convinced that that and other adjustments to authorities can be made, while fully protecting our cherished civil rights…A senior official of our national government is purported to have remarked recently that "Americans will willingly give up some of their civil rights" if a catastrophic terrorist event occurs. Mr. Chairman, I believe that, with proper planning and oversight, reasonable men and women, at all levels of government and from the private sector, can find ways to improve our own efforts to combat terrorism without having to resort to such measures."[9]

As mentioned in Wermuth's statement, the American populace is willing to trade some civil liberties for security from terrorism.

Anecdotal and statistical evidence demonstrate the public's willingness to trade some civil liberties for increased protection from terrorism. The public's willingness to endure increased security to include searches when entering public buildings (e.g., Federal courthouse), public gatherings (e.g., football stadiums), and public transportation facilities (e.g., airports) demonstrates a willingness to trade civil liberty for security. Public opinion polls captured data that supported the anecdotal evidence. The polls demonstrated that the public was willing to give up civil liberties if necessary to curb terrorism. However, this willingness decreased as time passed between a terrorist attack and the poll. For example, in the two years after the Oklahoma City bombing, the percentage of Americans willing to give up their civil liberties was almost

inverse of the original poll.[10] The lesson for these polls is that changes in current restrictions can be made but they must be done judiciously and not in haste after a terrorist attack.

Argument Against Revising Intelligence Oversight

There is an argument against making any changes to the current intelligence oversight rules because the rules are adequate and the threat environment does not warrant such changes. As mentioned previously, Wermuth from the Rand Corporation argued against reacting to the worse-case scenario. Using this logic, we should avoid making changes until the US knows conclusively there is an increased threat and changing the IO rules can prevent it. Otherwise, we may repeat the past.

There is the argument that future abuses will occur based on the country's previous experiences. Jack Blum, a Partner at Lobel, Novins and Lamont, testified to Congress his concerns on this issue:

> "The criminal laws of the United States are prospective. We as a society accept the law and most people obey it. Law enforcement is always post facto. A policeman cannot start examining your life till you've broken the law. And that's very fundamental to the way we do business and it's why, when I hear things like the integration of intelligence in law enforcement, I get very nervous because it is our fundamental constitutional right not to have police exploring our lives until we've broken the law…I really worry about people who say the solution to the terrorism problem is additional legislation and additional criminal law, particularly additional police authority to do prospective listening, looking, and poking. That makes me very, very nervous because the long history of this, however well-intentioned the authority is when it's first granted, it winds up being misused."[11]

The final argument against changing the IO rules is the current provision to collect information on a US Person and retain temporarily for 90 days to evaluate the information. [12] This provision can be used to overcome any shortcomings of the IO rules.

The arguments against revising intelligence oversight rules highlight legitimate concerns. However, as mentioned in the previous section, a careful, judicious review of the guidelines can

lead to needed modifications. Also, continued monitoring by the responsible office (ATSD(IO)) should prevent future abuses.

Notes

[1] The National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (Washington, D.C.: Government Printing Office, 2000), ii; on-line, Internet, 18 March 2001, available from http://w3.access.gpo.gov/nct.

[2] USS Cole Commission, *USS Cole Commission Report, Executive Summary*, 9 January 2001, n.p.; on-line, Internet, 22 March 2001, available from http://www.defenselink.mil/pubs/cole20010109.html.

[3] The recommendation was aimed at allowing the CIA to recruit "dirty" sources. The recommendation still applies in this case. U.S. Commission on National Security/21st Century, Phase III Report, *Roadmap for National Security: Imperative for Change*, 15 February 2001, xiv; on-line, Internet, 10 February 2001, available from http://www.nssg.gov/PhaseIIIFR.pdf.

[4] Statement of L. Paul Bremer, former Ambassador-at-Large for Counterterrorism, in House, *The Future of U.S. Antiterrorism Policy: Hearing and Markup of H. Res. 118 to Condemn the Release by the Government of Malta of Convicted Terrorist Mohammed Ali Rezaq before the Subcommittee on International Security, International Organizations and Human Rights,* 103rd Cong., 1st Sess., 1993: 24.

[5] Statement of Honorable William H. Webster, former Director Central Intelligence Agency and former Director Federal Bureau of Investigations, in House, *The Future of U.S. Antiterrorism Policy: Hearing and Markup of H. Res. 118 to Condemn the Release by the Government of Malta of Convicted Terrorist Mohammed Ali Rezaq before the Subcommittee on International Security, International Organizations and Human Rights,* 103rd Cong., 1st Sess., 1993: 63.

[6] The National Commission on Terrorism, 7.

[7] Statement of Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, in Senate, *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*, 106th Cong., 2nd sess., 2 February 2000, 24.

[8] Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service, in House, *Hearings before the House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations*, 26 July 2000, n.p.

[9] Statement of Michael A. Wermuth, in House, *Combatting Terrorism: Assessing Threats, Risk Management, and Establishing Priorities: Hearings before the Subcommittee on National Security, Veterans Affairs, and International Relations*, 106th Cong., 2nd sess., 26 July 2000, n.p.

[10] Lynn M. Kuzma, "Terrorism in the United States," *Public Opinion Quarterly* 64, no. 1 (Spring 2000): 90-105.

[11] Statement of Jack Blum, in House, *Terrorism – Looking Ahead: Issues and Options for Congress, Proceedings of a Seminar Held by the Congressional Research Service, December 7, 1995,* 104th Cong., 2nd Sess., July 1996, 33-34, 36.

[12] DOD Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982, para 3.C.4.

Chapter 6

Conclusions

> *We must get out of the purely defensive mode by proactively applying AT/FP techniques and assets to detect and deter terrorists.*
>
> —USS Cole Commission[1]

Intelligence oversight rules should be modified to provide military counterintelligence agencies a greater capability to collect information on impending terrorist attacks. This paper started with four assumptions. Each of the four assumptions had to be demonstrated to be valid in order to justify changing the fundamental rules that guide the counterintelligence mission in the United States.

All four assumptions are valid. First, it was demonstrated that the terrorist threat in the United States has increased. Using the DoD terrorist threat level methodology and applying publicly available information, it appears the terrorist threat in the US should be assessed as Medium. Most terrorism experts agree there will be a terrorist attack in the US in the future. Second, even taking into account the objections of the GAO, most experts agree that a terrorist group will employ WMD, possibly in the US and possibly against the military. These two assumptions demonstrate that the risks of failing to prevent a terrorist attack are greater than ever. To highlight these risks, the commission chartered by the Secretary of Defense made the following controversial recommendation, "The Department of Defense, which has placed its

highest priority on preparing for major theater war, should pay far more attention to the homeland security mission."[2]

Given the importance of detecting and preventing a terrorist attack, the current intelligence oversight guidelines do restrict some counterintelligence collections. As mentioned in Chapter 4, the current IO guidelines do not address domestic terrorism. The rules should include provisions to collect on US persons reasonably believed to be involved in domestic terrorism. Also the rules should allow for full utilization of open source intelligence (OSINT). A revision of IO rules should remove any ambiguity on what OSINT is collectable and retainable. Nearly all public information is available via the Internet, either for free or for a fee. The revised IO rules should address if CI agencies can do some type of "data mining" from the Internet to collect information on US Persons and under what conditions. The IO rules were established long before the Internet technology was in place and should be revised to account for the technology. This approach will best prepare the military counterintelligence agencies to perform their tasked missions and provide warnings of possible terrorist attacks.

Notes

[1] USS Cole Commission, USS Cole Commission Report, Executive Summary, 9 January 2001, n.p.; on-line, Internet, 22 March 2001, available from http://www.defenselink.mil/pubs/cole20010109.html.

[2] U.S. Commission on National Security/21st Century, Phase III Report, *Roadmap for National Security: Imperative for Change*, 15 February 2001, 23; on-line, Internet, 10 February 2001, available from http://www.nssg.gov/PhaseIIIFR.pdf.

Appendix A

Terrorism Threat Level Matrix

The following table is a matrix used to determine the terrorist threat level of a given location. The DoD methodology is provided below.

Table 4. Terrorism Threat Level Matrix

	Existence	Capability	Intentions	History	Targeting
Critical	x	x	#	#	x
High	x	x	x	x	
Medium	x	x	#	x	
Low	x	x		#	
Negligible	#	#			

Source: JP 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism, 17 Mar 1998, V-7 to V-8.
x = must be present, # = may or may not be present

A threat analysis should be written to the factors below:
Factor 1, Existence: A terrorist group is present, assessed to be present, or able to gain access to a given locale.
Factor 2, Capability: The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.
Factor 3, Intentions: Recent demonstrated anti-US terrorist activity, or stated and/or assessed intent to conduct such activity.
Factor 4, History: Demonstrated terrorist activity over time.
Factor 5, Targeting: Current credible information on activity indicative of preparations for specific terrorist operations and/or specific intelligence which shows that an attack is imminent.
Factor 6, Security Environment: The internal political and security considerations that impact on the capability of terrorist elements to carry out their operations.
Critical: 1,2,5 are present. 3 or 4 may or may not be present.
High: 1,2,3,4 are present.
Medium: 1,2,4 are present. 3 may or may not be present.
Low: 1,2 present. 4 may or may not be present.
Negligible: 1,2 may or may not be present.

Glossary

AFOSI	Air Force Office of Special Investigations
AT	Antiterrorism
ATSD(IO)	Assistant to the Secretary of Defense (Intelligence Oversight)
CBRN	Chemical, Biological, Radiological, Nuclear
CI	Counterintelligence
CIA	Central Intelligence Agency
CONUS	Continental United States
CT	Counterterrorism
DIA	Defense Intelligence Agency
DoD	Department of Defense
FBI	Federal Bureau of Investigations
FP	Force Protection
GAO	Government Accounting Office
IO	Intelligence Oversight
IR	Information Requirement
NCIS	Naval Criminal Investigative Service
OSINT	Open Source Intelligence
UN	United Nations
US	United States
USAF	United States Air Force
USCNS/21	United States Commission on National Security/21st Century
WMD	Weapons of Mass Destruction

antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or

international terrorist activities, but not including personnel, physical, document, or communications security programs.

counterintelligence (CI) collection. The systematic acquisition of information concerning espionage, sabotage, terrorism, and related foreign activities conducted for or on behalf of foreign nations, entities, organizations, or persons and that are directed against or threaten DoD interests.

counterintelligence investigation. Includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

international terrorist activities. Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

lawful investigation. An investigation qualifies as a lawful investigation if the subject of the investigation is within DoD investigative jurisdiction; if it is conducted by a DoD component that has authorization to conduct the particular type of investigation concerned (for example, counterintelligence, personnel security, physical security, communications security); and if the investigation is conducted in accordance with applicable law and policy, including E.O. 12333 and this Regulation.

military department counterintelligence (CI) agency. The Military Department CI Agencies include Army CI, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

no double standard policy. Commanders may immediately disseminate to DoD personnel and facilities information on specific terrorist threats directed against DoD personnel and facilities. However, it is the policy of the United States Government that no double standard regarding availability of information will exist. Official Americans cannot benefit from receipt of information that might equally apply to the public, but is not available to the public. Responsibility for the release of threat information to the public in CONUS remains with the FBI and overseas with the Department of State. Threats directed against or affecting the American public, or against events/locales visited/utilized by the American public, will be coordinated with the FBI or DoS, as appropriate, prior to release. This policy applies only when the information available is sufficient for DoD activities to conclude that an act of terrorism will occur and to predict, with reasonable accuracy, the time, place, mode of the attack, and, if possible, the perpetrators. When such specificity exists, but it is impossible to determine that only Government targets might be affected, it is DoD policy that the reporting entity unilaterally disseminating the information will include both DoS and the AMEMBASSY or AMEMBASSIES concerned, on the message or correspondence. The "No Double Standard" requirement for commanders at all levels is simple: keep either the American Embassy or the local office of the FBI informed of your threat levels and threat conditions. This can be accomplished through direct liaison if authorized or through the CINC via the chain of command.

open source information. This information is publicly available and can be collected, retained, and stored without special authorization.

United States. When used to describe a place, the term shall include the territories under the sovereignty of the United States.

United States person.

a. The term "United States person" means:

(1) A United States citizen;

(2) An alien known by the DoD intelligence component concerned to be a permanent resident alien;

(3) An unincorporated association substantially composed of United States citizens or permanent resident aliens;

(4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person.

b. A person or organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained. An alien in the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained.

c. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.

Bibliography

Air Force Policy Directive (AFPD) 71-1. *Criminal Investigations and Counterintelligence*. 1 July 1999.

Department of Defense (DoD) Directive 2000.12. *DoD Antiterrorism/Force Protection (AT/FP) Program*. 13 April 1999.

Department of Defense (DoD) Directive 5240.1-R. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982.

Dickinson, Lansing E. *The Military Role in Countering Terrorist Use of Weapons of Mass Destruction*. The Counterproliferation Papers, Future Warfare Series No. 1. Maxwell AFB, AL: Air University, September 1999.

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

Kuzma, Lynn M. "Terrorism in the United States." *Public Opinion Quarterly* 64, no. 1 (Spring 2000): 90-105.

Holzer, Robert. "Threats to US Homeland Loom Larger: Terror Attacks, Emergencies Test Pentagon, Civil Response." *Defense News.* 15 January 2001.

Joint Pub (JP) 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 1998.

Meyer, Josh. "Border Arrest Stirs Fear of Terrorist Cells in US." *Los Angeles Times.* 11 Mar 2001.

"Mission and History: Assistant to the Secretary of Defense (Intelligence Oversight)." On-line. Internet, 7 February 2001. Available from http://www.dtic.mil/atsdio/mission.html.

Sykes, Charles J. "Beware the Brave New World." *Hoover Digest*, 2000 No. 2, n.p. On-line. Internet, 12 February 2001. Available from http://www-hoover.stanford.edu/publications/digest/002/sykes.html.

The National Commission on Terrorism. *Countering the Changing Threat of International Terrorism.* Washington, D.C.: Government Printing Office, 2000. On-line. Internet, 18 March 2001. Available from http://w3.access.gpo.gov/nct.

US Cole Commission. *USS Cole Commission Report, Executive Summary*. 9 January 2001. On-line. Internet, 22 March 2001. Available from http://www.defenselink.mil/pubs/cole20010109.html.

US Commission on National Security/21st Century. Phase I Report. *New World Coming: American Security in the 21st Century*. 15 September 1999, 4. On-line. Internet, 10 February 2001. Available from http://www.nssg.gov/Reports/NWC.pdf.

US Commission on National Security/21st Century. Phase III Report. *Roadmap for National Security: Imperative for Change*. 15 February 2001, v, 130. On-line. Internet, 10 February 2001. Available from http://www.nssg.gov/PhaseIIIFR.pdf.

US Department of Defense. *Proliferation: Threat and Response.* Washington, D.C.: Office of the Secretary of Defense, January 2001.

US Department of Justice. *Terrorism in the Untied States, 1995*. Washington, D.C.: Federal Bureau of Investigations, 1995.
US Department of Justice. *Terrorism in the Untied States, 1996*. Washington, D.C.: Federal Bureau of Investigations, 1996.
US Department of Justice. *Terrorism in the Untied States, 1997*. Washington, D.C.: Federal Bureau of Investigations, 1997.
US Department of Justice. *Terrorism in the United States, 1998*. Washington, D.C.: Federal Bureau of Investigations, 1998.
US House. *The Future of U.S. Antiterrorism Policy: Hearing and Markup of H. Res. 118 to Condemn the Release by the Government of Malta of Convicted Terrorist Mohammed Ali Rezaq before the Subcommittee on International Security, International Organizations and Human Rights*. 103rd Cong., 1st Sess., 1993.
US House. *Terrorism – Looking Ahead: Issues and Options for Congress, Proceedings of a Seminar Held by the Congressional Research Service, December 7, 1995*. 104th Cong., 2nd Sess., July 1996.
US House. *Combatting Terrorism: Assessing Threats, Risk Management, and Establishing Priorities: Hearings before the Subcommittee on National Security, Veterans Affairs, and International Relations*. 106th Cong., 2nd sess., 26 July 2000.
US Senate. *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*. 105th Cong., 2nd sess., 1998.
US Senate. *Current and Projected National Security Threats to the United States: Hearings before the Select Committee on Intelligence*. 106th Cong., 2nd sess., 2 February 2000.
"Welcome to the Intelligence Oversight Office." On-line. Internet, 7 February 2001. Available from http://www.dtic.mil/atsdio/welcome.html.